Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 29

А. В. ТЕЛЬНЫЙ

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Проектирование технических средств защиты территорий и объектов от несанкционированного доступа

Учебное пособие

Под редакцией профессора М. Ю. Монахова

Владимир 2020

УДК 004.056.3
ББК 32.971.35-5
Т31

Редактор серии – доктор технических наук, профессор М. Ю. Монахов

Рецензенты:
Доктор технических наук, профессор
зав. кафедрой вычислительной техники и систем управления
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
В. Н. Ланцов

Кандидат технических наук
зам. руководителя Регионального аттестационного центра
ООО «ИнфоЦентр»
Н. В. Вертилевский

Издается по решению редакционно-издательского совета ВлГУ

Т31 **Тельный, А. В.** ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Проектирование технических средств защиты территорий и объектов от несанкционированного доступа : учеб. пособие / А. В. Тельный ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 251 с. – (Комплексная защита объектов информатизации. Кн. 29). – ISBN 978-5-9984-1172-4.

Изложен систематизированный материал по второй части учебного курса «Техническая защита информации»: основные понятия, их определения, требования к проектированию и оснащению территорий и объектов средствами охранно-тревожной сигнализации, контроля и управления доступом и охранного телевидения.

Предназначено для студентов вузов 3 – 4-го курсов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» и специальности 10.05.04 «Информационно-аналитические системы безопасности» очной формы обучения.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Ил. 21. Табл. 13. Библиогр.: 79 назв.

УДК 004.056.3
ББК 32.971.35-5

ISBN 978-5-9984-1172-4

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В настоящее время обеспечение охраны территорий, объектов и конкретных помещений от несанкционированного доступа потенциальных нарушителей становится все более актуальной задачей. Кроме преступных посягательств с целью завладения материальными ценностями широкое распространение получила конкурентная разведка для создания экономического преимущества, а предметом посягательства стали защищаемые информационные ресурсы организаций и предприятий.

В качестве технических средств защиты территорий, объектов и помещений от несанкционированного доступа выступают средства инженерно-технического укрепления элементов строительных конструкций, системы охранно-тревожной сигнализации, контроля и управления доступом и охранного телевидения.

Технические возможности нарушителей по преодолению инженерно-технической защиты объектов постоянно возрастают. Физический доступ к защищаемым материальным и информационным ценностям остается самым эффективным средством конкурентной борьбы в условиях рыночной экономики. При этом используются самые современные технические средства и методы несанкционированного доступа к защищаемой информации.

Однако в сложившихся условиях развиваются и совершенствуются и технические средства защиты информации от несанкционированного доступа. Появляются новые виды охранных извещателей, контрольных панелей, систем передачи извещений, технических средств аппаратуры СКУД и систем видеонаблюдения (СВН), использующих новейшие достижения микроэлектроники, радиотехники, акустики, оптики, приборостроения. Наиболее перспективное направление развития средств защиты от НСД – комплексирование технических средств защиты от несанкционированного доступа в интегрированные системы безопасности (ИСБ). Совершенствуется программное обеспечение таких программно-аппаратных комплексов. Кроме того,

модернизируется и нормативно-правовая база, регламентирующая вопросы монтажа, пусконаладочных работ и эксплуатационно-технического обслуживания технических средств охраны и безопасности для защиты территорий, объектов и помещений от НСД.

Широкое применение современных систем безопасности для защиты объектов от НСД требует и качественного повышения уровня подготовки кадров, способных профессионально и грамотно проектировать средства инженерно-технической защиты от НСД и организовывать проведение монтажных и пусконаладочных работ. Кроме того, уровень подготовки будущих специалистов в данной области должен быть достаточным для формирования у них профессиональных компетенций, необходимых для обеспечения должного проектирования, надзора за монтажными работами, эксплуатационно-технического обслуживания комплексов средств охраны и безопасности и оперативного устранения возникающих неполадок.

В предлагаемом учебном пособии даны классификация и характеристики технических средств инженерно-технического укрепления территорий и объектов, охранно-тревожной сигнализации (ОТС), систем контроля и управления доступом и систем видеонаблюдения (технических средств охранного телевидения).

В пособии рассмотрены основные требования организационно-распорядительных, методических документов и стандартов по организации обследования объектов для оснащения их техническими средствами охраны и безопасности, проектирования технических средств охранно-тревожной сигнализации, СКУД и СВН. Приведены практические решения и рекомендации по выбору технических средств охраны и безопасности для оборудования объектов.

Пособие предназначено для студентов и аспирантов, специализирующихся в вопросах комплексной защиты объектов информатизации, и может быть полезным в системе переподготовки и повышения квалификации инженерно-технических кадров. Для более углубленного изучения приводится рекомендательный библиографический список.

Глава 1. ОРГАНИЗАЦИЯ ОБСЛЕДОВАНИЯ ОБЪЕКТОВ ДЛЯ ОСНАЩЕНИЯ ИХ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ОХРАНЫ И БЕЗОПАСНОСТИ

1.1. Общие положения

Один из факторов, определяющих надежность защиты объектов, материальных и иных ценностей, которые находятся в отдельных зданиях, строениях, сооружениях, помещениях или на территории, – наличие на защищаемом объекте инженерных средств защиты на путях возможного проникновения нарушителей. Совокупность этих средств определяет техническую укрепленность защищаемого объекта. К инженерным средствам защиты относятся различные заборы, ограждения, решетки, жалюзи, ставни, замки, засовы, специальным образом укрепленные двери, ворота, стены, полы, потолки, оконные проемы, воздуховоды и другие элементы строительных конструкций. Такие средства кроме физического препятствия выполняют функции и психологического воздействия на потенциального нарушителя, заставляя его отказаться от попытки проникновения на объект.

Инженерные средства защиты увеличивают время, необходимое нарушителю для их преодоления, что делает более вероятной возможность его обнаружения и задержания, особенно если эти средства используются в сочетании с техническими средствами охраны (охранная сигнализация, системы охранного телевидения и т. п.).

Требования к технической укрепленности защищаемого объекта должны определяться значимостью объекта, видом и концентрацией материальных или иных ценностей на нем, его строительными и архитектурно-планировочными решениями, режимом работы и многими другими факторами, которые необходимо учитывать при проектировании комплексной системы защиты объекта.

Таким образом, техническая укрепленность объекта – это совокупность мероприятий, направленных на усиление конструктивных элементов зданий, сооружений, помещений и защищаемых территорий, обеспечивающих необходимое и достаточное противодействие несанкционированному проникновению нарушителя в защищаемую зону, взлому и другим преступным посягательствам. При несоответствии объектов требованиям охраны или недостаточной технической укрепленности строительных конструктивных элементов объекта эти

элементы или объект следует усиливать дополнительными техническими средствами (рубежами) охраны.

Требования к категорированию и инженерно-техническому укреплению объектов для недопущения несанкционированного проникновения на них являются ведомственными и определяются в основном значимостью объектов. Таких документов достаточно много. Наиболее полно вопросы технической укрепленности различных строительных конструкций, зданий, сооружений и периметров территорий объектов освещены в нормативно-технических документах Федерального государственного казенного учреждения «Управление вневедомственной охраны войск национальной гвардии РФ» (ФГКУ УВО (ОВО) ВНГ) [5].

Основные понятия и определения

Инженерно-технический состав – руководители и сотрудники (работники) инженерно-технических служб ФГКУ УВО (ОВО) ВНГ России по субъектам Российской Федерации или состав частной охранной организации, начальники пунктов централизованной охраны (ПЦО), дежурные ПЦО, инженерный состав, осуществляющие реализацию мероприятий по обеспечению охраны объектов и имущества с помощью технических средств.

Инженерно-техническое средство охраны (ИТСО) – конструктивно законченное, выполняющее самостоятельные функции устройство, которое входит в состав систем охранной и тревожной сигнализации, контроля и управления доступом, охранного телевидения, освещения, оповещения, инженерной укрепленности и других систем, предназначенных для охраны объекта.

Инженерно-техническая укрепленность объекта (ИТУ) – совокупность прочностных характеристик и свойств конструктивных элементов зданий, помещений и ограждения охраняемых территорий, обеспечивающих необходимое противодействие несанкционированному проникновению в охраняемую зону, взлому и другим преступным посягательствам.

Классификация охраняемого объекта – комплексная оценка состояния объекта, учитывающая его экономическую или иную (например, культурную) значимость в зависимости от характера и концентрации сосредоточенных ценностей, оценка последствий от

возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны.

Данные условия не распространяются на объекты государственной важности, а также объекты, подлежащие обязательной охране войсками национальной гвардии Российской Федерации в соответствии с перечнем, утвержденным распоряжением Правительства Российской Федерации от 15 мая 2017 г. № 928-р.

Места проживания и хранения имущества граждан (МПХИГ) – индивидуальные дома (коттеджи, таунхаусы, дачные дома), хозяйственные постройки, индивидуальные отдельно стоящие гаражи, индивидуальные боксы в гаражно-строительных кооперативах.

Криминальная угроза – совокупность условий и факторов, связанная с несанкционированным проникновением на охраняемый объект и/или совершением на его территории противоправных действий.

Канал системы передачи извещений – совокупность совместно действующих технических средств охраны и модулей и используемой(ых) сред(ы) передачи, осуществляющих обмен информацией между подсистемой(ами) объектовой(ыми) и подсистемой пультовой.

Место вероятного проникновения – это конструктивные элементы объекта (помещения), квартиры или МПХИГ (оконные проемы, входные двери, некапитальные стены и перекрытия, воздуховоды и вентиляционные короба), через которые наиболее вероятно несанкционированное проникновение.

Критические элементы объекта – потенциально опасные элементы (участки) объекта, совершение акта незаконного вмешательства в отношении которых приведет к прекращению нормального функционирования объекта, его повреждению или аварии на объекте.

Охраняемый объект – отдельное помещение или несколько помещений в одном здании, объединенные единым периметром, здания, строения, сооружения, прилегающие к ним территории и акватории, помещения, транспортные средства, а также грузы, денежные средства и иное имущество, подлежащее защите от противоправных посягательств.

Объект с массовым пребыванием граждан – здание или сооружение с одновременным пребыванием 50 и более человек (зри-

тельные, обеденные, выставочные, торговые, биржевые, спортивные, культовые и другие залы).

Помещения повышенного риска – это помещения (квартиры) первого, второго и последнего этажей здания, имеющие совмещенные балконы, а также окна (независимо от этажности), выходящие к пожарным лестницам, крышам разновысоких строений, козырькам, карнизам, деревьям, трубам.

Радиоканальная система передачи извещений (РСПИ) – система передачи извещений по радиочастотным каналам связи.

Пункт централизованной охраны (мониторинговый центр) – структурное подразделение организации, обеспечивающей круглосуточную централизованную охрану объектов с применением систем(ы) централизованного наблюдения в целях организации оперативного реагирования при поступлении информации о проникновении (попытке проникновения), а также о возникновении криминальных и технологических угроз.

Рубеж охранной сигнализации – совокупность зон обнаружения и средств инженерно-технической укрепленности, условно образующих границу, преодоление которой должно приводить к формированию извещения о тревоге.

Система передачи извещений (СПИ) – совокупность совместно действующих технических средств охраны, предназначенных для передачи по каналам связи и приема в ПЦО извещений о состоянии охраняемых объектов, служебных и контрольно-диагностических извещений, а также (при наличии обратного канала) для передачи и приема команд телеуправления.

Техническое средство охраны (ТСО) – конструктивно законченное устройство, выполняющее самостоятельные функции в составе системы, предназначенной для обеспечения охраны или безопасности объекта.

Централизованная охрана объекта – охрана территориально рассредоточенных объектов с помощью пунктов централизованной охраны.

Уязвимые места – критические элементы объекта, в отношении которых в силу их недостаточной защищенности или устойчивости могут быть спланированы и успешно реализованы несанкционированные действия, а также элементы системы физической защиты,

преодолевая которые нарушитель может успешно реализовать свои цели.

Задание на проектирование ТСО – обязательный для проведения проектирования документ, содержащий перечень требований к системе охранной сигнализации, условиям ее функционирования, целям и задачам и определяющий порядок работ по проектированию, инсталляции ТСО на объекте и последующей эксплуатации системы.

Взломостойкость – характеристика конструкции, обеспечивающая ее способность выполнять защитные функции и определяющая класс устойчивости к взлому.

Дополнительное ограждение – инженерно-строительная конструкция, применяемая для создания дополнительных затруднений (препятствий) нарушителю, проникающему на охраняемый объект.

Защитное ограждение – инженерное средство физической защиты, предназначенное для исключения случайного прохода людей, животных, въезда транспорта, препятствующее проникновению нарушителя на территорию охраняемого объекта.

Техническое обслуживание ТСО – комплекс организационно-технических мероприятий планово-предупредительного характера по поддержанию ТСО в состоянии, соответствующем требованиям технической документации на ТСО, в течение всего срока эксплуатации.

Зона отторжения – зона, непосредственно примыкающая к инженерным ограждениям охраняемого объекта и свободная от построек, деревьев, кустарника и тому подобного, для обеспечения нормальной работы извещателей, предназначенных для открытых площадок и периметров объектов.

Предупредительное ограждение – физическое препятствие, предназначенное для обозначения границ рубежа охраны и предотвращения появления в запретной зоне случайных посторонних лиц, животных и транспорта, вызывающих ложные срабатывания технических средств охраны.

Устойчивость к взлому – способность конструкции противостоять разрушающему воздействию, приводящему к утрате конструкцией заданных целевых физических свойств и функций назначения.

Ущерб от преступного посягательства – экономические, экологические или социальные последствия (убытки, потери) от преступного воздействия на охраняемый объект (МПХИГ).

Шлейф сигнализации – электрическая цепь, линия связи, предназначенные для передачи извещений на средство сбора и обработки информации.

Классификация объектов

Все защищаемые объекты в зависимости от их социальной значимости, наличия и концентрации культурных, исторических, материальных, информационных и других ценностей, возможных последствий от преступных посягательств на них подразделяют на следующие классы [5].

Объекты класса Б2 – государственные и коммерческие объекты, собственниками которых принято решение об установке системы тревожной сигнализации:

– служебные помещения охраны гаражно-строительных кооперативов (ГСК), автостоянок, помещения консьержей в подъездах жилых домов;

– объекты капитального строительства (строительные площадки);

– объекты, подходящие по своему функциональному назначению под категорию Б1, администрация которых направила заявку на оборудование объекта только системой тревожной сигнализации.

Объекты класса Б1 – объекты организаций различных форм собственности с сосредоточением материальных ценностей, преступные посягательства на которые могут привести к крупному или значительному ущербу для собственника имущества:

– объекты организаций различных форм собственности (в том числе расположенные в жилых домах и квартирах, выведенных из жилого фонда);

– объекты с хранением, размещением и реализацией товаров, предметов повседневного спроса, продуктов питания, табачной и алкогольной продукции;

– объекты ЖКХ (ТСЖ, управляющие компании);

– иные объекты потребительского рынка.

Объекты класса А3 – критически важные и потенциально опасные объекты, объекты, подлежащие обязательной охране поли-

цией в соответствии с перечнями, утверждаемыми Правительством Российской Федерации, особо важные объекты, объекты жизнеобеспечения, а также объекты с массовым пребыванием граждан, на которых охрана общественного порядка и материальных ценностей обеспечивается постами физической охраны и выводом тревожной сигнализации на ПЦО подразделений вневедомственной охраны:

– контрольно-пропускные пункты охраны (службы безопасности) объекта;

– служебные помещения и посты охраны (службы безопасности) объекта;

– иные служебные помещения внутри объекта;

– объекты образования, здравоохранения, культуры и спорта.

Объекты класса А2 – государственные и коммерческие объекты с оборотом денежных средств, драгоценных металлов, драгоценных камней, ювелирных изделий и иных материальных и культурных ценностей, преступные посягательства на которые могут иметь широкий международный и общественный резонанс и (или) привести к особо крупному (свыше 1 млн рублей) экономическому ущербу для государства или собственника имущества (не вошедшие в класс А1):

– обособленные помещения критически важных объектов, особо важных и потенциально опасных объектов инфраструктуры Российской Федерации, объектов, подлежащих обязательной охране в соответствии с перечнями, утвержденными Правительством Российской Федерации;

– ювелирные магазины, базы, склады и другие объекты, использующие в своей деятельности ювелирные изделия, драгоценные металлы и камни;

– объекты (комнаты) хранения оружия и боеприпасов, наркотических, сильнодействующих и психотропных веществ и препаратов;

– объекты кредитно-финансовой системы (банки, операционные кассы, дополнительные офисы, кассы самообслуживания, банкоматы);

– объекты (помещения) с обработкой сведений, составляющих персональные данные граждан;

– помещения для хранения наличных денежных средств (кассы) предприятий, организаций и учреждений;

– помещения с хранением документов строгой отчетности или спецпродукции;

– объекты с хранением и экспонированием оружия и боеприпасов, предметов старины, искусства и культуры;

– объекты отправления религиозного культа, представляющие историческую ценность.

Объекты класса А1 (наивысший) – специальные помещения особо важных объектов, объектов, подлежащих обязательной охране и определенных перечнями, утвержденными Правительством Российской Федерации:

– хранилища (склады) огнестрельного оружия, взрывчатых веществ, сильнодействующих, ядовитых, бактериологических, токсичных веществ;

– помещения с хранением сведений, составляющих государственную тайну;

– хранилища и кладовые (сейфовые комнаты) денежных и валютных средств, ценных бумаг объектов кредитно-финансовой системы;

– хранилища наркотических и психотропных веществ и препаратов;

– хранилища (сейфовые комнаты) ювелирных изделий, драгоценных металлов и камней;

– фондохранилища музеев, библиотек и других объектов культуры, являющихся историческими и архитектурными памятниками.

Классификация квартир

В зависимости от наличия и концентрации культурных, материальных, информационных и других ценностей, благосостояния собственника жилища на момент обследования, а также в зависимости от возможных последствий ущерба при реализации преступных посягательств квартиры делятся на следующие классы.

Квартиры класса В1 (наивысший) – квартиры антикваров, коллекционеров, деятелей науки, культуры и искусства, содержащих в своих квартирах предметы, художественная ценность которых не имеет денежного эквивалента (определяется экспертным путем).

Квартиры класса В2 – квартиры собственников, преступные посягательства на которые могут привести к особо крупному ущербу для собственника.

Квартиры класса В3 – квартиры собственников, преступные посягательства на которые могут привести к крупному или значительному ущербу для собственника.

Классификация МПХИГ

В зависимости от материального состояния (платежеспособности и благосостояния) собственника МПХИГ на момент проведения обследования, наличия и сосредоточения культурных, материальных и прочих ценностей и возможного материального ущерба от кражи МПХИГ делятся на следующие классы.

МПХИГ класса Г1 – частные дома, коттеджи, преступные посягательства на которые могут привести к особо крупному ущербу для собственника.

МПХИГ класса Г2 – частные дома, коттеджи, преступные посягательства на которые могут привести к крупному или значительному ущербу для собственника.

МПХИГ класса Г3 – индивидуальные гаражи (отдельно стоящие или в составе ГСК), индивидуальные постройки хозяйственного назначения (бани, хозблоки и т. д.).

1.2. Требования по инженерно-техническому укреплению ограждений территорий и элементов строительных конструкций объектов

Средства инженерно-технического укрепления (ИТУ) должны обеспечивать защиту от несанкционированного проникновения и иметь свой класс защиты, при этом особое внимание следует уделять направлениям, ведущим к критическим элементам объекта (территории), на труднопросматриваемых участках периметра и уязвимых местах объекта (территории).

Каждому классу объектов (МПХИГ), охраняемых или принимаемых под централизованную охрану, должен соответствовать класс защиты их конструктивных элементов в соответствии с нормативными и методическими актами Российской Федерации в сфере стандартизации и технического регулирования, а также организационно-

методическими документами Росгвардии, касающимися вопросов ИТУ [6].

Средства ИТУ предназначены:

– для защиты объекта (МПХИГ), людей путем создания физических преград для несанкционированных действий нарушителей;

– организации препятствия на пути движения нарушителей с главной задачей, состоящей в обеспечении временной задержки их продвижения к объектам защиты. Задержка должна предоставить время, достаточное для прибытия наряда физической охраны (группы задержания (ГЗ), группы быстрого реагирования (ГБР) и т. д.).

При организации и проведении первоначального обследования к следующим элементам строительных конструкций предъявляются требования по соответствию их классов защиты:

1) защитные элементы строительных конструкций ограждений территорий:

– защитные ограждения (постоянные и временные);

– ворота, калитки, двери и т. д.;

2) защитные элементы строительных конструкций зданий и сооружений:

– стеновые и потолочные конструкции кладовых, хранилищ, фондов, сейфовых комнат;

– наружные стены здания первого этажа, а также стены, перекрытия охраняемых помещений, расположенных внутри здания, примыкающие к помещениям других (неохраняемых) собственников;

– наружные стены охраняемых помещений, расположенных на втором этаже здания и выше, а также стены, перекрытия помещений, расположенных внутри здания, не примыкающие к помещениям других (неохраняемых) собственников;

– внутренние стены, перегородки в пределах каждой подгруппы, вентиляционные короба, вентиляционные каналы, водостоки и т. п.;

3) дверные конструкции:

– входные двери в здание, выходящие на оживленные улицы и магистрали;

– двери запасных выходов, двери, выходящие на крышу (чердак), во внутренние дворы;

– входные двери охраняемых помещений;

– внутренние двери в помещениях в пределах каждой подгруппы;

4) оконные строительные конструкции:

– окна первого, цокольного и подвального этажей, выходящие на оживленные улицы и магистрали;

– окна второго этажа и выше, не примыкающие к пожарным лестницам, балконам, карнизам, козырькам и т. п.;

– окна первого и подвального этажей, выходящие во внутренние дворы, малолюдные переулки;

– окна, примыкающие к пожарным лестницам, балконам, карнизам, козырькам и т. п.;

– оконные проемы помещений с постами охраны;

5) замки и запирающие устройства:

– запирающие устройства входных и запасных (эвакуационных) дверей в здание, входных дверей защищаемых помещений, дверей, выходящих на крышу или чердак;

– кодово-замочные или запирающие устройства внутренних дверей.

Уязвимые места возможного проникновения на объект могут быть дополнительно оснащены средствами охранного телевидения (видеонаблюдения), предназначенными для визуального обнаружения попыток несанкционированного проникновения.

Средства инженерно-технического укрепления должны удовлетворять следующим типовым требованиям:

– препятствовать свободному доступу и несанкционированному проникновению на охраняемый объект и/или охраняемую территорию;

– ограничивать использование нарушителем подручных средств, специального инструмента;

– создавать необходимые условия для выполнения задач по охране объекта со стороны службы безопасности объекта;

– не оказывать дестабилизирующего влияния на функционирование ТСО, применяемых на защищаемом объекте;

– обеспечивать заданную пропускную способность при санкционированном доступе и/или при необходимости экстренной эвакуации в чрезвычайной ситуации;

– обладать достаточной надежностью, устойчивостью к взлому, прочностью и долговечностью.

Выбор средств ИТУ для конкретного объекта (МПХИГ) определяется комиссионно по данным, полученным при комплексном обследовании. Средства ИТУ предназначены для усиления элементов строительных конструкций объектов (МПХИГ), обеспечивающих необходимую защиту от проникновения на охраняемую территорию или в зону внутри объекта, защиту от взлома или прочих криминальных посягательств путем создания физического заграждения несанкционированным действиям со стороны нарушителей. Ограждение территорий должно выполняться в виде преимущественно прямых участков с минимальным количеством изломов и поворотов, чтобы не создавать ограничений для проведения наблюдения и не затруднять использование периметральных ТСО. Защитное ограждение территорий должно исключать случайный проход (свободный доступ) людей и/или животных, въезд транспортных средств и не допускать возможности проникновения нарушителей на охраняемую территорию без прохождения контрольно-пропускных пунктов.

Ограждение не должно иметь проломов, проемов, лазов и каких-либо других повреждений, не оборудованных запорными устройствами дверей, ворот и калиток [6].

Ограждение 4-го класса защиты (специальная степень защиты объекта от проникновения) – основное ограждение, изготовленное из оцинкованного листа толщиной не менее 2 мм либо из жесткого металлического сетчатого полотна с диаметром вертикальных прутков 6 мм, сваренных в пересечениях и усиленных двойным горизонтальным прутком диаметром 8 мм, с ячейкой размерами не более 50×200 мм, оцинкованных и покрытых полимерным материалом. Ограждение устанавливается на ленточный железобетонный фундамент высотой над уровнем грунта не менее 0,5 м.

Ограждение 3-го класса защиты (высокая степень защиты объекта от проникновения) – основное ограждение, состоящее из просматриваемого секционного жесткого металлического сетчатого полотна, изготовленного из оцинкованного просечно-вытяжного листа толщиной не менее 2 мм или стальных прутков диаметром от 6 мм, сваренных в пересечениях и усиленных двойным горизонтальным прутком, с ячейкой размерами не более 50×200 мм, или ограждения с

диаметром прутков 5 мм, с ячейкой размерами 25×100 мм, оцинкованных и покрытых полимерным материалом. Основное ограждение может устанавливаться на ленточный железобетонный фундамент высотой над уровнем грунта не менее 0,5 м или на свайный фундамент. При установке на свайный фундамент основное ограждение должно оборудоваться дополнительным нижним ограждением. Основное ограждение должно иметь дополнительное верхнее и предупредительное ограждения. Для исключения прорыва на охраняемую территорию автотранспортных средств должны быть установлены противотаранные заграждения.

При необходимости (оговаривается в акте обследования, техническом задании на проектирование) в соответствии с архитектурно-конструктивными решениями данных территорий допускается в качестве основного ограждения использовать:

– железобетонное ограждение толщиной не менее 100 мм;

– каменное или кирпичное ограждение толщиной не менее 250 мм;

– сплошное металлическое ограждение с толщиной листа не менее 2 мм, усиленное ребрами жесткости, установленное на ленточный железобетонный фундамент высотой над уровнем грунта не менее 0,5 м, с заглублением в грунт не менее 0,5 м.

Ограждение 2-го класса защиты (средняя степень защиты объекта от проникновения) – основное ограждение, состоящее из просматриваемого секционного металлического сетчатого либо жесткого решетчатого полотна, изготовленного из стальных прутков диаметром от 6 мм, сваренных в пересечениях, с ячейкой размерами не более 50×200 мм, оцинкованных и покрытых полимерным материалом. Допускается использование деревянного сплошного ограждения толщиной не менее 40 мм.

Ограждение 1-го класса защиты (минимально необходимая степень защиты объекта от проникновения) – основное ограждение с просматриваемым гибким или жестким полотном, изготовленное из стальных прутков диаметром 4 – 5 мм, сваренных в пересечениях, с ячейкой размерами не более 50×200 мм, оцинкованных и покрытых полимерным материалом, либо из других различных конструктивных материалов.

Детальные вопросы применения различных видов ограждения отражены в ГОСТ Р 57278-2016 и методических рекомендациях [8]. Противотаранные и специальные виды ограждений территорий охраняемых объектов рассматриваются в документе [9].

Классификация ограждений в соответствии с классом обеспечиваемой защиты охраняемого объекта приведена в табл. 1.1.

Таблица 1.1

Классификация ограждений в соответствии с классом обеспечиваемой защиты охраняемого объекта

Класс ограждения	Вид используемого ограждения		
	Основное	Дополнительное	Предупредительное
I	+/–	–	–
II	+	Верхнее и/или нижнее	–
III	+	Верхнее и/или нижнее	Внутреннее
IV	+	Верхнее и/или нижнее	Внутреннее и наружное

Примечания. 1. Классификацию применяют для определения конфигурации системы ограждения охраняемого объекта (МПХИГ). Она не учитывает технические параметры и материал, из которого изготовлено ограждение. 2. Знак «+/–» показывает наличие или отсутствие вида ограждения.

В зависимости от класса объекта (МПХИГ) основное ограждение может оборудоваться дополнительным как верхним, так и нижним, а также предупредительным ограждением. При необходимости (прописывается в задании на проектирование или акте обследования) в соответствии с архитектурно-планировочными задачами для конкретной территории допускается в качестве основного ограждения использовать:

– монолитное железобетонное ограждение толщиной не менее 120 мм;

– каменное или кирпичное ограждение толщиной не менее 380 мм;

– вариант декоративного ограждения.

На въездах на территорию защищаемых объектов устанавливают ворота. Ворота устанавливаются также на стоянки автомобилей,

отдельно стоящие гаражи, боксы гаражно-строительных кооперативов, гаражи загородных домов. По периметру защищаемой территории объекта могут быть смонтированы как основные, так и запасные (аварийные, эвакуационные) ворота. Конструкция ворот должна предусматривать необходимую жесткую фиксацию створок в закрытом положении и обеспечивать:

– защиту объекта (МПХИГ) от НСД;

– санкционированное управление доступом персонала и транспорта на территорию или в защищаемую зону охраняемого объекта (МПХИГ);

– единое целое с функциональной принадлежностью и ландшафтно-архитектурными решениями объекта (МПХИГ).

Ворота с электроприводом и/или дистанционно управляемые должны оборудоваться устройствами аварийной остановки. Должна быть возможность открыть их вручную при неисправности или отключении электропитания.

Для предотвращения произвольного открывания или движения ворот их необходимо оснащать ограничителями, или стопорами. Запирающие и блокирующие устройства при закрытом состоянии ворот должны обеспечивать необходимую степень устойчивости к взлому и работоспособность при большой влажности в широком диапазоне температур (–40 °С … +50 °С), воздействии воды, снега, града, песка и других дестабилизирующих климатических факторов. При использовании замков в качестве запирающих устройств основных ворот следует устанавливать замки гаражного типа или висячие (навесные). Конструкция и крепление запирающих устройств и петель должны обеспечивать невозможность открытия или демонтажа изделий с наружной стороны. Редко открываемые ворота (запасные или аварийные) со стороны охраняемой территории должны запираться на засовы и висячие (навесные) замки. Калитку следует запирать на врезной (накладной) замок или на засов с висячим замком.

Элементы строительных конструкций зданий и помещений

Для зданий по конструкциям, соответствующим типовым панельным, блочным и кирпичным проектам, планировочные решения стандартные, с высокими прочностными характеристиками конструк-

тивных элементов зданий, таких как капитальные и армированные внешние стены, внутренние и межкомнатные стены, межэтажные перекрытия.

Здания монолитных и монолитно-кирпичных проектов в большинстве случаев имеют свободную планировку и низкие прочностные характеристики для внешних, внутренних межквартирных и/или межкомнатных стен (неармированные стены из легких бетонов, кирпичные стены малой толщины, внутренние перегородки из гипсо- или пеноблоков).

Для наружных и внутренних стен зданий, полов и потолков помещений объектов (МПХИГ) конструктивная прочность должна обеспечивать достаточное препятствие для проникновения нарушителей и иметь соответствующий класс защиты от взлома. Класс защиты достигается правильным выбором материалов строительных конструкций, соблюдением технологий их изготовления. Класс защиты элементов строительных конструкций должен соответствовать классу охраняемого объекта (МПХИГ) [6].

Строительные конструкции 4-го класса защиты (специальная степень защиты объектов от проникновения) – конструкции, соответствующие 5-му классу устойчивости к взлому и выше по ГОСТ [15].

Усиление стен должно производиться по всей площади с внутренней стороны помещения. Решетки приваривают к стальным анкерам диаметром не менее 12 мм, заглубленным в стену на 80 мм, к закладным деталям из стальной полосы размерами 100×50×6 мм, пристреливаемым четырьмя дюбелями, с шагом по вертикали и горизонтали не более 500 мм. После установки решетки должны быть замаскированы штукатуркой или облицовочными панелями.

Строительные конструкции 3-го класса защиты (высокая степень защиты объекта от проникновения):

– кирпичные стены толщиной более 380 мм;

– пустотные железобетонные плиты толщиной не менее 220 мм из тяжелых бетонов;

– сплошные железобетонные перекрытия толщиной не менее 120 мм из тяжелых бетонов;

– стеновые наружные панели, внутренние панели, блоки стеновые из легких бетонов толщиной более 300 мм;

– стеновые панели наружные, панели внутренние, блоки стеновые и стены из монолитного железобетона из тяжелых бетонов толщиной от 100 до 300 мм;

– строительные конструкции 1-го класса защиты, усиленные стальной решеткой, сваренной в пересечениях, из прутка диаметром не менее 10 мм и ячейкой размерами не более 150×150 мм;

– строительные конструкции 2-го класса защиты, усиленные стальной решеткой, сваренной в пересечениях, из прутка диаметром не менее 8 мм и ячейкой размерами не более 100×100 мм.

Строительные конструкции 2-го класса защиты (средняя степень защиты от проникновения):

– конструкции из бревен или бруса толщиной не менее 200 мм;

– кирпичные стены толщиной не менее 250 мм;

– стены из природного камня типа «ракушечник» марки М35 толщиной не менее 190 мм;

– пустотные железобетонные плиты толщиной не менее 220 мм из легких бетонов и толщиной не менее 160 мм из тяжелых бетонов;

– сплошные железобетонные перекрытия толщиной 120 и 160 мм из легких бетонов;

– стеновые наружные панели по ГОСТ 11024-2012, внутренние панели, блоки стеновые из легких бетонов толщиной от 100 до 300 мм;

– стены из монолитного железобетона, изготовленные из тяжелых бетонов, толщиной до 100 мм;

– строительные конструкции 1-го класса защиты, усиленные стальной решеткой, сваренной в пересечениях, из прутка диаметром не менее 8 мм и с ячейкой размерами не более 100×100 мм.

Строительные конструкции 1-го класса защиты (минимально необходимая степень защиты объекта от проникновения):

– гипсолитовые, гипсобетонные конструкции толщиной не менее 75 мм;

– щитовые деревянные конструкции толщиной не менее 75 мм;

– конструкции из бревен или бруса толщиной не менее 100 мм;

– каркасные перегородки толщиной не менее 20 мм с обшивкой металлическими, в том числе профилированными, листами толщиной не менее 0,55 мм;

– кирпичные перегородки толщиной не менее 138 мм;

– перегородки из легких теплоизоляционных бетонов толщиной не менее 300 мм;

– внутренние стеновые панели толщиной не менее 100 мм;

– пустотные железобетонные конструкции толщиной не менее 160 мм;

– перегородки из стеклопрофилита и стеклоблоков.

Технологические и вентиляционные каналы, шахты, короба, дымоходы и прочие отверстия, диаметр которых более 200 мм, если имеют выход за пределы охраняемых помещений, выход на крышу (чердак), в смежные помещения и своим сечением входят в помещения, где размещаются защищаемые ценности, должны быть оборудованы на входе в данные помещения металлическими решетками. Решетки выполняются из прутков арматурной стали диаметром не менее 16 мм с размерами ячейки не более чем 150×150 мм, сваренной в перекрестиях.

Решетки в вентиляционных коробах, шахтах, дымоходах со стороны охраняемых помещений должны отстоять от внутренней поверхности стены или перекрытия не более чем на 100 мм. Допускается для данных целей использовать фальшрешетки с ячейкой размерами 100×100 мм. Для объектов классов А1, А2 и Б1 в случае прохождения вентиляционных коробов и дымоходов диаметром более 200 мм в стенах помещений стены таких помещений с внутренней стороны должны укрепляться по всей граничащей с коробом (вентканалом) площади стальной решеткой с диаметром прутка не менее 8 мм и размерами ячейки не более чем 100×100 мм, сваренной в перекрестиях.

Монтаж решеток аналогичен монтажу решеток при усилении стен. Усиление стен вентиляционных шахт и воздуховодов на защищаемых объектах (МПХИГ) должно проводиться на этапе строительных или ремонтных работ. При обследовании объекта и определении мест вероятного проникновения, подлежащих блокированию, необходимо предусматривать оснащение данных строительных элементов ТСО с подключением на отдельные шлейфы ОТС или объектовые оконечные устройства систем передачи извещений (УОО СПИ), например извещателем раннего обнаружения поверхностным вибрационным (пьезоэлектрическим) на разрушение венткороба или извещателем пассивным инфракрасным на проникновение в охраняемое помещение из венткороба.

Двери разгрузочных люков по конструкции и прочности должны быть аналогичны ставням, запираться снаружи на навесные замки. Деревянная обвязка разгрузочного люка крепится к капитальным конструкциям стальными скобами с внутренней стороны или «ершами» из стали диаметром не менее 16 мм и встраивается в строительные конструкции на глубину не менее 150 мм. Двери и коробки чердачных люков должны закрываться с внутренней стороны и по прочности должны быть аналогичны входным наружным дверям.

Водопропуски сточных или проточных вод, подземные коллекторы (кабельные, канализационные) при диаметре труб или коллектора от 300 до 500 мм на выходе с защищаемой территории или объекта должны оборудоваться металлическими решетками.

Защитные решетки изготавливают из прутков арматурной стали диаметром не менее 16 мм, образующих ячейки размерами не более чем 150×150 мм, сваренных в перекрестиях. В трубах или коллекторах большого диаметра, если имеется возможность использования слесарного или другого инструмента взлома, устанавливаются решетки, заблокированные охранной сигнализацией на разрушение или открывание.

Воздушные трубопроводы, теплотрассы или каналы, пересекающие ограждения периметра защищаемой территории, по которым возможно проникновение нарушителя, оборудуются элементами дополнительного ограждения: козырьком из колючей проволоки или инженерным средством защиты типа «Спираль АКЛ». Последняя разворачивается сверху трубопровода или вокруг него. В случае наличия на защищаемых объектах (МПХИГ) неиспользуемых помещений, в том числе подвальных, граничащих с помещениями других организаций и собственников, а также арендуемых помещений необходимо в общих коридорах, проходных помещениях, на общих лестничных клетках и так далее устанавливать металлическую или решетчатую дверь с запирающими устройствами.

Дверные конструкции

Двери, дверные блоки и элементы конструкций для защиты дверных проемов зданий и помещений должны обеспечивать необходимую устойчивость к взлому, надежную защиту помещений объекта

(МПХИГ), обладать достаточным классом защиты к разрушающим воздействиям. Их конструкция должна обеспечивать безотказное открытие и закрытие в течение всего срока эксплуатации.

Выбор дверных блоков для помещений охраняемого объекта и их класс защиты должны определяться классом охраняемого объекта. По требованиям нормативных документов в области пожарной безопасности входные наружные двери должны открываться наружу. Их оснащают не менее чем двумя замочными устройствами с разнотипными механизмами секретности (сувальдный, цилиндровый), которые устанавливают на расстоянии не менее 300 мм друг от друга. Дверные блоки объектов (МПХИГ) должны быть исправны и хорошо подогнаны под дверную коробку и дверной проем.

Двустворчатые двери оборудуются двумя стопорными задвижками (шпингалетами) в верхней и нижней части двери. Сечение задвижки должно быть не менее 100 мм^2, глубина ответной части – не менее 30 мм. Для снижения вероятности совершения скоротечной кражи (на рывок) проем входной двери на объекте (МПХИГ) рекомендуется оборудовать дополнительной внутренней запирающейся дверью.

Дополнительная внутренняя дверь должна иметь более высокий класс защиты, чем внешняя дверь. Однако допускается менять местами классы защиты внешней и дополнительной входных дверей. При этом внешняя дверь в обязательном порядке подлежит блокировке средствами охранной сигнализации. Допускается оборудование внешней входной двери дополнительным электромагнитным замком скрытой установки. Дверные проемы в тамбурах центрального и запасного (эвакуационного) выходов на объект (МПХИГ) при отсутствии около них суточных постов физической охраны следует оснащать дополнительной запирающейся дверью, в качестве которой допускается использование решетчатой распашной или раздвижной двери. Дополнительные двери объектов классов А1 и А2 должны быть не ниже 2-го класса защиты, а классов А3, Б1 и Б2 – не ниже 1-го класса защиты. Допускается менять местами классы защиты основной входной двери и дополнительной.

При отсутствии технической возможности установки дополнительных дверей входные двери блокируются техническими средствами охранной сигнализации раннего обнаружения, которые обеспечи-

вают выдачу тревожного извещения при попытке подбора ключа или взлома замка. Дверные конструкции специальных помещений для хранения ценностей объектов класса А1 и А2 (комнаты хранения драгоценных металлов, камней и изделий из них, комнаты хранения оружия, помещения, в которых осуществляется деятельность, связанная с оборотом наркотических средств и психотропных веществ, прочие особо важные помещения, требующие дополнительных мер защиты) должны оснащаться дополнительной запирающейся металлической решетчатой распашной или раздвижной дверью. Класс защиты дополнительной решетчатой двери должен быть не ниже второго.

Для повышения охранных свойств дверных блоков и их безопасности в карте петли могут быть предусмотрены дополнительные противосъемные элементы. Для предотвращения снятия или отжатия дверного полотна рекомендуется использовать противосъемные штыри или противосъемный лабиринт. Для защиты от пролома или выбивания двери рекомендуется выполнять закрепление дверной коробки с помощью крепежных анкеров или других изделий по всему контуру дверного короба. Для повышения уровня устойчивости к взлому дверных конструкций допускается использование скрытых дверных петель.

Конструкция дверных петель должна предусматривать надежное крепление к створкам (полотнам) и дверным коробкам. Рекомендуется комплектовать дверные блоки устройствами закрывания (доводчиками), дверными глазками и т. д. Дверной глазок должен иметь угол обозрения не менее 180°, быть оснащен защитой от извлечения и обеспечивать возможность визуального наблюдения предметов в поле зрения на расстоянии от 0,5 до 5,0 м при условии средней освещенности. Допускается использовать дверные видеоглазки с выводом изображения на видеодомофон.

Для дверей эвакуационных и аварийных выходов в соответствии со строительной проектной документацией дверные блоки оснащаются устройствами экстренного открывания по ГОСТ 31471-2011 и/или другими устройствами, позволяющими обеспечить быструю эвакуацию людей из здания.

Для таких дверей устройство «Антипаника» должно предусматривать автоматическое возвращение в исходное положение «Закрыто» после выполнения цикла «открывание/закрывание». При приме-

нении сертифицированных дверей количество и класс кодово-замочных устройств указывается в соответствующей документации на дверь по ГОСТ Р 51072-2005. Выбор и применение дверных блоков более подробно изложены в документах [10; 11]. Требования к дверным конструкциям по классу защиты указаны в документе [6].

Дверные конструкции 4-го класса защиты (специальная степень защиты объекта от проникновения):

– двери, соответствующие классу устойчивости к взлому III по ГОСТ Р 51072-2005;

– двери класса защиты III по ГОСТ 51072-2005 с пулестойким стеклом (бронестеклом) по ГОСТ Р 30826-2014.

Дверные конструкции 3-го класса защиты (высокая степень защиты объекта от проникновения):

– двери, соответствующие классу устойчивости к взлому II по ГОСТ Р 51072-2005;

– двери класса защиты от взлома II по ГОСТ Р 51072-2005 с защитным остеклением из взломостойкого стекла не ниже класса Р6В по ГОСТ Р 30826-2014.

Дверные конструкции 2-го класса защиты (средняя степень защиты объекта от проникновения):

– двери, соответствующие классу устойчивости к взлому I по ГОСТ Р 51072-2005;

– двери класса защиты I по ГОСТ Р 51072-2005 с защитным остеклением из ударостойкого стекла класса Р3А по ГОСТ Р 30826-2014;

– решетчатые металлические двери, изготовленные из стального прутка диаметром не менее 16 мм, сваренного в пересечениях, с ячейкой размерами не более 160×160 мм;

– решетчатые раздвижные металлические двери, изготовленные из полосы сечением не менее 30×4 мм, с ячейкой размерами не более 150×150 мм.

Дверные конструкции 1-го класса защиты (минимально необходимая степень защиты объекта от проникновения):

– двери деревянные внутренние со сплошным или мелкопустотным заполнением полотен по ГОСТ 475-2016; толщина полотна менее 40 мм;

– двери деревянные со стеклянными фрагментами из листового стекла марок М4 – М8 по ГОСТ 111-2014, армированного по ГОСТ 7481-2013, узорчатого по ГОСТ 5533-2013, тонированного по ОСТ 3-1901-95, ударостойкого класса Р2А по ГОСТ Р 30826-2014; толщина стекла фрагмента не нормируется;

– двери с полотнами из стекла в металлических рамах или без них: стекло обычное марок М4 – М8 по ГОСТ 111-2014, закаленное по ГОСТ 32565-2013, армированное по ГОСТ 7481-2013, узорчатое по ГОСТ 5533-2013, трехслойное («триплекс») по ГОСТ 32565-2013 или ударостойкое класса Р2А по ГОСТ Р 30826-2014;

– решетчатые металлические двери произвольной конструкции, изготовленные из стального прутка диаметром не менее 7 мм, сваренного в пересечениях, с ячейкой размерами не более 50×250 мм.

Оконные конструкции

Оконные конструкции, в том числе оконные блоки, стеклопакеты, форточки, фрамуги, мансардные окна, витрины и так далее в помещениях охраняемого объекта (МПХИГ) должны быть полностью остеклены, а также иметь надежные и исправные запирающие устройства. Стекла оконных блоков должны быть надежно закреплены в рамах, а рамы должны быть надежно закреплены в оконных проемах.

Оконные конструкции должны обеспечивать надежную защиту помещений объекта (МПХИГ) и обладать достаточным классом защиты к разрушающим воздействиям. Выбор материалов для изготовления оконных конструкций и их класс защиты определяются классом охраняемого объекта (МПХИГ) [6]. Оконные проемы специальных и особо важных помещений, в том числе, например, касс предприятий, сейфовых и оружейных комнат, других специальных помещений, требующих повышенных мер защиты, независимо от этажности в обязательном порядке должны быть оборудованы защитными конструкциями или защитным остеклением соответствующего класса по ГОСТ [23]. При проектировании новых зданий и сооружений на 1-м и 2-м этажах рекомендуется устанавливать стеклопакеты с нанесенной защитной пленкой классом устойчивости к взлому в соответствии с классом охраняемого объекта. Ударостойкое защитное остекление класса Р1А, Р2А по ГОСТ 30826-2014 устанавливается на объ-

ектах, не имеющих значительных защищаемых ценностей и находящихся под централизованной или внутренней физической охраной. При круглосуточном нахождении в витринах, окнах или около них защищаемых ценностей требуемый класс устойчивости к взлому защитного остекления повышается.

Ударостойкое защитное остекление класса Р3А, Р4А по ГОСТ 30826-2014 рекомендуется устанавливать:

– на объектах, имеющих материальные ценности высокой потребительской стоимости, исторические и культурные ценности и находящихся под централизованной или внутренней физической охраной;

– в операционных залах банков, помещениях органов управления и власти (если не требуется установка пулестойкого остекления), торговых залах ювелирных, оружейных магазинов, аптек (при условии отсутствия в них во внерабочее время драгоценных металлов, оружия, наркотиков);

– музеях, картинных галереях (в виде экранов, витрин для защиты отдельных экспонатов в экспозиционных залах);

– квартирах класса В2, В3 и МХИГ класса Г2, расположенных на промежуточных этажах здания;

– квартирах класса В1 для защиты отдельных предметов.

Взломостойкое защитное остекление класса Р6В по ГОСТ 30826-2014 рекомендуется устанавливать:

– на объектах, не имеющих значительных материальных ценностей, при отсутствии централизованной или постоянной физической охраны;

– в складских помещениях независимо от вида охраны;

– хранилищах, депозитариях музеев, находящихся под централизованной или внутренней физической охраной;

– на окнах, выходящих к пожарным лестницам, крышам разновысоких строений, козырькам, карнизам, деревьям, трубам;

– в квартирах первого, второго и последнего этажей здания, имеющих совмещенные балконы, а также окна (независимо от этажности);

– квартирах и МХИГ всех классов вне зависимости от этажности расположения.

Взломостойкое защитное остекление класса Р7В, Р8В по ГОСТ 30826-2014 рекомендуется устанавливать:

– в торговых залах ювелирных, оружейных магазинов, аптек (при наличии в них во внерабочее время драгоценных металлов, оружия, наркотиков), кассах;

– хранилищах, депозитариях музеев, не имеющих централизованной или внутренней физической охраны;

– на объектах, имеющих материальные ценности высокой потребительской стоимости, при отсутствии централизованной или внутренней физической охраны;

– во внутренних помещениях банков (если не требуется установка пулестойкого остекления);

– в квартирах класса В1, расположенных на первом, втором и последнем этажах здания, имеющих совмещенные балконы, а также окна (независимо от этажности), выходящие к пожарным лестницам, крышам разновысоких строений, козырькам, карнизам, деревьям, трубам.

Пулестойкое защитное остекление должно устанавливаться на охраняемых объектах любого класса и МПХИГ любого класса при возможной угрозе вооруженного нападения на людей.

Оконные проемы первого, второго и последнего этажей здания, совмещенных балконов, а также окна (независимо от этажности), выходящие к пожарным лестницам, крышам разновысоких строений, козырькам, карнизам, деревьям, трубам теплотрасс и тому подобному, рекомендуется оборудовать механическими защитными конструкциями, например «Спираль АКЛ».

При оборудовании оконных конструкций металлическими решетками их следует устанавливать с внутренней стороны помещения и делать распашными или раздвижными. В отдельных случаях допускается по согласованию с охранной организацией установка решеток с наружной стороны при их обязательной блокировке средствами охранной сигнализации.

Если в защищаемом помещении все оконные проемы оснащаются решетками, как минимум одна из них делается открывающейся (распашной или раздвижной). Раздвижные или распашные решетки должны запираться с внутренней стороны на замок соответствующего класса защиты или на иное запорное устройство, обеспечивающее

надежное запирание решетки и эвакуацию людей из помещения в экстремальных ситуациях. Ключи от замков должны храниться в специальных ящиках в комнате охраны, в недоступном для общего доступа месте.

Для больших помещений с количеством окон более пяти или большой площадью непрерывного остекления, например витрины, количество открывающихся решеток определяется условиями обеспечения необходимого времени для эвакуации людей. Если несколько помещений на объекте имеют по одному оконному проему, то для обеспечения эвакуации людей из помещения каждый оконный проем оборудуется открывающимися распашными или раздвижными решетками.

Оконные проемы первых этажей объектов и МПХИГ с длительным или сезонным отсутствием собственников следует защищать специальными щитами или ставнями не ниже 2-го класса защиты по методическим рекомендациям [6]. При монтаже щитов и ставен с внешней стороны окна они должны запираться на засовы и навесные замки. При большой высоте окон (более 1,5 м) щиты и ставни запираются на два засова и два замка. При установке данных конструкций с внутренней стороны окон щиты и ставни запираются только на засовы. Допускается для защиты оконных проемов использовать решетки, рольставни и жалюзи, которые по прочности и устойчивости к взлому не уступают щитам и ставням. При установке рольставен и жалюзи снаружи остекленных проемов они блокируются техническими средствами охранной сигнализации на открытие и отрыв от стены.

Более подробно информация по устойчивости к взлому различных видов оконных блоков, жалюзи и оконных решеток приведена в методических рекомендациях [7]. Технические требования к защитному остеклению различного типа приведены в документах [16; 17; 18; 21; 23; 24].

Оконные конструкции 4-го класса защиты (специальная степень защиты объекта от проникновения):

– окна с обычным стеклом, дополнительно усиленные защитными конструкциями, соответствующими категории и классу устойчивости С-II и выше по ГОСТ Р 51242-98;

– окна специальной конструкции с защитным остеклением класса Р6В и выше по ГОСТ Р 30826-2014;

– окна с пулестойким стеклом (бронестекло) по ГОСТ Р 30826-2014;

– остекление кабин защитных по ГОСТ Р 50941-2017.

Оконные конструкции 3-го класса защиты (высокая степень защиты объекта от проникновения):

– окна специальной конструкции с защитным остеклением класса Р3А, Р4А, Р6В и выше по ГОСТ Р 30826-2014 или стекла, оклеенные защитной пленкой, обеспечивающей класс устойчивости остекления Р3А, Р4А, Р6В и выше по ГОСТ Р 30826-2014;

– окна с обычным стеклом, дополнительно защищенные:

– щитами или деревянными ставнями со сплошным заполнением полотен при их толщине не менее 40 мм, обитыми с двух сторон стальными листами толщиной не менее 0,6 мм;

– металлическими решетками, изготовленными из стальных прутьев диаметром не менее 16 мм, образующих ячейки размерами не более 150×150 мм, или другими конструкциями соответствующей прочности.

Оконные конструкции 2-го класса защиты (средняя степень защиты объекта от проникновения):

– окна специальной конструкции с защитным остеклением класса Р3А и выше по ГОСТ Р 30826-2014 или из обычного стекла, оклеенного защитной пленкой, обеспечивающей класс устойчивости остекления Р3А и выше по ГОСТ Р 30826-2014;

– окна с обычным стеклом, дополнительно оснащенные защитными конструкциями, соответствующими категории и классу устойчивости О-II и выше по ГОСТ Р 51242-98:

– деревянными ставнями со сплошным заполнением полотен при их толщине не менее 40 мм;

– щитами или деревянными ставнями из досок или фанеры толщиной 12 мм, обитыми стальными листами толщиной не менее 0,3 мм;

– металлическими решетками произвольной конструкции из прутков диаметром не менее 6 мм, сваренных в пересечениях и образующих ячейки размерами не более 150×150 мм.

Оконные конструкции 1-го класса защиты (минимально необходимая степень защиты объекта от проникновения):

– окна с обычным стеклом (стекло марки М4 – М8 по ГОСТ 111-2014 толщиной от 2,5 до 8 мм);

– окна с обычным стеклом, дополнительно оклеенным защитной пленкой, обеспечивающей класс устойчивости остекления Р2А по ГОСТ Р 30826-2014.

Запирающие устройства

Для обеспечения надежного функционирования всех открывающихся элементов строительных конструкций, в том числе дверей, ворот, люков, ставень, жалюзи и тому подобного, требуется установка на них соответствующих по классу защиты запирающих кодово-замочных устройств. Выбор запирающих устройств и оценка их устойчивости к взлому осуществляется в соответствии с классом охраняемого объекта (МПХИГ).

Способы установки и крепления кодово-замочных изделий не должны нарушать герметичности элементов строительных конструкций. Закрепление запирающих устройств должно исключать возможность их демонтажа с наружной стороны. Для усиления замочных устройств обычно используют защитные пластины. При наличии самоимпрессионного (или самонаборного) ключа среднее время вскрытия классического сувальдного механизма составляет 1 – 2 минуты. Движения при вскрытии при этом настолько примитивны, что вскрыть сувальдный замок этим инструментом может буквально каждый школьник. Для защиты от самоимпрессии замочных устройств применяют специальные накладки (втулка, вмонтированная в замок), закрывающие скважину замка. Для защиты от химических веществ рекомендуется применять накладки, которые перекрывают доступ к механизму замка.

К замкам, применяемым на противопожарных дверях, предъявляются особые требования: они должны изготавливаться из стали и не содержать в своей конструкции легкоплавких материалов. Замочные устройства могут дополнительно комплектоваться защитными накладками, цепочками, а также кодовыми, электромеханическими, магнитными и другими устройствами для повышения охранных свойств. Навесные замки применяют для запирания ворот, чердачных и под-

вальных дверей, решеток, ставен и других конструкций. Данные замки должны иметь защитные пластины и кожухи.

Проушины для навесных замков изготавливают из стальной полосы сечением не менее 6×40 мм. Цилиндровая часть врезного замка после установки предохранительной накладки, розетки, щитка не должна выступать более чем на 2 мм. Ключи от замков на оконных решетках и дверях запасных выходов размещаются в специально выделенном помещении (обычно в комнате охраны) в ящиках, шкафах или нишах, исключающих свободный доступ к ним посторонних лиц.

Для обеспечения защищенности материальных ценностей могут применяться электромеханические запорные устройства совместно с электронными устройствами управления и контроля доступом, которые могут быть интегрированы в общую систему безопасности объекта и имеют автоматическую блокировку или разблокировку.

Для таких типов замочных устройств дополнительный электромеханический блокирующий механизм должен разблокироваться при отключении электропитания или нажатии на кнопку экстренного отпирания, а также должна быть возможность ручного открытия дверного полотна. Более подробно требования к кодово-замочным устройствам изложены в обзорах методических документов Росгвардии и в методических рекомендациях [6].

Запирающие устройства 4-го класса защиты (очень высокая или специальная степень защиты объекта от проникновения) – замки, соответствующие 4-му классу по ГОСТ 5089-2011 и классу устойчивости U4 по ГОСТ Р 52582-2006, и сейфовые замки по ГОСТ 34024-2016.

Запирающие устройства 3-го класса защиты (высокая степень защиты объекта от проникновения) – замки, соответствующие 3-му классу по ГОСТ 5089-2011 и классу устойчивости U3 по ГОСТ Р 52582-2006.

Запирающие устройства 2-го класса защиты (средняя степень защиты объекта от проникновения) – замки, соответствующие 2-му классу по ГОСТ 5089-2011 и классу устойчивости U2 по ГОСТ Р 52582-2006.

Запирающие устройства 1-го класса защиты (минимально необходимая степень защиты объекта от проникновения) – замки, соответствующие 1-му классу по ГОСТ 5089-2011 и классу устойчивости U1 по ГОСТ Р 52582-2006.

Требования к классу защиты средств ИТУ объекта и МПХИГ

Каждому классу объектов (МПХИГ) должен соответствовать определенный класс защиты конструктивных элементов (средств ИТУ) (табл. 1.2 и 1.3).

Таблица 1.2

Требования к классу защиты средств ИТУ объектов

Конструктивный элемент	Класс объекта				
	А1	А2	А3	Б1	Б2
	Класс защиты				
Защитные конструкции					
Ограждения	–	3 (4*)	2 (3*)	1 (2*)	1 (2*)
Ворота	–	3 (4*)	2 (3*)	1 (2*)	1 (2*)
Строительные конструкции					
Оболочка кладовой, хранилища	4	–	–	–	–
Наружные стены первого этажа здания, а также стены, перекрытия охраняемых помещений, расположенных внутри здания, примыкающие к помещениям других собственников	–	3	–	2	–
Наружные стены охраняемых помещений, расположенных на втором этаже здания и выше, а также стены, перекрытия этих помещений, расположенных внутри здания, не примыкающие к помещениям других собственников	–	2	–	1	–
Внутренние стены, перегородки в пределах каждой подгруппы	1	1	–	1	–
Дверные конструкции					
Входные двери в здание, выходящие на оживленные улицы и магистрали	–	3	–	2	–
Двери запасных выходов, двери, выходящие на крышу (чердак), во дворы, малолюдные переулки	–	3	–	3	–
Входные двери охраняемых помещений	4	3	–	2	–
Внутренние двери в помещениях в пределах каждой подгруппы	1	1	–	1	–
Оконные конструкции					
Оконные проемы первого и подвального этажей, выходящие на оживленные улицы и магистрали	–	3	–	2	–

Окончание таблицы 1.2

Конструктивный элемент	Класс объекта				
	А1	А2	А3	Б1	Б2
	Класс защиты				
Оконные проемы второго этажа и выше, не примыкающие к пожарным лестницам, балконам, карнизам и т. п.	–	2	–	1	–
Оконные проемы первого и подвального этажей, выходящие во дворы, малолюдные переулки	–	3	–	3	–
Оконные проемы, примыкающие к пожарным лестницам, балконам, карнизам и т. п.	–	3	–	3	–
Оконные проемы помещений охраны	–	3 (4*)	2	2	1
Запирающие устройства					
Запирающие устройства входных и запасных дверей здания, входных дверей охраняемых помещений, дверей, выходящих на крышу (чердак)	4	3	3	2 (3*)	–
Запирающие устройства внутренних дверей	1	1	1	1	–

* По заданию на проектирование.

Таблица 1.3

Требования к классу защиты средств ИТУ МПХИГ

Конструктивный элемент	Класс квартиры			Класс МПХИГ		
	В1	В2	В3	Г1	Г2	Г3
	Класс защиты					
Защитные конструкции						
Ворота	–	–	–	2	2	2
Строительные конструкции						
Наружные стены здания, а также стены, перекрытия помещений, расположенных внутри здания, примыкающие к помещениям других собственников	3	3	3	2 (3)	2	1 (2)
Стены помещений, расположенных внутри здания, не примыкающие к помещениям других собственников	2	2	2	1	1	1
Дверные конструкции						
Основные входные и дополнительные двери в квартиру или МПХИГ	3	2	1 (2)	2 (3)	2 (3)	1 (2)

Окончание таблицы 1.3

Конструктивный элемент	Класс квартиры			Класс МПХИГ		
	В1	В2	В3	Г1	Г2	Г3
	Класс защиты					
Дополнительные (внутренние) входные двери	1 (2)	–	–	–	–	–
Оконные конструкции						
Оконные проемы подвальных, первых, вторых и последних этажей, а также оконные проемы, примыкающие к пожарным лестницам, балконам, карнизам	3	2 (3)	2 (3)	2 (3)	2 (3)	1 (2)
Оконные проемы третьего этажа и выше, не примыкающие к пожарным лестницам, балконам, карнизам	2	2	2	1 (2)	1 (2)	–

1.3. Требования по инженерно-техническому укреплению специальных помещений

Кассовый узел, операционные кассы кредитных организаций

Типовые требования по инженерно-техническому укреплению специальных помещений изложены согласно рекомендациям [6].

Кассовый узел, операционные кассы кредитных организаций оборудуются в соответствии с требованиями нормативных документов Центрального Банка Российской Федерации, в том числе ВНП 001-01-2009 «Проектирование зданий банков». Помещение кассы должно иметь: один вход/выход; специальное окно с дверцей для выдачи денег; сейф (или металлический шкаф) для хранения денежной наличности и других ценностей.

Размеры специальных окон для банковских операций с клиентами должны быть не более 200×300 мм. Окно может быть в наружной двери или стене, а также в кассовом барьере. Если размеры окна превышают 200×300 мм, то снаружи его укрепляют металлической решеткой или иными защитными конструкциями. Допускается использование специализированных и сертифицированных бронелотков.

Дверца для специального окна должна соответствовать классу защиты всей конструкции, в которую она установлена. Закрываться дверца должна с внутренней стороны на замок и задвижку (шпингалет). Специальное окно может быть выполнено в виде передаточного узла или бро-

нелотка по ГОСТ Р 50941-2017. Хранение денежной наличности и других ценностей осуществляется в специализированных сейфах, соответствующих требованиям ГОСТ Р 50862-2017. При отсутствии сейфов, имеющих сертификаты соответствия, допускается хранить денежную наличность, а также другие ценности в металлических шкафах в пределах разрешенных лимитов хранения. В этом случае шкафы или подходы к ним должны быть защищены средствами охранной сигнализации.

Хранить особо ценные и особо важные ценности, в первую очередь материальные, следует в специально предназначенных для этих целей хранилищах (кладовых), а также сейфовых комнатах.

Банкоматы и другие устройства самообслуживания

Организация противокриминальной защиты банкоматов, платежных терминалов и иных устройств самообслуживания (УС) осуществляется комплексно, с использованием средств ИТУ, ТСО, СКУД, СОТ и других средств защиты.

Независимо от типа банкомата и/или устройств самообслуживания у них выделяют две зоны: зону самообслуживания (специально выделенное помещение для доступа клиентов к УС либо территория непосредственно перед банкоматом); сервисную зону (помещение, где осуществляется загрузка/выгрузка кассет с денежной наличностью инкассаторами, а также техническое обслуживание данных устройств).

Сервисной зоной банкомата может быть как специально выделенное внутреннее помещение, так и используемое для этих целей специальное служебное помещение. Банкоматы и другие устройства самообслуживания по месту установки подразделяются:

– на офисные: свободная установка внутри помещения без выделения выгораживаемой сервисной зоны и зоны самообслуживания. Существуют модели банкоматов, в которых загрузка и техническое обслуживание могут производиться с передней и задней сторон корпуса банкомата;

– вестибюльно-офисные: установка через стену внутри помещения. Доступ клиентов к УС возможен только из внутренних помещений организации. При этом загрузка денежных средств и техническое обслуживание банкомата могут производиться только сзади;

– вестибюльно-уличные: установка через наружную стену фронтальной частью в вестибюль (тамбур), имеющий выход на улицу. До-

ступ клиентов к УС осуществляется без непосредственного входа в организацию;

– уличные: установка через наружную стену фронтальной частью на улицу без выделения выгораживаемой зоны самообслуживания. При этом загрузка денежных средств и техническое обслуживание банкомата могут производиться только сзади.

Инженерно-техническое укрепление зоны самообслуживания вестибюльно-уличных и уличных банкоматов, которые для клиентов работают в режиме круглосуточного обслуживания, следующее. Помещение для зоны самообслуживания вестибюльно-уличных УС выбирается из условия удобства клиентов и конфиденциальности проводимых операций. В качестве таких помещений могут быть: тамбур основного входа в здание; вестибюль здания; отдельное помещение с выходом на фасадную сторону здания.

Остекленные конструкции зоны самообслуживания, выходящие наружу, а также двери для клиентов должны быть выполнены из защитного остекления класса защиты не ниже Р3А по ГОСТ [23] в металлических переплетах или остекления из обычного стекла, но оклеенного с внутренней стороны защитной пленкой класса защиты не ниже Р3А по ГОСТ [23]. Внутренние двери, ограждающие конструкции и перегородки зоны самообслуживания, смежные со служебными помещениями, должны быть не ниже III класса устойчивости к взлому по ГОСТ Р 51113-97.

Лицевые панели банкоматов должны иметь защиту от воздействия внешних климатических условий и при необходимости от механических воздействий (вандалозащищенное исполнение). Для достижения эффективной работы охранного телевидения в местах размещения банкоматов уровень освещенности зоны самообслуживания должен составлять не менее 200 лк. В зоне самообслуживания вестибюльно-уличных УС не допускается установка банкоматов офисного типа.

Инженерно-техническое укрепление сервисной зоны следующее. Для вестибюльно-уличных УС необходимо специально выделенное помещение сервисной зоны. Стена, в которую встраивается фронтальная часть УС, должна быть не ниже III класса устойчивости к взлому по ГОСТ Р 51113-97. Ограждающие конструкции сервисной зоны, а также внутренние стены должны быть не ниже II класса устойчивости к взлому по ГОСТ Р 51113-97. Двери в сервисную зону

должны иметь класс защиты от взлома не ниже III, быть оборудованы внутренним замком, металлической задвижкой изнутри и смотровым глазком.

Требования к площади помещений для размещения сервисной зоны определяются заказчиками и фирмами-производителями для обслуживания каждого типа УС. Общие требования к инженерно-техническому укреплению помещений и банкоматов приведены в табл. 1.4.

Таблица 1.4

Общие требования ИТУ помещений и банкоматов

Тип УС / Требования	Офисный	Вестибюльно-офисный	Вестибюльно-уличный	Уличный
Крепление УС или сейфа банкомата к капитальным конструкциям (пол, стена) или основанию	+	+	+	+
ИТУ остекления зоны самообслуживания (ГОСТ Р 30826-2014)	–	–	А2	–
ИТУ стены, в которую встраивается УС	–	3-й класс	3-й класс	3-й класс
ИТУ внутренних стен сервисной зоны	–	2-й/3-й класс	2-й/3-й класс	2-й/3-й класс

Более подробно требования по инженерно-техническому укреплению банкоматов и банковских устройств самообслуживания изложены в рекомендациях [39].

Хранилище ценностей (сейфовая комната)

Хранилище ценностей (сейфовая комната) должно иметь конструкторское и технологическое исполнение для эффективной защиты от НСД через железобетонную оболочку (стены, пол, потолок), а также через дверь с использованием любого ручного электрифицированного инструмента, домкратов, газорежущего оборудования, отмычек, взрывчатки и иных орудий взлома. Хранилище ценностей (сейфовая комната) должно быть сертифицировано и иметь класс устойчивости к взлому не ниже пятого согласно ГОСТ [25]. Выбор необходимого класса устойчивости хранилища определяется собственником.

Стены ограждения хранилища ценностей должны иметь класс защиты не ниже третьего. Допускается, чтобы внутренние и наружные стены здания, имеющие 3-й класс защиты, были одновременно и стенами ограждения хранилища. В случае если стены ограждения хранилища, расположенного на первом или втором этаже здания, являются наружными стенами, то между ними и оболочкой хранилища предусматривается смотровой коридор шириной не менее 0,6 м.

Смотровые коридоры предполагаются также и при расположении хранилища на верхних этажах и в подвалах, если на примыкающей к нему наружной стене имеются балконы, карнизы и другие сооружения, позволяющие вести скрытые работы по разрушению наружных стен.

Если стены ограждения хранилища – внутренние стены в здании, за которыми размещаются помещения охраняемого объекта, оборудованные охранной сигнализацией, смотровой коридор между стенами ограждения и оболочкой допускается не создавать. Вход в смотровой коридор осуществляется из предкладовой и должен защищаться решетчатой дверью с запорными устройствами. Если над хранилищем имеется чердачное помещение, кровля, технические помещения или помещения, принадлежащие другой организации, между оболочкой хранилища и плитой перекрытия должен быть зазор (смотровой просвет) размером не менее 250 мм, открытый со стороны предкладовой и смотрового коридора.

Вход в хранилище осуществляется из предкладовой через бронедверь. В качестве запасного аварийного входа в хранилище при необходимости следует предусматривать люк размерами не менее 500×650 мм или диаметром не менее 700 мм. Люк в оболочке хранилища рекомендуется размещать на расстоянии не менее 1 м от бронедвери. Вход в хранилище через люк должен осуществляться из предкладовой. Класс устойчивости бронедвери, аварийного люка, количество и класс замковых устройств должны соответствовать классу устойчивости оболочки хранилища. Окна в хранилище, предкладовой и смотровых коридорах не допускаются.

На объектах, где строительство хранилища невозможно, в качестве хранилища ценностей может быть оборудована сейфовая комната для хранения ценностей в сейфах.

Вход в помещение сейфовой комнаты должен быть один. Смотровые коридоры для сейфовых комнат не предусматриваются. Хранение ценностей должно осуществляться в сейфах, отвечающих требованиям ГОСТ [25]. Сейфы массой менее 1000 кг должны крепиться с помощью анкерного крепления к полу и стене либо встраиваться в стену.

Помещения для хранения гражданского и служебного оружия, боеприпасов и взрывчатых веществ

Помещения для хранения гражданского и служебного оружия, боеприпасов и взрывчатых веществ оборудуются в соответствии с требованиями постановления Правительства РФ от 21.07.1998 г. № 814 «О мерах по регулированию оборота гражданского и служебного оружия и патронов к нему на территории Российской Федерации», приказа МВД России от 12.04.1999 г. № 288 «О мерах по реализации постановления Правительства Российской Федерации от 21 июля 1998 г. № 814».

Объекты и помещения, в которых осуществляется деятельность, связанная с оборотом наркотических и психотропных веществ

Объекты и помещения, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список I перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, прекурсоров, и/или культивирование наркосодержащих растений, оборудуются в соответствии с требованиями постановления Правительства РФ от 17.12.2010 г. № 1035 «О порядке установления требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и их прекурсоров, и (или) культивирование наркосодержащих растений», а также в соответствии с требованиями постановления Правительства РФ от 31.12.2009 г. № 1148 «О порядке хранения наркотических средств, психотропных веществ и их прекурсоров» и приказа Федеральной службы войск национальной гвардии РФ и МВД РФ от 09.01.2018 г. № 1/5 «Об утверждении Требований к

оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список I перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, прекурсоров, и/или культивирование наркосодержащих растений для использования в научных, учебных целях и в экспертной деятельности».

1.4. Обследование объектов для оснащения их средствами охранно-тревожной сигнализации, системой контроля и управления доступом и системой видеонаблюдения

Обследование объектов для оснащения их средствами охранно-тревожной сигнализации, системой контроля и управления доступом и системой видеонаблюдения для приема под централизованную охрану имущества физических и/или юридических лиц проводится без взимания платы на основании заявления (письма), направленного (в том числе и в электронном виде) в подразделение вневедомственной охраны или частную охранную организацию (для частных организаций может существовать и другой порядок). Регистрация и рассмотрение заявления о приеме под охрану осуществляются в порядке, установленном для делопроизводства в системе Росгвардии или охранной организации.

Обследование проводится комиссионно в составе уполномоченных представителей подразделения охраны, собственника и иных заинтересованных органов и/или организаций. Первичное обследование объектов (квартир, МПХИГ) проходит в случае отсутствия обстоятельств, препятствующих обеспечению охраны имущества физических и юридических лиц (в первую очередь отсутствие судебных споров о собственности объектов). Обследование ведется в течение пяти рабочих дней (частные охранные организации устанавливают срок самостоятельно) с момента регистрации заявления путем изучения на месте состояния, характеристик и особенностей помещений и территорий, передаваемых под централизованную охрану, а также определения их устойчивости к криминальным посягательствам на момент обследования.

На основе полученных в ходе первичного обследования данных уполномоченным инженерно-техническим сотрудником охранной организации в течение трех рабочих дней после обследования проводится следующая работа:

– обобщаются предложения комиссии по приведению в согласованные сроки текущего состояния объекта (квартиры, МПХИГ) собственника предъявляемым требованиям к инженерно-техническому укреплению, параметрам оборудования, организации рубежей охранной сигнализации, каналов передачи извещений. Требования установлены нормативными документами Правительства РФ, нормативно-техническими документами вневедомственной охраны Росгвардии или частной охранной организации;

– передается собственнику для согласования и выполнения предложений подписанный уполномоченными членами комиссии и составленный в необходимом количестве экземпляров «Акт первичного обследования» с указанием класса объекта (МПХИГ) в соответствии с требованиями, установленными нормативными документами Правительства РФ к конкретной категории объекта, а также нормативными документами вневедомственной охраны Росгвардии России или частной охранной организации в отношении принимаемых под охрану объектов.

В «Акте первичного обследования» указываются дата проведения контрольного обследования, организационные мероприятия, которые необходимы для заключения договора на централизованную охрану объекта (МПХИГ), с приложением схем оснащения средствами сигнализации объекта (здания, помещения, прилегающей территории, элементов строительных конструкций, особо важных помещений и отдельных предметов). Если объект большой, то формируются исходные данные для составления технического задания на проектирование систем охранной сигнализации и/или других подсистем охраны и безопасности объекта (МПХИГ) по документу [1].

Один экземпляр акта обследования после подписания передается в подразделение охранной организации, при этом в обязательном порядке учитываются:

– размеры помещений (длина, ширина и высота) в метрах;

– распределение шлейфов и/или рубежей охранной сигнализации;

– места установки устройств объектовых оконечных СПИ (РСПИ), а также охранных извещателей, оповещателей, места подключения к абонентской линии связи и иные технические особенности установки ИТСО;

– места нахождения щита электроснабжения.

По результатам контрольного обследования уполномоченный инженерно-технический сотрудник докладывает непосредственному начальнику о степени готовности объекта (МПХИГ) к приему под охрану и заключении соответствующего договора.

В случае отказа от выполнения предложенных сотрудниками охранной организации мероприятий по обеспечению ИТУ собственника предупреждают о возможных последствиях отказа, что письменно подтверждается в акте приема/обследования объекта, а также в договоре на охрану. Данный отказ должен быть зафиксирован документально в договоре на охрану объекта/имущества отдельным пунктом и не подлежать последующему оспариванию в судебных инстанциях. При необходимости изменения сроков выполнения мероприятий, прописанных в акте первичного обследования, собственнику предлагается в письменном виде уведомить об этом охранную организацию.

В обязательном порядке при приемке объекта (МПХИГ) осуществляются мероприятия по первичному обследованию принимаемого под охрану объекта (имущества). Основные цели первичного обследования:

– определение размера возможного ущерба предприятию (организации) или собственнику имущества и связанного с ним класса объекта (МПХИГ), подлежащего принятию под охрану;

– определение мест вероятного проникновения;

– выработка согласованных с собственником единых технических решений по организации централизованной охраны с учетом требований действующих нормативных актов Росгвардии или частной охранной организации, а также иных действующих нормативных актов для установленных категорий объектов (МПХИГ).

При наличии на объекте или МПХИГ обособленных строений (помещений), попадающих под разные классы, допускается составление на них отдельных актов обследования. Задание на проектирование составляется собственником с привлечением организации-

проектировщика и организации-подрядчика монтажных работ и последующим согласованием принятых решений руководством подразделения охранной организации. В ходе обследований выбирают оптимальный с точки зрения надежности охраны и расходов собственника вариант обеспечения безопасности с обязательной блокировкой средствами охранной сигнализации всех уязвимых мест вероятного проникновения нарушителя.

Перед обследованием собственнику должны быть разъяснены основные положения организации централизованной охраны объектов (имущества) силами подразделения охранной организации на договорной основе, а именно:

– положения типового договора на централизованную охрану;

– стоимость услуг по договору на централизованную охрану;

– требования по проектированию, монтажу, техническому обслуживанию и ремонту технических средств охраны и безопасности;

– требования по инженерно-техническому укреплению, предъявляемые к различным классам объектов (МПХИГ);

– порядок проведения обследования.

При согласии собственника с предлагаемыми условиями по централизованной охране имущества с ним оговариваются дата, время и состав комиссии по обследованию. При первичном обследовании объекта, принимаемого под охрану, необходимо учесть, что объект перед заключением договора с подразделением охранной организации может быть уже оборудован техническими средствами охраны и безопасности. Комиссией, сформированной для первичного обследования объекта (квартиры, МПХИГ), устанавливаются:

– производственное или иное назначение объекта;

– наименование объекта и юридического лица собственника имущества;

– фактический и юридический адрес объекта;

– принадлежность объекта недвижимости собственнику имущества (срок действия договора аренды, пользования, оперативного управления, хозяйственного ведения и т. п.);

– ведомственная принадлежность объекта;

– предполагаемый размер экономического (материального) ущерба, а также возможный политический или общественный резонанс в случае преступных посягательств на объект;

– расположение объекта на местности относительно рядом стоящих зданий и сооружений, наличие подъездных путей для организации реагирования по сигналу «тревога» силами групп задержания вневедомственной охраны;

– границы внешнего периметра объекта;

– наличие смежных помещений (строений);

– наличие кабельных или иных абонентских сетей связи, места расположения распределительных (коммуникационных) узлов;

– возможность использования для охраны объекта иных каналов связи (выделенной линии оператора связи (Ethernet-канал, в том числе оптоволокно)/канала открытой сети Интернет/УКВ-радиоканала/GSM-канала);

– места вероятного проникновения, способы проникновения через них (открывание, пролом и др.);

– категория энергоснабжения объекта, наличие резервного энергоснабжения на объекте и охранного (дежурного) освещения;

– наличие акустических и электромагнитных помех, шумов промышленных установок, проходящих транспортных магистралей, высоковольтных линий электропередач, радиоустановок и иных факторов, влияющих на работу ИТСО;

– строительная готовность объекта.

Каждому классу объектов (МПХИГ), принимаемых под централизованную охрану подразделением вневедомственной охраны или частной охранной организацией, должен соответствовать класс защиты их конструктивных элементов строительных конструкций в соответствии с методическими рекомендациями [5; 6], нормативными техническими актами РФ в сфере стандартизации и технического регулирования, а также организационно-методическими документами Росгвардии или ведомственными нормативными документами, касающимися вопросов инженерно-технического укрепления.

Под классом защиты понимают комплексную оценку, учитывающую размещение, устойчивость к взлому, надежность, особенности конструктивных элементов и показывающую степень достаточности обеспечения надлежащей защиты объекта (МПХИГ). При проведении первичного обследования требования к соответствию классов защиты предъявляются к следующим элементам.

Строительные конструкции:

– стеновые и потолочные строительные конструкции кладовой, хранилища;

– наружные стены здания, первого этажа, а также стены, перекрытия охраняемых помещений, расположенных внутри здания, примыкающие к помещениям других собственников;

– наружные стены охраняемых помещений, расположенных на втором этаже здания и выше, а также стены, перекрытия этих помещений, расположенных внутри здания, не примыкающие к помещениям других собственников;

– внутренние стены, перегородки в пределах каждой подгруппы, вентиляционные короба.

Дверные конструкции:

– входные двери в здание, выходящие на улицы и магистрали;

– двери запасных выходов, двери, выходящие на крышу (чердак), во дворы;

– входные двери охраняемых помещений;

– внутренние двери в помещениях в пределах каждой подгруппы.

Элементы оконных конструкций:

– оконные проемы первого и подвального этажей, выходящие на оживленные улицы и магистрали;

– оконные проемы второго этажа и выше, не примыкающие к пожарным лестницам, балконам, карнизам и т. п.;

– оконные проемы первого и подвального этажей, выходящие во дворы, малолюдные переулки;

– оконные проемы, примыкающие к пожарным лестницам, балконам, карнизам и т. п.;

– оконные проемы помещений охраны.

Запирающие устройства:

– запирающие устройства входных и запасных дверей в здание, входных дверей охраняемых помещений, дверей, выходящих на крышу (чердак);

– запирающие устройства внутренних дверей.

Комиссия проверяет инженерно-техническое укрепление ограждений периметров территорий, зданий, сооружений и помещений объекта, в том числе места проведения скрытых строительных работ,

наличие на оконных и дверных проемах металлических решеток или защитного остекления по ГОСТ [23], наличие и исправность запирающих и кодово-замочных устройств, определяет количество и характеристики (размер, материал и др.) элементов строительных конструкций (окна, двери, люки, стены, перекрытия) и т. д. По результатам первичного обследования составляется соответствующий акт обследования.

Особенности первичного обследования объектов, ранее оборудованных СПИ (РСПИ). При приеме под охрану сотрудникам охранной организации объектов (МПХИГ), уже оборудованных СПИ (РСПИ), необходимо учесть следующее:

– объект должен быть оборудован ТСО, соответствующими требованиям документов [3; 4];

– достаточность количества средств охраны (количество извещателей, взаимное перекрытие зон доступа к ним);

– количество рубежной зоны;

– построение зон охраны;

– защиту технических средств охраны от несанкционированного доступа, вандализма и саботажа, в том числе в режиме «снят с охраны»;

– наличие диагностических извещений и функций устройства объектового оконечного СПИ (РСПИ), позволяющих выявить несанкционированное вмешательство в его работоспособность.

Передача извещений СПИ (служебных и тревожных) на ПЦО охранной организации должна быть реализована с использованием проводной или беспроводной среды передачи информационных сигналов с учетом класса принимаемого под охрану объекта, согласно требованиям нормативных правовых актов и действующих рекомендаций Росгвардии, рекомендаций ведомственных нормативных документов в данной сфере деятельности.

Плановое обследование объекта. Плановые обследования охраняемых объектов проводятся инженерно-техническими сотрудниками охранной организации в соответствии с разрабатываемым для конкретного ПЦО графиком. В ходе проведения планового обследования охраняемых объектов уполномоченный инженерно-технический сотрудник подразделения вневедомственной охраны проверяет:

– соответствие состава и мест установки ТСО проекту или схеме блокировки, использование ТСО в соответствии с назначением, условиями применения и тактико-техническими характеристиками;

– состояние шлейфов сигнализации ТСО;

– работоспособность ТСО и каналов связи, обеспечивающих передачу извещений на ПЦО;

– соответствие ИТУ конструктивных элементов требованиям, установленным для данного класса объекта;

– выполнение собственником правил технического обслуживания и эксплуатации ТСО;

– наличие и актуальность инструкции по пользованию ТСО на объекте;

– соответствие ответственных лиц за снятие/прием объекта под охрану сведениям, указанным в оперативной карточке и базе данных ПЦО;

– визуально целостность изоляции проводной линии абонентской связи, используемой для передачи извещений на ПЦО (в том числе в доступных местах за пределами периметра объекта), целостность печати (пломбы) и исправность запорных устройств шкафов коммуникационного оборудования;

– исполнение собственником ранее предписанных мероприятий по усилению ИТУ и эксплуатации ТСО;

– достаточность блокировки ТСО мест вероятного проникновения.

Результаты планового обследования отражаются в соответствующем акте с указанием выявленных недостатков в состоянии ТСО, ИТУ объекта и срока (сроков) их устранения. На основе результатов проверки состояния и работоспособности ТСО с ПЦО принимается решение о возможности их дальнейшей эксплуатации. Допускается использование предыдущего акта планового обследования для отметок в разделе контрольных обследований о проведении очередного обследования (технического осмотра) при отсутствии изменений в состоянии технического укрепления элементов строительных конструкций объекта (МПХИГ), а также средств сигнализации и связи охраняемого объекта (МПХИГ).

Особенности обследования объектов, оборудованных (оборудуемых) системами контроля и управления доступом. При обследовании объекта определяют характеристики значимости помещений объекта, его строительные и архитектурно-планировочные особенности, условия эксплуатации, режим работы, ограничения или расширения права доступа отдельных сотрудников, параметры установленных (или предполагаемых к установке на данном объекте) технических средств, входящих в систему контроля управления доступом. По результатам обследования выявляют технические решения и структуру организации СКУД, которые вносят в акт обследования объекта. В нем указывают:

– назначение СКУД, техническое обоснование и описание схемы;

– размещение составных частей системы.

Размещение составных частей системы определяют путем изучения чертежей, обхода и осмотра архитектурно-планировочных и строительных решений, реализованных или предполагаемых на объекте, а также путем проведения необходимых измерений выявляют:

– количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т. п.);

– материал строительных конструкций;

– количество отдельно стоящих зданий, их этажность;

– количество открытых площадок;

– количество отапливаемых и неотапливаемых помещений и их расположение.

Особенности обследования объектов, оборудованных системами видеонаблюдения (СВН). При обследовании объекта определяют виды и типы угроз, которые планируется обнаруживать и визуально выявлять с помощью внедрения системы видеонаблюдения. Видеонаблюдение предназначено для решения нескольких видов задач. Вместе с задачей обнаружения попыток противоправного воздействия могут быть поставлены задачи разрешения и идентификации.

Среди основных задач при определении эксплуатационных требований к системе видеонаблюдения следует выделить составление графической схемы места предполагаемого оснащения СВН и выделение на ней зон, где потенциально могут возникнуть проблемы в области безопасности. На схеме необходимо указать источники освещения, места предполагаемого размещения камер, поля обзора камер,

области с плохим естественным и искусственным освещением и «мертвые» зоны, где нет возможности проводить наблюдение.

Кроме того, на плане могут быть отображены наиболее вероятные места проникновения нарушителей, что позволит объективно определить требуемый уровень покрытия объекта полями зрения телекамер. Некоторые области, такие как входы или проходные, могут потребовать наблюдения под несколькими углами и в нескольких аспектах, например слежение за людским потоком и выявление попыток противоправного и террористического воздействия, а также других нежелательных действий.

Кроме условий эксплуатации систем видеонаблюдения необходимо учесть уровень подготовки персонала, расположение поста наблюдения, алгоритм реагирования на различные ситуации и т. п.

При необходимости организации поста наблюдения следует определить место расположения, размер и степень технической оснащенности поста наблюдения на охраняемом объекте, обусловливающие эффективность системы видеонаблюдения и возможности наблюдения изображения с каждой из камер при требуемом уровне детализации.

Также необходимо определить требования по обеспечению охраны помещения самого поста видеонаблюдения для предотвращения несанкционированного доступа к видеоматериалам и вмешательства в работу системы видеонаблюдения.

Типовые исходные данные к заданию на проектирование охранной (охранно-тревожной) сигнализации на объектах (квартирах, МХИГ), подлежащих подключению на пульты централизованного наблюдения охранной организации, приведены по документу [1].

1. *Класс объекта* определяется по методическим рекомендациям [5].

2. *Составляющие объекта*, подлежащие оборудованию ТСО:

– здания и сооружения;

– отдельные помещения в здании (квартире);

– отдельные предметы.

3. *Криминальные угрозы:*

– попытка проникновения на объект путем механического воздействия на замки и строительные конструкции, подбора ключей, несанкционированного снятия объекта с охраны;

– подмена оконечного объектового устройства имитирующим средством;

– умышленный вывод из строя питающей сети 220 В объекта и/или проводной абонентской телефонной линии связи (Интернета);

– подавление сети сотовой связи, создание радиопомех для РСПИ;

– обрыв или замыкание шлейфов охранной сигнализации;

– нападение на персонал и/или сотрудников охраны объекта.

4. *Электроснабжение ТСО*

4.1. Электропитание ТСО должно быть обеспечено по 1-й категории согласно ПУЭ.

4.2. При условии, что объект имеет 1-ю категорию согласно ПУЭ, резервное электропитание должно обеспечивать работу ТСО в дежурном режиме 4 часа и в тревожном режиме 1 час.

4.3. Если объект не обеспечен электропитанием по 1-й категории, то резервное питание должно обеспечивать работу ТСО в течение не менее 24 часов в дежурном режиме и в течение не менее 3 часов в режиме тревоги.

4.4. Все устройства охранной сигнализации, выполненные в металлических корпусах, должны быть заземлены.

5. *Охранная и тревожная сигнализация*

5.1. В обязательном порядке подлежат оборудованию ТСО периметры помещений первого и последнего этажей здания, подвала, чердака (на разрушение стекла и открывание), помещений, расположенных на промежуточных этажах, помещений, примыкающих к пожарным лестницам, балконам, карнизам. Остальные помещения объекта оборудуются ТСО в зависимости от функционального назначения и наличия в них ценностей.

5.2. Технические средства охраны выбирают (рекомендуется выбирать) из действующего списка технических средств безопасности, предназначенных для применения в подразделениях ВНГ РФ. Они должны обеспечивать автоматизированное управление постановкой/снятием с охраны и отображение тревожных извещений.

5.3. Комплекс охранной сигнализации организуется в соответствии с требованиями нормативных актов Росгвардии [6] или ведомственных нормативных требований и должен обеспечивать вывод всех рубежей охранной сигнализации на ПЦО охранной организации.

5.4. При охране только отдельных устройств (банкоматы, устройства самообслуживания, распределительные шкафы и другие аналогичные устройства) на ПЦО выводится один рубеж охранной сигнализации (блокировка на «разрушение» и «вскрытие») или данный рубеж включается в состав тревожной сигнализации.

5.5. Стационарные извещатели тревожной сигнализации устанавливаются:

– в кладовой и предкладовой ценностей;

– на рабочих местах персонала объекта, производящего операции с сведениями, содержащими государственную тайну, и персональными данными граждан, денежными средствами, драгоценными металлами и камнями, наркотическими, сильнодействующими и психотропными препаратами, токсичными и взрывоопасными веществами;

– на посту физической охраны;

– в помещениях хранения оружия и боеприпасов;

– в помещениях фондохранилищ и экспозиционных залах музеев, библиотек и других объектов культуры, являющихся историческими и архитектурными памятниками;

– на путях проноса ценностей;

– в иных местах по требованию собственника объекта или по рекомендации сотрудников ВНГ РФ или охранной организации.

5.6. Рекомендуется предусмотреть оснащение руководства объекта и сотрудников охраны объекта радиоканальными носимыми тревожными извещателями (брелоками), а также оснащение рабочих мест сотрудников, производящих операции с денежными и ювелирными ценностями, специальными тревожными извещателями (ловушками), формирующими сигнал тревоги без участия персонала.

5.7. Электрическую разводку для ТСО и прокладку шлейфов сигнализации необходимо спроектировать с учетом их скрытой прокладки.

5.8. Технические средства охраны должны функционировать круглосуточно при номинальном питающем напряжении сети.

5.9. Конфигурация систем охранной и/или охранно-тревожной сигнализации и применяемое оборудование должны обеспечивать возможность наращивания системы за счет расширения аппаратной и

программной частей без нарушения работоспособности смонтированного оборудования.

6. *Передача информации на ПЦО*

6.1. Передача извещений о срабатывании охранной сигнализации организуется по установленным в соответствии с договорными обязательствами каналам связи с учетом технической оснащенности ПЦО, при этом проводная среда при выборе каналов связи приоритетная [6; 29; 42].

6.2. При отсутствии возможности организации охраны объекта на базе проводной среды основной канал передачи информации – выделенная рабочая частота УКВ-радиодиапазона РСПИ [42; 61; 63; 65; 67].

6.3. Переход ТСО на резервный канал и обратно должен осуществляться автоматически без выдачи тревожного извещения.

7. *Состав разрабатываемой документации* должен соответствовать общим требованиям по ГОСТ [12; 13; 14] и включает в себя следующее:

– пояснительную записку, содержащую характеристику объекта, описание системы сигнализации, расчеты необходимых характеристик;

– поэтажные планы размещения элементов системы;

– структурные схемы организации системы;

– спецификацию оборудования системы;

– документы рабочего проекта (схемы соединений, монтажные схемы и т. п.).

Техническое задание на проектирование объектовых комплексов средств охраны и безопасности должно соответствовать требованиям документа [1]. Техническая документация на оборудование объекта техническими средствами охраны и безопасности должна быть на русском языке, иметь при необходимости соответствующий гриф секретности (конфиденциальности), выполняться в необходимом количестве экземпляров, которые после завершения проектных работ передаются собственнику объекта и другим заинтересованным организациям. Один экземпляр остается в охранной организации. Форма актов обследования приведена в соответствии с требованиями методических рекомендаций [5] в прил. 1, 2.

Контрольные вопросы

1. Какие требования предъявляются к параметрам решеток для укрепления некапитальных стен?
2. Какие требования предъявляются к параметрам решеток для укрепления оконных проемов?
3. Назовите категории (группы) объектов по техническому укреплению. Как распределяются объекты по категориям?
4. Каковы основные требования по технической укрепленности периметров охраняемых территорий?
5. Какие существуют виды ограждений периметров территорий защищаемых объектов?
6. Назовите основные требования по техническому укреплению дверных конструкций объектов.
7. Назовите основные требования по техническому укреплению оконных конструкций объектов.
8. Назовите основные требования по техническому укреплению запирающих устройств на объектах.
9. Назовите основные меры по усилению дверных конструкций объектов.
10. Назовите основные меры по усилению укрепленности коробов, люков и технологических каналов.
11. Назовите количество классов защиты элементов строительных конструкций.
12. Назовите основные меры по усилению оконных конструкций объектов.
13. Каковы основные требования по техническому укреплению кассовых узлов и сейфовых комнат?
14. Каковы основные требования по техническому укреплению банкоматов и банковских устройств самообслуживания?
15. Какая информация отражается в акте обследования состояния инженерно-технического укрепления объекта?

Глава 2. ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАННО-ТРЕВОЖНОЙ СИГНАЛИЗАЦИИ

2.1. Требования по оснащению средствами охранно-тревожной сигнализации периметров охраняемых территорий

Для обеспечения комплексной системы безопасности важный элемент – система защиты периметра объекта. Для критически важных объектов, объектов жизнеобеспечения и повышенной опасности периметральные технические средства защиты территорий обязательны. Общие требования к периметральным средствам охраны описаны в рекомендациях [26]. Для проектирования систем защиты периметра территорий необходимо учитывать следующие особенности и дестабилизирующие факторы:

– топографию территории защищаемого объекта, в том числе планы конфигурации его периметра;

– состав, конструктивные особенности и технические характеристики ограждений периметра защищаемого объекта;

– характер рельефа местности защищаемого объекта;

– состав почв и особенности геологии территории защищаемого объекта;

– наличие и расположение железных дорог и автомобильных магистралей, газопроводов, ЛЭП, кабельных линий и т. д.;

– наличие животных и птиц, вероятность их появления и пути движения на территории защищаемого объекта;

– дестабилизирующие климатические аспекты, характерные для данного региона.

Монтаж и эксплуатация периметральных средств охраны (ПСО) могут осуществляться в совершенно разных климатических, геологических условиях и на разных почвах на всей территории Российской Федерации. При этом возможны совершенно разные сезонные колебания влажности, температуры, ветров, осадков и так далее, что характерно для многих регионов РФ. Данные обстоятельства вызывают необходимость жестких требований к надежности функционирования ПСО [15; 19; 20] в течение всего срока эксплуатации (по ГОСТ [51] – не менее восьми лет). Периметральные средства охраны, смонтированные на территории защищаемого объекта, должны обнаруживать самые разнообразные типы и способы преодоления периметра защи-

щаемого объекта, в том числе перелазы через ограждение, разрушение ограждения, подкопы под ограждением и пр.

Периметральные средства охраны должны обладать высокой помехоустойчивостью и сохранять свою работоспособность при помехах самого различного происхождения, в том числе при порывах ветра, осадках, граде, в снег, туман, при выпадении росы, обледенении конструкций извещателей и элементов ограждений, сейсмических и виброакустических воздействиях от транспортных средств и других техногенных факторов. Кроме того, необходимо учитывать перемещения животных и птиц, грозы, помехи от высоковольтных ЛЭП, подземных и воздушных коммуникаций, а также преднамеренные дестабилизирующие воздействия, которые могут создаваться в том числе и нарушителем.

Организация защиты периметра охраняемого объекта всегда решается путем комплексирования средств инженерно-технического укрепления ограждений территорий и технических средств ПСО. Такое комплексирование технических средств должно быть максимально оптимальным. Все технические средства ПСО классифицируются исходя из физического принципа функционирования в них чувствительных элементов (ЧЭ) различных видов и конструктивного исполнения. Многообразие видов различных конфигураций территорий защищаемых объектов, типов используемых ограждений, разновидностей существующих для данной территории дестабилизирующих факторов обусловливает разнообразие средств ПСО. Кроме того, в зависимости от категории защищаемого объекта и его потенциальной опасности требуется организация различного числа рубежей охраны.

Современные ПСО классифицируются прежде всего по физическим принципам их функционирования. При этом различают ЧЭ. Так, в *электромеханических ПСО* ЧЭ – натянутые проволочные нити с датчиками. Механическое воздействие на нити, в том числе их раздвижение, обрыв или короткое замыкание, формирует тревожное извещение. Однако такой вид ПСО в настоящее время применяется весьма редко из-за сложного эксплуатационного обслуживания и низкой имитостойкости.

В вибрационных ПСО в качестве ЧЭ применяются датчики вибраций для кабелей (оптоволоконные или трибоэлектрические), а так-

же системы точечных датчиков, которые могут быть пьезоэлектрическими или электромагнитными. Физический принцип действия *вибрационных ПСО* основан на деформировании ограждения или его механических колебаниях при попытках перелезть через ограждение или под ограждением путем отгиба нижнего края, повреждения полотна ограждения, подкопа и т. п.

Принцип действия *емкостных ПСО* основан на изменении емкости ЧЭ или самого металлического ограждения, если оно изолировано от земли, при прикосновении или приближении нарушителя, а также при попытке перелезть через ограждение, разрушении или подкопе.

Индуктивные ПСО срабатывают при изменении индуктивности электрических цепей с включенным ЧЭ, при изменении формы электрического проводника, при обрыве, коротком замыкании проводников, определенным образом установленных на защищаемом ограждении. *Радиоволновые локационные средства обнаружения* (РЛСО) состоят из разнесенных в пространстве передатчиков и приемников СВЧ-излучений. Базовый принцип действия РЛСО основан на изменении принимаемого сигнала при пересечении нарушителем зоны обнаружения между передатчиком и приемником. В *проводноволновых ПСО* существует система параллельных проводов с протекающими по ним радиочастотными сигналами, создающими излучения вдоль этих проводов. Извещение о тревоге формируется при изменении параметров принимаемого сигнала в результате воздействия нарушителя, появившегося рядом с системой параллельных проводов ПСО. Обычно такие ПСО используют для защиты ограждения в верхней (козырьковой) части.

Физический принцип действия *магнитометрических ПСО*, которые представляют собой систему проводов, чувствительную к изменению напряженности магнитного поля, состоит в срабатывании ПСО при перемещении через неё металлических предметов. *Сейсмические средства обнаружения* (ССО) состоят из системы специфических кабелей и датчиков, установленных в почве. Принцип их действия основан на регистрации сейсмических колебаний грунта, формируемых перемещающимся по охраняемой зоне транспортным средством или человеком.

Манометрические ПСО состоят из протяженных гидравлических извещателей (датчиков) давления, могут использоваться для защиты как огражденных, так и неограждаемых периметров территорий объектов. Такие ПСО могут применяться и для раннего обнаружения потенциального нарушителя, и для выявления подкопа под защитным ограждением или зданием.

Оптико-электронные средства обнаружения (ОЭСО) подразделяются на активные и пассивные. В зависимости от особенностей защищаемых территорий в некоторых случаях используют активные оптико-электронные ПСО, состоящие из пространственно разнесенных передатчика и приемника, создающих ИК-барьеры. Прерывание ИК-лучей со стороны нарушителя формирует тревожное извещение.

Волоконно-оптические (ВОС) *ПСО* обладают наиболее протяженным ЧЭ и обеспечивают защиту наиболее протяженных участков периметров защищаемых территорий. В таких ПСО ЧЭ используется как для обнаружения перелаза или разрушения защищаемого ограждения, так и для защиты неограждаемых участков периметра. Физическое воздействие нарушителя на волоконно-оптический кабель приводит к изменению свойств его светопередачи и формирует тревожное извещение в данных ПСО.

Радиолокационные станции (РЛС) обычно применяют на объектах со значительной протяженностью. При этом осуществляется контроль периметра объекта и внутренней территории. С помощью РЛС возможно эффективно решать задачи защиты подступов к охраняемым объектам и задачи защиты отдельных площадок.

В некоторых группах ПСО выделяют быстроразворачиваемые комплексы (БРК), которые могут использовать различные физические принципы и предназначены для оперативной и временной охраны отдельных участков периметров, подступов к ним, открытых площадок или отдельных объектов, в том числе и мобильных. Такие ПСО выделяют в отдельную группу исходя из области применения. Как показывает анализ практики эксплуатации ПСО, использование ПСО, основанных только на каком-либо одном физическом принципе обнаружения, не эффективно, так как не обеспечивается необходимая помехоустойчивость, особенно на объектах, где существует большое количество дестабилизирующих факторов и сложная помеховая об-

становка. Такая ситуация приводит к большому количеству ложных срабатываний и частым выездам групп задержания, иногда и на значительные расстояния. Также БРК не обеспечивают эффективную защиту ограждений периметров объектов от наиболее вероятных способов преодоления периметра (перелаз, разрушение ограждения, подкоп под ограждением и др.).

Наиболее перспективное направление развития ПСО в настоящее время – использование комбинированных и комбинированно-совмещенных ПСО, которые основаны на нескольких физических принципах функционирования, что обеспечивает более качественную защиту ограждений защищаемых территорий объектов от большего количества потенциально возможных вариантов их преодоления. Такие ПСО обладают необходимыми параметрами достоверности обнаружения, функциональной надежности, имитостойкости, помехоустойчивости и технико-экономической эффективности.

Наиболее вероятные способы преодоления ограждений периметров объектов нарушителями

Для обеспечения эффективной охраны периметров защищаемых территорий при проектировании комплекса средств ПСО необходимо учитывать все возможные действия нарушителя при проникновении (попытке проникновения) на защищаемый объект [26; 27]. С данной целью составляется модель нарушителя. При проектировании периметровой сигнализации обычно подразумевается модель стандартного («нормального»), т. е. одиночного и неосведомленного, нарушителя, имеющего с собой только стандартный слесарный инструмент, с помощью которого можно повредить ограждение, доску или лестницу для совершения перелаза, лопату для подкопа и пытающегося преодолеть ограждение «с ходу» в среднем или даже быстром темпе. Такое допущение справедливо согласно практике функционирования ПСО для большей части (согласно экспертным оценкам от 85 до 95 %) нарушителей без четких криминальных целей. Основная цель типового нарушителя – хулиганство, кража или вандализм. Наиболее опасны с точки зрения проникновения на объект:

– группа нарушителей, которые имеют распределенные обязанности и помогают друг другу при пересечении рубежа (например,

вставая на плечи или разжимая проволочные нити ограждения) или создают «поток тревог» ПСО по защищаемому объекту, дезориентируя физическую охрану;

– нарушители со специальными средствами, позволяющими осторожно преодолеть охраняемый рубеж путем перелаза (с помощью лестницы), организации «моста» (доска, лестница) над ограждением;

– разрушение ограждения специальным гидравлическим или пневматическим инструментом, автогеном и так далее, а также преодоление его изощренными, но возможными способами, например перекатом, прыжком, подкопом или перелетом на планере;

– подготовленный нарушитель, который (визуально, путем наблюдения или с помощью аппаратуры, путем разведданных) выявляет тип и вид ПСО, изучает соответствующую документацию, определяет уязвимые технические параметры ПСО, способы преодоления ЧЭ, при которых эффективность обнаружения снижается до минимума, например построение «моста» над зоной обнаружения (ЗО) с помощью доски, лестницы и т. д.;

– очень медленное (менее 0,1 м/с), а в некоторых случаях очень быстрое (более 10 м/с, прыжком) пересечение зоны обнаружения ЧЭ, при котором возникающие сигналы срабатывания ЧЭ либо находятся за пределами диапазона регистрируемых воздействий, либо воспринимаются со стороны блоков обработки ЧЭ как помеховые воздействия;

– постепенное и осторожное разрушение конструкции защитного ограждения, например для сетки это выкусывание нитей с промежутком один раз в несколько минут, одновременное «гашение» вибраций и последующее проникновение на объект через отверстие или аналогичные способы.

В табл. 2.1 представлены возможные способы действий подготовленных нарушителей и соответствующие меры противодействия, которые необходимо учитывать при проектировании периметральных систем охраны, включая выбор (если такое возможно) типов и вариантов ограждений и уровня их технического укрепления.

Таблица 2.1

Способы действий нарушителей и соответствующие меры противодействия

Этап преодоления ПСО	Способ квалифицированного воздействия нарушителя	Меры по противодействию нарушителям
Подготовка к преодолению ПСО	Визуальное выявление установки ПСО	Использование ПСО, предназначенных для скрытой установки, или ПСО с малозаметным ЧЭ. Использование сплошного непрозрачного основного ограждения высотой не менее 2,5 м
Подготовка к преодолению ПСО	Определение границ зоны обнаружения ПСО	Использование охранных телевизионных систем для обнаружения подозрительной активности на внешнем рубеже охраны. Применение совмещенных (комбинированно-совмещенных) ПСО, формирующих разнесенные ЗО таким образом, чтобы исследование внутренних ЗО с внешней стороны ограждения было невозможным. Применение пассивных ПСО, например сейсмических, вибрационных, ВОС и т. д.
	Неправомерный доступ к информации о структуре системы охраны периметра (СОП)	Выполнение необходимого комплекса организационно-технических мероприятий по защите информации о составе и структуре СОП, расположении ее элементов
Преодоление ПСО	Подкоп	Бетонирование фундамента ограждения. Применение противоподкопного ПСО, установленного на нижнем дополнительном ограждении, или сейсмического ПСО
	Замедленное или убыстренное преодоление периметра	Выбор оптимальной конструкции ограждения, максимально затрудняющей ее преодоление. Выбор ПСО с соответствующими тактико-техническими характеристиками (высокая обнаружительная способность, широкий диапазон обнаруживаемых скоростей перемещения нарушителя)

Окончание табл. 2.1

Этап преодоления ПСО	Способ квалифицированного воздействия нарушителя	Меры по противодействию нарушителям
Преодоление ПСО	Замедленное разрушение полотна ограждения	Профилактические охранные мероприятия, например регулярный обход периметра. Выбор ограждений, разрушение которых любым способом приводит к достаточному для обнаружения уровню полезного сигнала (например, АКЛ)
	Блокирование ПСО путем его зашумления	Применение ПСО, формирующих извещение о повышенной помеховой обстановке и саботаже. Применение ПСО с активным принципом обнаружения. Применение комбинированных или комбинированно-совмещенных ПСО

Общая классификация ПСО и тактика применения

Общая классификация ПСО приведена в ГОСТ [51]. Периметральные средства охраны разделяют на два класса: *стационарные*, которые предназначены для длительной непрерывной работы (средний срок службы ПСО должен быть не менее 8 лет), и *быстроразворачиваемые комплексы*, которые предназначены для временной защиты периметров территорий или открытых площадок на время не более 2 – 3 месяцев.

Основные тактико-технические характеристики БРК уступают характеристикам стационарных ПСО, особенно по массогабаритным параметрам, гибкости тактики применения.

Некоторые средства обнаружения ПСО получили свои названия, использующиеся в технической литературе, не по регистрируемому физическому параметру или физическому принципу, положенному в основу действия, а по конструкции ЧЭ (например, трибоэлектрические или вибрационные) [26; 27].

Существуют различные типы ПСО, среди которых можно выделить:

– маскируемые или немаскируемые (видимые);

– пассивные или активные.

Маскируемые средства обнаружения (СО) размещают в почве, грунте или в другой среде. Они имеют важное тактическое преимущество: идентификация их зон обнаружения затруднена, что делает вторжение нарушителя каким-либо ухищренным способом маловероятным, при этом не допускается резкого снижения обнаружительной способности ПСО. Для маскируемых ПСО, как правило, источников существенных помех значительно меньше. Такие ПСО не требуют регулярного технического обслуживания, сужается диапазон предельных рабочих температур.

Немаскируемые СО, размещенные на поверхности земли, специальных конструкциях или защитном ограждении, в целом более дешевые и практичные, их монтаж и замена в случае поломок не представляют затруднений. Однако возможна их идентификация со стороны подготовленного («грамотного») нарушителя, что увеличивает уязвимость защиты периметра ПСО.

Немаскируемые ПСО подразделяют на заградительные, незаградительные и лучевые. В первом случае ЧЭ распределен вдоль зоны обнаружения и представляет собой совокупность проводов или кабелей, размещенных на ограждении. Может быть, что ЧЭ представляет собой ограждение, которое препятствует нарушителю свободно проникнуть на охраняемый объект, и подвергается механическому воздействию при попытке проникновения. Для незаградительных ПСО провода или кабели, распределенные вдоль рубежа и образующие ЧЭ, физически не препятствуют движению нарушителя, однако с их помощью формируется электромагнитное поле, параметры которого контролируются, и при их изменении создается тревожное извещение [26; 27]. Лучевые ПСО характеризуются зоной обнаружения, формируемой с помощью компактных излучателей электромагнитного поля, параметры которого контролируются компактным приемником, и при их изменении формируется тревожное извещение. Такие технические средства могут быть двухпозиционными или однопозиционными в соответствии с тем, разделены или совмещены в одном блоке передатчик (ПРД) и приемник (ПРМ).

Заградительные ПСО с точки зрения эксплуатации более предпочтительны, поскольку они осуществляют функцию задержки

проникновения нарушителя на время реагирования нарядами физической охраны, что весьма важно в оперативно-тактическом плане. Помехоустойчивость заградительных СО зависит от типа и конструкции защитного ограждения, его «качества», которое выявляется обычно при действии дестабилизирующих факторов, в том числе при сильном ветре («дребезжание» сетки, качание опор). Заградительные средства визуально обнаруживаются квалифицированным нарушителем. Их стоимость значительно выше, чем незаградительных средств.

Незаградительные средства при меньшей стоимости обладают малозаметностью, практически не зависят от конструкционных свойств ограждения. Лучевые СО обладают более низкой стоимостью относительно размеров защищаемого периметра территории, однако чувствительность по длине ЗО у них неравномерна, велико воздействие на чувствительность ЧЭ некоторых помеховых факторов (мелкие и средние животные). Ухудшаются их тактико-технические характеристики (ТТХ) вплоть до отказа при высоком снежном покрове, неровном рельефе местности. Часто случаются ложные срабатывания от падающих веток деревьев и листвы и т. д.

В *активных СО* нарушителя обнаруживают при его взаимодействии со специально создаваемым физическим (обычно электромагнитным) полем, например радиолучом; в *пассивных СО* его обнаруживают по вносимому возмущению в существующее поле, например в электростатическое поле или магнитное поле Земли. У пассивных СО меньшие массогабаритные характеристики и энергопотребление, что можно отнести к их преимуществам, а также они соответствуют требованиям визуальной и радиомаскировки [26; 27].

К преимуществам активных СО можно отнести высокую обнаружительную способность и помехоустойчивость, но при этом существует зависимость полезного сигнала от вида и состояния ограждения.

В зависимости от вида ЗО средства могут быть:

– объемного или линейного (контактного) обнаружения;

– повторяющими рельеф местности или распространяющимися вдоль рубежа по лучу.

Средства обнаружения с объемной (трехмерной) зоной обнаружения обладают большей обнаружительной способностью, чем средства с ЗО в виде чувствительной линии, для которых необходим физический контакт с нарушителем. Объемную зону всегда труднее обойти, даже используя имеющиеся подручные средства. Такую ЗО всегда трудно определить по границам ее действия. Преимущество СО с контактной ЗО – нечувствительность к объектам, перемещающимся рядом с ограждением (деревья при ветре, животные, транспорт), поэтому при прочих равных условиях они обладают большей помехоустойчивостью и меньшей трудоемкостью при обслуживании.

Средства обнаружения, у которых ЗО распространяется вдоль охраняемого периметра по лучу, более просты в установке и эксплуатационно-техническом обслуживании. Однако они требуют тщательной инженерной подготовки местности, им нужны основания (платформы) для установки (ограждение, стена сооружения). Такие ПСО легче идентифицируются со стороны нарушителя. Чем сложнее конфигурация периметра и рельеф местности, тем они менее эффективны, при этом возможно большее количество «мертвых» зон. Средства ПСО, которые следуют рельефу местности, обычно не нуждаются в проведении подготовительных земляных работ, однако их установка, настройка и эксплуатационно-техническое обслуживание более дорогие. Кроме того, немаловажные характеристики СО – вероятность обнаружения, имитостойкость, помехоустойчивость, длина защищаемого участка периметра территории, токопотребление, стоимость, надежность, а также уязвимость СО к нестандартным способам преодоления (обходу) и саботажа.

В России при проектировании и эксплуатации ПСО учитывается многообразие климатических и почвенно-геологических условий. Здесь наблюдаются значительные сезонные колебания температуры. Изменения климатических условий делают практически невозможным использование какой-либо единой системы для всех климатических зон России [26; 27]. Температурный диапазон применения для отечественных извещателей должен иметь границы от –40 до +50 °С. Для извещателей ПСО требуется универсальность и гибкость, а также возможность работы в широком диапазоне условий эксплуа-

тации. Любое ПСО должно легко сочетаться с другими ПСО, имеющими совершенно различные принципы физического действия ЧЭ, а также требуется обеспечение функционирования ПСО совместно с системами охранного телевидения.

Емкостные средства обнаружения

На рынке охранной сигнализации в настоящее время имеется большой выбор емкостных извещателей для охраны периметров [4; 26]. К достоинствам емкостных извещателей относят высокую чувствительность и отсутствие «мертвых» зон. Стандартно в емкостных извещателях присутствуют ЧЭ и БОС (блок обработки сигналов). Извещатели выдают тревожное извещение при касании или приближении нарушителя к ЧЭ. Особенно хорошо емкостные извещатели проявляют себя при функционировании на периметрах со сложной конфигурацией и рельефом. Извещатель выдает тревожное извещение при изменении электрической емкости антенны на заданное значение, которое превышает установленное пороговое значение формирования сигнала тревоги.

Чувствительный элемент этих извещателей состоит из одного или нескольких металлических электродов, закрепленных на специальных изоляторах вдоль или сверху защитного ограждения, представляющих собой антенну всей системы. Зона обнаружения емкостного извещателя формируется обычно в виде цилиндра и имеет основание в виде эллипсоида. При этом продольная ось эллипсоида параллельна проводникам антенны всей системы. Кроме того, использование инженерного ограждения в качестве ЧЭ – явное преимущество данного типа извещателей.

При монтаже емкостных ПСО необходимо всегда учитывать, что ЧЭ этих извещателей должен быть изолирован от земли. Все секции решетки ограждения должны быть соединены в общий электрический контур и изолированы от основной ограды. Антенная система подключена к БОС, который генерирует электрический сигнал, а также измеряет и контролирует емкость антенной системы.

Наиболее эффективным представляется использование ЧЭ в качестве козырьков из сварной сетки на периметрах охраняемых терри-

торий, где имеются прочные жесткие ограждения (сварные металлические панели, железобетонные плиты, кирпичные стены и т. п.). Емкостные ПСО подвержены воздействию дестабилизирующих факторов, влияющих на функционирование емкостных СО. В числе дестабилизирующих факторов:

1) воздействие вредных, паразитных сигналов от большого числа внешних, в том числе и электромагнитных, помех. Природа их возникновения может быть самой разнообразной:

– осадки (туман, гроза, дождь, снег, гололед, ветер и т. д.);

– индустриальные помехи (радионаводки и электрические помехи, акустический шум, вибрации);

2) птицы, садящиеся на ЧЭ;

3) влияние растительности (деревья и кусты) в ближней зоне ЧЭ или при непосредственном его касании;

4) сложность выделения и оценки характеристик полезного сигнала на фоне помех.

Полезный сигнал в виде изменения общей емкости (скорости изменения емкости) от воздействия нарушителя очень мал и составляет, как правило, сотые доли процента от контролируемого параметра. Например, 10 пФ при общей электрической емкости ЧЭ 5000 пФ. Все эти источники помех и некоторые другие могут вызывать ложные тревоги, поэтому при применении емкостных извещателей самое пристальное внимание уделяется исследованию различных помех на объекте и правильной установке и настройке извещателя. Современные емкостные извещатели используют специальные схемы обработки сигнала и обладают повышенной помехозащищенностью для снижения ложных тревог, которые формируются только при нарушении правил монтажа или эксплуатации извещателей, а также при экстремальных условиях. Один из лидеров по разработке и производству емкостных извещателей СПИ – СНПО «Элерон», создавшее новые периметровые извещатели: «Ромб-12МП», «Радиан-14», «Радиан-15МП», «Радиан-16». На рис. 2.1 показан внешний вид емкостного СО, установленного на железобетонном заборе.

Рис. 2.1. Внешний вид емкостного СО, установленного
на железобетонном заборе

Достоинства емкостных извещателей:

– могут использоваться для построения системы охраны с уже имеющимися ограждениями;

– в качестве ЧЭ используется инженерное ограждение;

– отсутствуют «мертвые» зоны, обладают высокой чувствительностью;

– ЗО легко настраивается и регулируется;

– позволяет устанавливать контроль над периметром со сложной конфигурацией;

– универсальны, нечувствительны к неровностям профиля грунта или профиля ограждения.

Недостатки емкостных извещателей:

– усложнение аппаратуры для снижения воздействия дестабилизирующих факторов – вредных, паразитных сигналов от большого

числа внешних помех (индустриальные помехи, метеорологические осадки и пр.);

– птицы, садящиеся на ЧЭ, и растительность в ближней зоне ЧЭ или при непосредственном его касании оказывают значительное влияние на работу емкостного извещателя;

– требуется надежное закрепление ЧЭ и заземление БОС.

Радиоволновые средства обнаружения

Радиоволновые средства обнаружения (РВСО) и РЛСО различаются тем, что у них разный способ формирования чувствительной зоны:

– РВСО использует ближнюю зону распространения радиоволн (менее 10λ);

– РЛСО использует дальнюю зону распространения радиоволн (более 100λ).

В зависимости от принципа действия также различаются активные и пассивные РВСО и РЛСО [4; 26; 48; 55]. *Пассивные РВСО и РЛСО* используют собственное излучение обнаруживаемого объекта или вызываемое данным объектом изменение электромагнитного поля от внешних источников – в основном от вещательных телевизионных и радиостанций. *Активные РВСО и РЛСО* используют собственные электромагнитные поля, формирующие зоны обнаружения РВСО и РЛСО. Кроме того, существуют одно- и двухпозиционные РВСО и РЛСО. В однопозиционных РВСО и РЛСО совмещен в одном устройстве блок приемопередатчика (пассивные РВСО и РЛСО всегда только однопозиционные); двухпозиционные РВСО и РЛСО имеют разнесенные приемник и передатчик.

Пассивные РЛСО применяют для обнаружения нарушителей в том случае, если они имеют собственное электромагнитное излучение, т. е. нарушитель должен иметь при себе какое-то электрооборудование или малоразмерное транспортное средство с таким оборудованием, например малоразмерный летательный аппарат и т. п. Активные однопозиционные РЛСО включают в себя однопозиционную РЛСО, нелинейный радиолокатор, радиоволновой извещатель.

Радиоволновые локационные средства обнаружения, функционирующие в метровом, дециметровом, сантиметровом и миллиметро-

вом диапазоне волн, применяют для контроля территорий, прилегающих к особо важным объектам, а также для охраны береговой полосы, прибрежной зоны и ближней разведки в условиях боевых действий. Существуют стационарные, мобильные (установленные на подвижной платформе) и носимые РЛСО. Нелинейный радиолокатор анализирует широкополосный сигнал специальной формы и предназначен для обнаружения подвижного человека за неподвижными физическими укрытиями и преградами (деревянные, кирпичные и железобетонные стены, перекрытия и т. п.).

Радиоволновой однопозиционный извещатель применяют для временной защиты проемов в ограждениях, охраны внутренних объемов помещений, перекрытия «мертвых» зон при охране периметров, организации скрытых рубежей защиты охраняемых помещений.

Однопозиционные микроволновые СО работают в дециметровом, сантиметровом и миллиметровом диапазонах. Для обнаружения движущегося человека (нарушителя) используется изменение расположения стоячих волн в защищаемом объеме при появлении объекта обнаружения либо изменение частоты отраженного сигнала от нарушителя на основе эффекта Доплера при движении объекта обнаружения. Двухпозиционные РЛСО работают в дециметровом, сантиметровом и миллиметровом диапазонах и используются для защиты периметров территорий объектов, открытых площадок хранения материальных ценностей, автотранспорта, грузов и т. п. Сигнал о срабатывании формируется на основе анализа динамики изменения объектом обнаружения (нарушителем) зондирующего сигнала от извещателя. Двухпозиционные РВСО работают в декаметровом, метровом и дециметровом диапазонах длин волн и используются для защиты периметров территорий объектов, а также для формирования скрытых рубежей охраны. В качестве антенных систем РВСО могут использоваться радиоизлучающие кабели (другое название – линия вытекающей волны (ЛВВ)), а также кусочно-ломаные двух- и однопроводные специализированные линии. Зона обнаружения двухпозиционных РВСО представляет собой участок защищаемого периметра охраняемой территории, появление в котором объекта обнаружения (нарушителя) вызывает в РВСО возникновение полезного сигнала с уровнем, превышающим пороговый уровень, а также уровень шума или помехи. За границей зоны обнаружения необходимо расположить зону от-

чуждения, в которой никто (или ничто) не должен находится. Появление в зоне отчуждения людей, перемещение техники или колебание кустов, деревьев могут привести к превышению полезным сигналом порогового значения формирования тревожного извещения.

Радиоволновые однопозиционные извещатели

В основе принципа действия данных извещателей лежит эффект Доплера. Применение традиционных однопозиционных радиоволновых извещателей требует соблюдения достаточно большого количества технических ограничений и условий [26; 48; 55]. Данным извещателям присущи типовые недостатки: неравномерная чувствительность (зависимость чувствительности от расстояния до обнаруживаемого объекта), низкая помехоустойчивость к близко расположенным колеблющимся и вибрирующим предметам, электромагнитные помехи и пр. Они ограничивают использование таких извещателей. Неравномерная чувствительность проявляется в том, что крупногабаритные объекты даже за пределами ЗО (для человека) формируют такой же сигнал обнаружения, как и мелкие объекты, находящиеся рядом с извещателем. На рис. 2.2 показана ЗО радиоволнового однопозиционного извещателя.

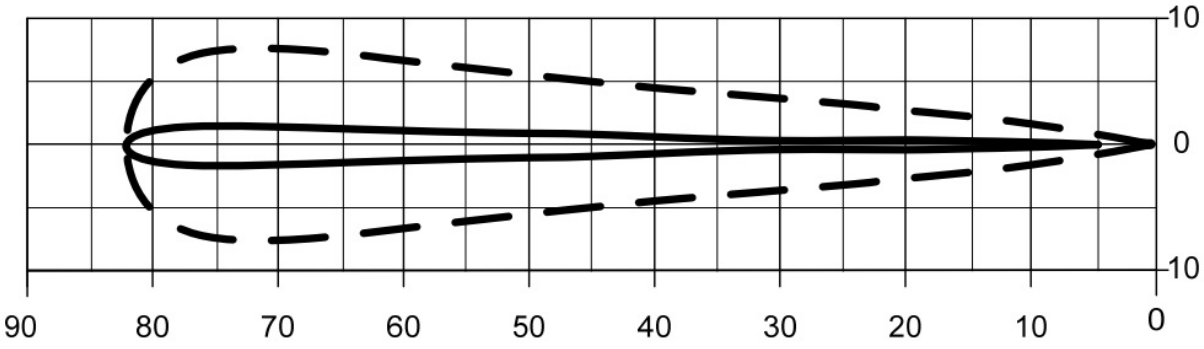


Рис. 2.2. Зона обнаружения радиоволнового однопозиционного извещателя

Излучение сложного сигнала для таких извещателей позволяет измерять расстояние до объекта, определять, перемещается ли объект и в какую сторону, вибрирует ли он. На этом принципе построен алгоритм обнаружения извещателей ИО407-14/2 «Фон-3Т», ИО407-14/3 «Фон-3Т/1» (ЗАО «Аргус-Спектр») и ИО407-18 «Волна- 6» (ЗАО «ЮМИРС»).

Радиоволновые двухпозиционные извещатели

Извещатель состоит из передатчика и приемника, между которыми создается сплошной радиоволновой барьер обычно в форме эллипсоида с большой осью, совпадающей с условной прямой линией, соединяющей центры антенных устройств приемника и передатчика или точки максимального излучения и приема радиоволн.

На рис. 2.3 показана ЗО радиоволнового двухпозиционного извещателя. Видно, что вблизи передающего и приемного блоков ЗО в сечении практически совпадает с апертурой (эффективной площадью) антенн и значительно расширяется к середине контролируемого участка.

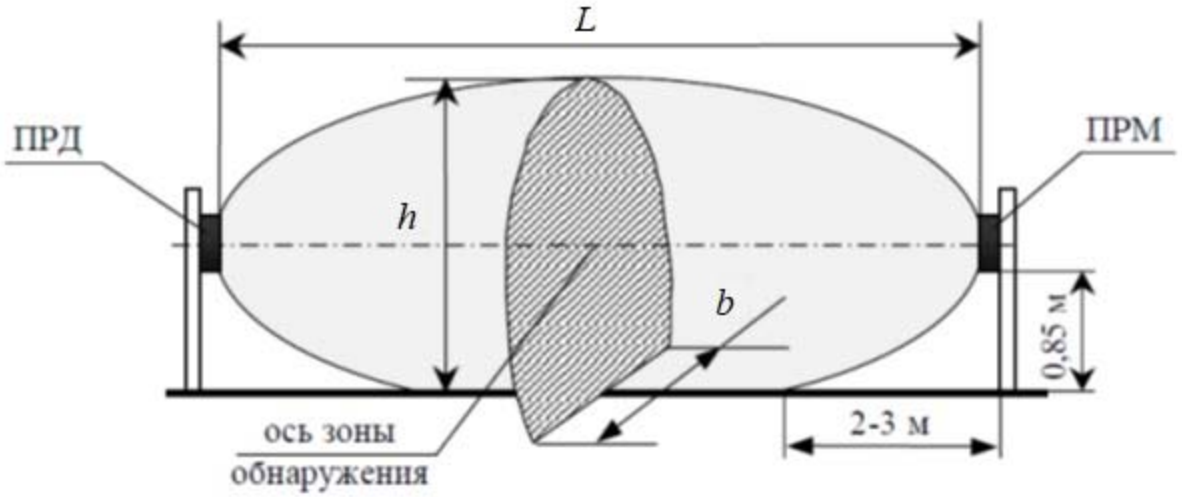


Рис. 2.3. Зона обнаружения радиоволнового двухпозиционного извещателя:
L – длина участка; *h* – высота зоны обнаружения; *b* – ширина зоны обнаружения

Передатчик излучает радиоимпульсы специальной формы, а приемник их принимает. Принцип действия извещателей основан на регистрации и анализе колебаний, принимаемых ПРМ. При этом формы диаграммы направленности, ширина и высота ЗО определяются выбранной рабочей частотой (обычно от 1 до 28 ГГц и выше), алгоритмом обработки сигналов, а также включением в обработку сигналов высших зон Френеля, значениями порогов и боковыми лепестками антенн.

Для рабочей частоты около 10 ГГц диаметр ЗО (эллипсоида) в середине участка длиной (250±50) м примерно равен 5 м. Выбор ра-

бочей частоты ограничивает возможности антенн по направленности излучения и приему СВЧ-сигнала. При этом чем лучше направленность антенн, тем больше дальность и меньше ширина ЗО, меньше влияние окружающих дестабилизирующих факторов. Минимизация габаритов антенн снижает их направленность, а увеличение частоты, наоборот, повышает направленность. Однако увеличение частоты приводит к увеличению влияния метеорологических дестабилизирующих факторов, мелких предметов и животных, попадающих в ЗО. При этом снижается информативность ПСО, увеличиваются вероятность ложных тревог, зоны нечувствительности вблизи антенн, снижается обнаружительная способность извещателя в целом.

В силу данного обстоятельства большинство разработчиков и производителей находят «золотую середину» (используют диапазон около 10 ГГц) и проектируют параметры антенн данных извещателей, исходя из компромисса между направленностью (шириной ЗО), информативностью детектированного сигнала и конструктивными решениями, для получения высоких эксплуатационных характеристик при невысокой стоимости.

Достоинства радиоволновых извещателей охраны периметра следующие:

– безопасный уровень излучения;

– объемная невидимая ЗО;

– малое энергопотребление;

– РЛСО обладают устойчивостью к изменениям условий окружающей среды и помехам в виде тумана, ветра, снега, дождя, мелких животных, птиц, от радиостанций, вибрации, по питанию, электростатическим разрядам, устойчивостью к воздействию внешнего излучения в рабочем диапазоне частот с целью саботажа и т. д.

Недостатки радиоволновых извещателей охраны периметра следующие:

– для устойчивой работы РЛСО должна быть обеспечена зона отторжения, превышающая размеры ЗО;

– РЛСО требуют прямую видимость между приемником и передатчиком;

– для обеспечения устойчивой работы РЛСО необходимо обслуживать ЗО охраняемого периметра, а также и зону отторжения.

Проводноволновые средства обнаружения (ПВСО)

Физический принцип действия извещателя ПВСО состоит в формировании объемной ЗО «козырькового» типа вокруг ЧЭ из двух изолированных проводов, которые закреплены параллельно друг другу на диэлектрических изоляторах (консолях) [26]. Такие параллельные провода образуют как бы «открытую антенну» (линейную часть) извещателя. К одному концу такой линии подключается передатчик (ПРД), а к другому – приемник (ПРМ). При пересечении ЗО нарушителем происходит изменение параметров электромагнитной волны, которая распространяется от ПРД к ПРМ, и формируется тревожное извещение. Попадание нарушителя в ЗО приводит к локальному изменению диэлектрической проницаемости среды, а следовательно, вызывает изменение электрического сигнала, поступающего на приемник. В результате этого и формируется тревожное извещение.

В настоящее время в проводноволновых средствах обнаружения ПРД формирует импульсный сигнал с широким спектром для обеспечения равномерной чувствительности извещателя по всей длине двухпроводной линии. Изменения принимаемого сигнала анализируются в ПРМ, который в соответствии с заданным алгоритмом выдает сигнал тревоги. Передатчик формирует импульсный высокочастотный сигнал, создающий электромагнитное поле между проводниками. Вокруг проводящей пары («открытой антенны») образуется объемная ЗО с поперечным сечением эллипсоидной формы, в фокусах которого расположены проводники. Расстояние между проводниками обычно составляет 0,4 м; при этом ЗО имеет размеры 0,5×0,8 м.

В настоящее время широко представлены ПВСО отечественного производства: серия извещателей «Импульс», «Импульс-мини» (НТЦ «Электронная аппаратура»), «Газон-24» (НИКИРЭТ), «Рельеф», «Рельеф-2» (ЗАО «Охранная техника»), «Трасса»/«Трасса-2» (ООО ПМЦ «Старт-7»), «Параллель» (ЗАО «ЮМИРС») и др.

Проводноволновые средства обнаружения достаточно надежно охраняют периметры защищаемых территорий. Извещатели настраиваются на обнаружение объектов массой не менее (30 ± 10) кг, не выдают ложную тревогу при попадании мелких животных в ЗО, в том числе и при посадке птиц на проводники. Извещатели не формируют

извещение о тревоге при проезде транспорта на расстоянии более 3 м от охраняемого периметра, устойчивы к воздействию снега, града, сильного дождя (до 40 мм/ч). Длина защищаемого участка периметра территории для таких извещателей составляет до 250 до 500 м. На рис. 2.4 показана установка ЧЭ извещателя «Газон-24».

Рис. 2.4. Варианты установки проводноволнового извещателя

Достоинства ПВСО следующие:

– независимость ЗО от профиля грунта и точное следование линии ограждения;

– простота и небольшая стоимость ЧЭ, в качестве проводников ЧЭ используется провод полевой телефонной связи П-274М, который обладает достаточной механической прочностью и стойкостью к атмосферным воздействиям и при этом хороший проводник;

– нечувствительность к сейсмическим и акустическим воздействиям (их можно устанавливать на ограждении вблизи автомобильных дорог или железнодорожных путей);

– простой монтаж, нетрудоемкое эксплуатационно-техническое обслуживание (в основном это периодическая проверка работоспособности и контроль за состоянием натяжения и крепления проводов линейной части).

Недостатки ПВСО следующие:

– чувствительность к помехам при воздействии электромагнитного поля на ЧЭ, если ЧЭ – распределенная приемная антенна;

– при смещении проводов относительно друг друга в результате их провисания параметры импульсного сигнала могут изменяться, например при нахождении в ЗО качающихся ветвей деревьев, кустарников и птиц.

Средства обнаружения на основе линии вытекающей волны

Чувствительный элемент на основе линии вытекающей волны представляет собой перфорированный кабель, в котором внешний проводник не обеспечивает полного экранирования центрального проводника, в силу чего определенная часть энергии передаваемого СВЧ-сигнала излучается через отверстия во внешнюю среду, а часть энергии проникает в приемный кабель такой же конструкции [26].

В передающем ЧЭ устанавливается режим, близкий к режиму бегущей волны, а в приемном ЧЭ наводится опорный сигнал. Электромагнитное поле, распространяющееся в окружающей среде, попадает на приемный ЧЭ, а затем в анализатор для выделения признаков проникновения. Проникновение нарушителя в ЗО извещателя приводит к изменению распространения электромагнитного поля за счет отражения от нарушителя электромагнитных волн. Отраженное от

нарушителя поле также принимается ЧЭ, вследствие чего происходит низкочастотная модуляция амплитуды и фазы сигнала связи. На рис. 2.5 показана структурная схема ЛВВ-извещателя.

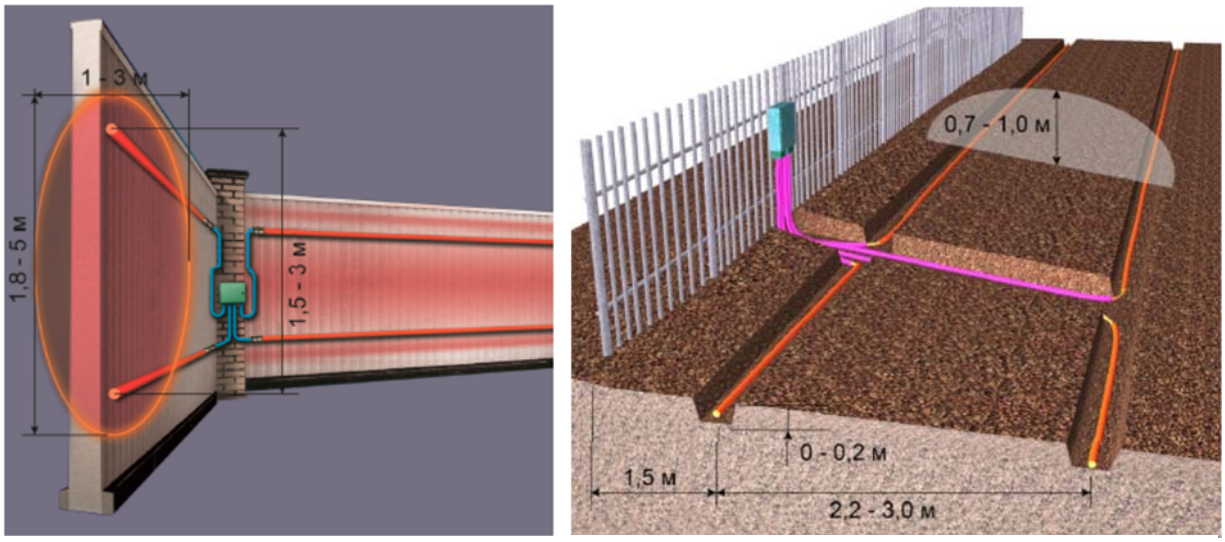


Рис. 2.5. Структурная схема ЛВВ-извещателя

Ширина ЗО ЛВВ зависит от чувствительности кабеля (вида его конструктивного исполнения), расстояния между кабелями, частоты сигнала, характера подстилающей поверхности, способа обработки сигнала и т. д. Зона обнаружения для извещателя ЛВВ по форме представляет собой цилиндр с основанием в виде эллипсоида. При этом большая диагональ эллипса составляет от 1,5 до 3 м, а меньшая – от 1 до 3 м. Чувствительные элементы для ЛВВ могут размещаться:

– на конструктивных элементах ограждения над поверхностью земли;

– на капитальном основании ограждения (кирпичном или бетонном) над поверхностью земли;

– один кабель – на ограждении (кирпичном или бетонном) над поверхностью земли, а другой кабель – под землей на глубине до 0,2 м;

– оба кабеля – под землей на глубине до 0,2 м и расстоянии до 3 м друг от друга.

Количество входов для подключения ЧЭ – один или два. Протяженность участка, блокируемого извещателем, составляет от 125 до

400 м. Например, зона обнаружения извещателя «Трезор-Р» ООО «НПЦ “Трезор”» (г. Москва) формируется двумя параллельными кабелями, закрепляемыми на ограждении и выступающими в качестве ЧЭ. В зависимости от необходимых размеров ЗО расстояние между кабелями может быть от 1,5 до 3 м. Смещение кабелей вверх или вниз по ограждению изменяет расположение и ЗО. Конструктивное расположение кабелей на ограждении позволяет использовать различные тактики охраны периметра территории объекта, в том числе защиты от подкопа.

Достоинства ЛВВ-извещателей следующие:

– при установке ЧЭ в грунт имеется возможность создания внешне не наблюдаемых рубежей охраны;

– при размещении ЧЭ на ограждении имеется возможность контроля проникновения через капитальные ограждения без дополнительного оборудования их металлическими козырьками и контроля разрушения капитальных конструкций (кирпич, железобетон, камень, дерево);

– формирование объемной ЗО, повторяющей рельеф местности и конфигурацию ограждений;

– устойчивость к дестабилизирующим факторам воздействия растительности высотой до 1 м и нечувствительность к мелким животным и птицам. В извещателе используется диапазон рабочих частот в пределах от 40 до 80 МГц, который позволяет обнаружить человека и пропустить мелких и средних животных;

– устойчивость к электромагнитным помехам;

– устойчивость к сейсмическим и акустическим помехам.

Недостатки ЛВВ-извещателей следующие:

– наличие вблизи ограждения крупных металлических предметов искажает конфигурацию зоны обнаружения;

– кабели для построения ЛВВ-извещателей отличаются большими массой и размерами;

– необходимость защиты оболочки: при любом повреждении диэлектрической оболочки может выйти из строя дорогостоящий кабель, поэтому его укладывают и заделывают в кабель-каналы, что значительно увеличивает стоимость монтажных работ;

– невозможность точной локализации места проникновения нарушителя: точность места проникновения обусловлена длиной плеча ЧЭ и обычно находится в пределах от 100 до 150 м;

– неравномерность чувствительности по длине кабеля; проблемы неравномерности чувствительности менее значимы при размещении кабелей на ограждении и наиболее остро ощутимы при их установке в почве. Кроме того, чувствительность сильно зависит от влажности почвы. Однако современные конструкции кабеля и новые методы зондирования ЛВВ многочастотным видеоимпульсом позволяют обеспечить равномерность чувствительности в 2 – 3 дБ;

– большая мощность потребления (десятки ватт), что ограничивает их использование с автономными источниками питания;

– высокая стоимость оборудования и монтажных работ.

Сейсмические средства обнаружения

Чувствительные элементы ССО устанавливаются непосредственно в почву и преобразуют микроперемещение слоев почвы под нарушителем в электрический сигнал ЧЭ (сейсмосигнал), анализируемый в блоке обработки сигналов [26]. Само понятие «вибросейсмический извещатель» означает то, что в вибрационном или сейсмическом извещателе зачастую используется одинаковый преобразователь результата физических воздействий в электрический сигнал. Например, вибрационный кабель, установленный на бетонном ограждении или в почве, полностью определяет назначение прибора – обнаружение пролома ограждения или подкопа. Другой термин – «сейсмоакустический» – обусловлен близостью физических процессов, происходящих при распространении акустических и сейсмических волн вдоль границы раздела двух сред с различной плотностью. Когда речь идет об измерении каких-либо параметров именно сейсмических сигналов, употребляют термин «сейсмометрический».

В настоящее время наблюдается активное развитие ССО в связи с открывшимися возможностями извлечения информации из сейсмосигналов за счет применения новой элементной базы, в том числе мощных микропроцессоров и адаптивных способов обработки сигналов. Развивается так называемая «концепция сейсмических информа-

ционных полей», определяющая совершенствование ССО на ближайшую перспективу. Классификация объектов сейсмического воздействия может осуществляться либо на основе анализа временной структуры сейсмосигнала, принимаемого одним преобразователем, либо на основе анализа принимаемых сигналов с нескольких ЧЭ ССО. В последнее время создаются многоканальные ССО нового поколения, способные обеспечить как обнаружение нарушителя, так и слежение за ним на основе использования методов пеленгации с помощью сейсмолокаторов.

Примером практического использования могут служить такие ССО, как «Годограф-Универсал» (СОГО «НИКИРЭТ»), сейсмическая станция обнаружения «Крот» (ГСО «Импульс Интернейшнл») и др.

В качестве ЧЭ в ССО обычно используется один из вариантов:

– кабель марки КТПЭДЭП специальной конструкции с усиленным и нормированным трибоэлектрическим эффектом;

– пьезоэлектрический сейсмочувствительный элемент;

– скрытый, маскируемый ЧЭ, который визуально не обнаруживает рубеж охраны, а пассивный принцип действия исключает возможность обнаружения ЧЭ по акустическим и электромагнитным полям, что фактически сравнивает шансы подготовленного и неподготовленного нарушителей;

– индукционные сейсмоприемники, представляющие собой проводящую обмотку и помещенный внутрь нее магнитный сердечник, который может свободно колебаться вдоль оси обмотки. При колебании магнита в катушке наводится напряжение, регистрируемое БОС.

Сейсмическое средство обнаружения «Годограф-СМ-С-1» (рис. 2.6) предназначен для организации скрытого рубежа охраны и обнаружения нарушителя, пересекающего рубеж шагом, бегом, ползком или перекатом. Извещатель позволяет организовать охраняемый рубеж как при наличии ограждения, так и без него. Один извещатель обеспечивает охрану двух последовательно расположенных участков периметра с выдачей извещений о тревоге и неисправности раздельно по каждому участку.

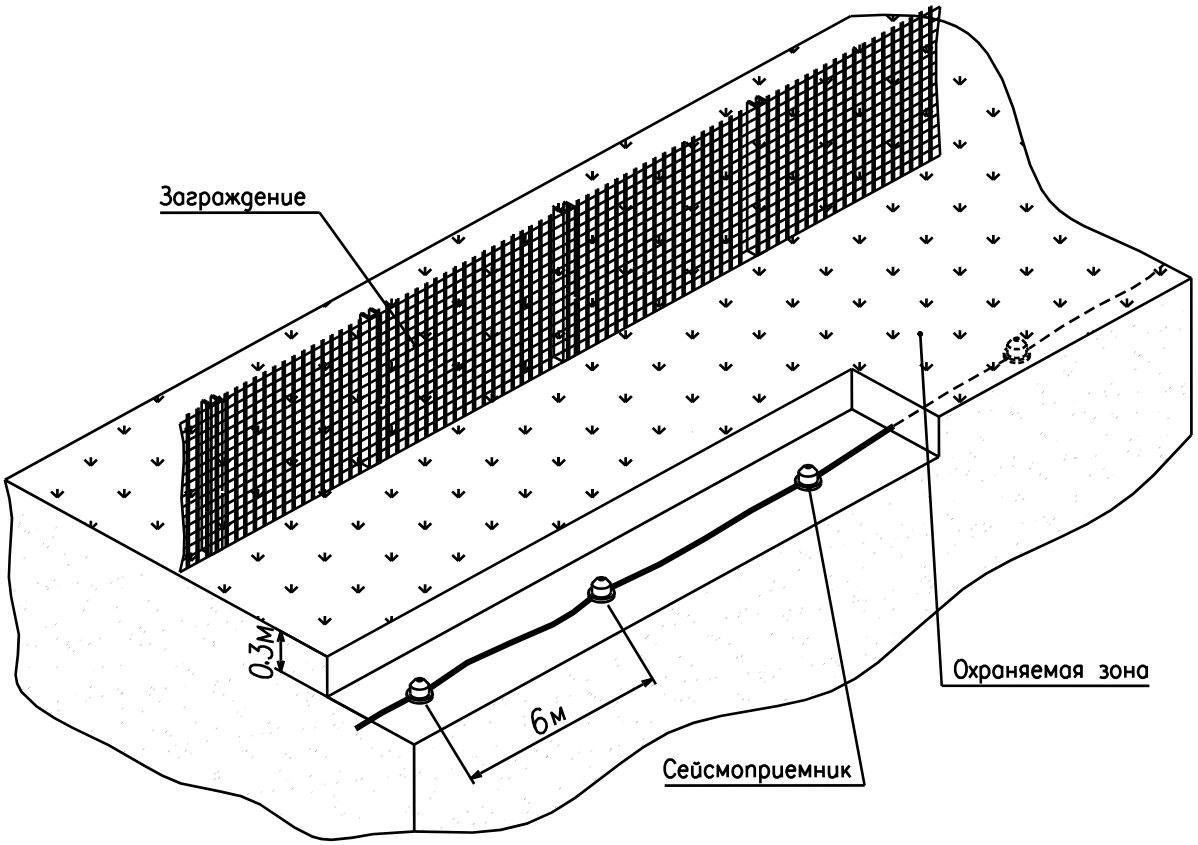


Рис. 2.6. Установка геофонов

При монтаже геофонов под землей надежно обнаруживается ползущий нарушитель или нарушитель, спрыгнувший с ограждения. Однако могут возникать ложные срабатывания, связанные с высокой чувствительностью геофонов. Установленный под землей геофон позволяет уверенно обнаруживать сигнал от идущего человека на расстоянии от 1,5 до 2,0 м, поэтому геофоны монтируют вдоль периметра на расстоянии 3,0 м друг от друга. Геофоны будут регистрировать движение транспорта или перемещение корней деревьев при порывах ветра на расстоянии нескольких десятков метров.

Достоинства ССО следующие:

– высокая степень скрытности установки ЧЭ;

– не содержат источников радиочастотного излучения, что препятствует обнаружению СО радиотехническими методами.

Недостатки ССО следующие:

– ЧЭ подвержены влиянию помех техногенного, метеорологического, биологического и прочего характера (для нейтрализации

транспортных и индустриальных помех используются специальные методы обработки сигналов подземных сенсоров);

– снижение чувствительности при промокании или промерзании грунта, высоком снежном покрове;

– высокая стоимость, в том числе и монтажа.

Манометрические средства обнаружения

Манометрический извещатель представляет собой электронный сенсор со специальными шлангами, заполненными незамерзающей жидкостью (антифризом), уложенными в землю на глубину от 0,25 до 0,3 м на расстоянии от 1,0 до 1,5 м друг от друга [26]. При попадании нарушителя в зону обнаружения извещателя создается градиент давления на грунт, который передается на ЧЭ, а сенсор измеряет дифференциальное изменение давления между ЧЭ (рис. 2.7).

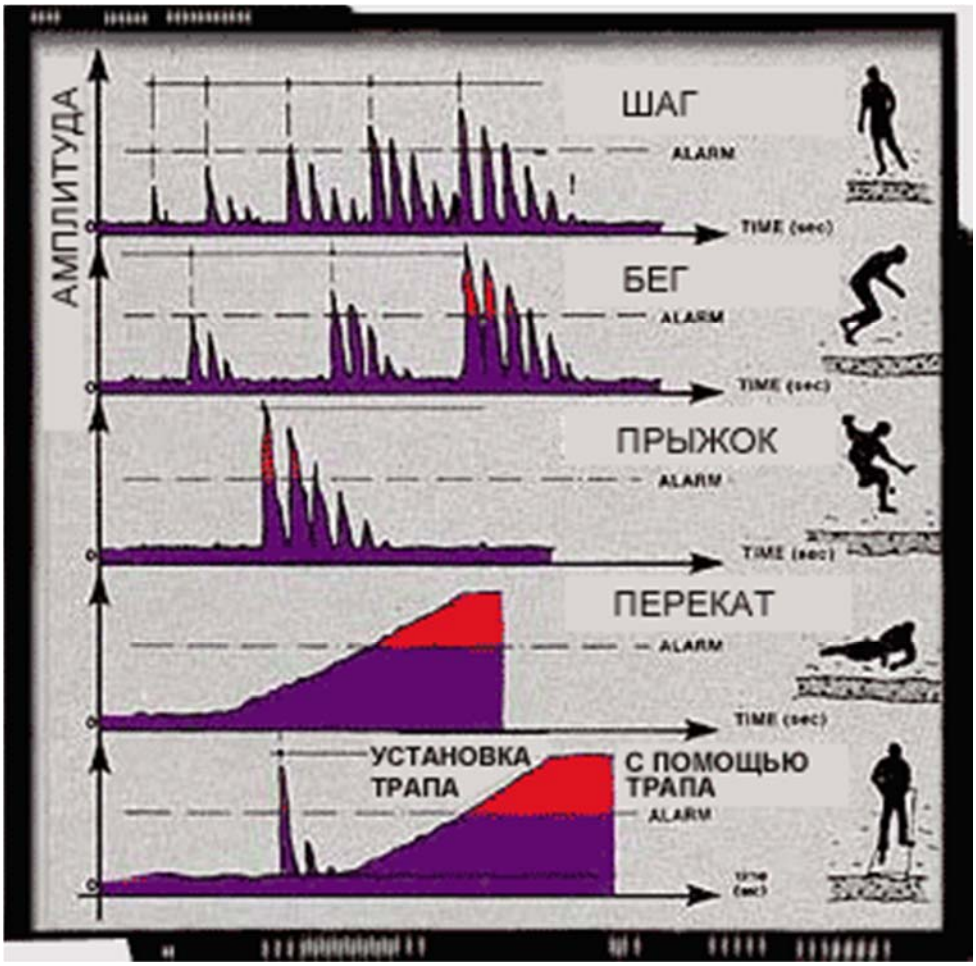


Рис. 2.7. Воздействие человека на ЧЭ и виды сигнала при пересечении ЗО

Изменение давления преобразуется в электрический сигнал, пропорциональный давлению, после чего он анализируется и сравнивается с заданными образцами сигналов, характерными для проходов нарушителей. В состав линейной части извещателей, устанавливаемых в почву, кроме шлангов и сенсоров входят компенсационные клапаны, обеспечивающие компенсацию давления в шлангах. В сенсоре размещаются высокочувствительные мембраны и микропроцессор для преобразования и анализа сигналов.

После обработки сигнал передается на блок управления, который с помощью встроенного интерфейса или релейных контактов формирует и передает тревожное сообщение. При изменении температуры и погодных условий имеется возможность с помощью динамической корректировки параметров автоматически менять уровень порога срабатывания извещателя.

Шланги могут быть уложены в почву произвольным способом благодаря их гибкости, что делает практически невозможным определение размеров ЗО нарушителем. Например, в СО марки КПТСО16-64 «ПАХРА» для организации подземных сейсмометрических рубежей используются протяженные гидравлические датчики давления. Средство обнаружения предназначено для защиты периметров территорий объектов и обнаружения нарушителя при взаимодействии его с ЧЭ.

Достоинства манометрических средств обнаружения следующие:

– надежное обнаружение нарушителей при пересечении ЗО шагом, бегом, прыжками, перекатыванием, с использованием трапов, досок или путем подкопа;

– высокая степень маскировки ЧЭ;

– поскольку ЧЭ устанавливается под землей, асфальтом или бетоном, то СО в большей степени подходит для объектов, где требуются определенная устойчивость к атмосферным и электромагнитным воздействиям (аэропорты, индустриальные и военные объекты), пожаро- и взрывобезопасность (нефтяные, газовые, химические предприятия), а также там, где важна эстетика (памятники архитектуры, музеи, коттеджи).

Недостатки манометрических средств обнаружения следующие:

– требуется большой объем подготовительных и монтажных работ при установке линейной части;

– сложность эксплуатации, особенно при замене ЧЭ;

– снижение обнаружительной способности при промерзании грунта или высоком снежном покрове;

– высокая стоимость.

Оптико-электронные средства обнаружения

Оптико-электронные средства обнаружения используют анализ электромагнитного излучения в оптическом диапазоне. Они подразделяются на активные и пассивные.

Активные ОЭСО регистрируют изменение отраженного потока собственного излучения (однопозиционные извещатели) или прекращение (изменение) принимаемого потока (двухпозиционные извещатели) энергии оптического излучения, вызванные нахождением нарушителя в ЗО. Пассивные ОЭСО регистрируют тепловое ИК-излучение от нарушителя.

Активные оптико-электронные средства обнаружения

Линейные активные ИК-извещатели, как правило, имеют двухблочную конструкцию и состоят из блока излучения (БИ) и блока приемника (БП), образующих оптическую систему. Блок излучения формирует поток ИК-луча (инфракрасный луч) с заданными характеристиками, который попадает на БП [26; 49; 50]. Появление в зоне обнаружения нарушителя или животного вызывает прерывание ИК-луча (или снижение его мощности). Последний попадает в БП, анализируется по уровню и длительности этого прерывания, и в соответствии с заложенным алгоритмом формируется тревожное извещение путем изменения сопротивления контактов, подключаемых к шлейфу сигнализации, или при размыкании релейных контактов.

Существуют активные извещатели, имеющие одноблочную конструкцию. В них оптическая система состоит из передатчика и приемника, объединенных в одном корпусе, и светоотражателя в виде катафота. В состав извещателей могут быть включены и зеркала как пассивные отражатели для изменения направленности инфракрасных

лучей. Входы БИ и БП обычно закрыты специальными фильтрами (иногда эти фильтры выполнены как единое целое с крышкой корпуса извещателя).

Активные ИК-извещатели могут быть однолучевыми или многолучевыми. Для многолучевых извещателей (более двух лучей) уменьшается вероятность ложного срабатывания, так как формирование сигнала тревоги происходит по схеме «И» при одновременном пересечении нарушителем всех лучей. ИК-излучение в данных типах ПСО монохромное для исключения взаимного помехового воздействия рядом расположенных двух и более ИК-барьеров.

Блок излучения генерирует импульсное излучение в виде одного или нескольких узконаправленных лучей в диапазоне волны от 0,8 до 0,9 мкм. Разбивка территории периметра объекта на отдельные участки должна быть проведена так, чтобы нарушитель не смог преодолеть периметр объекта без перекрытия ЗО извещателя. Таким образом, максимальное расстояние между конструкцией ограждения территории и ИК-лучом (линией между БИ и БП) должно быть меньше габаритов человека, не более 300 – 350 мм.

Основная сложность в эксплуатации активных ИК-извещателей – это высокий уровень ложных срабатываний от дестабилизирующих климатических факторов: тумана, дождя, снега и пр. Надежность функционирования извещателя в таких случаях обеспечивают многократным превышением энергии луча минимального порогового значения, необходимого для его срабатывания. Кроме того, серьезной помехой в работе извещателя может быть прямая засветка фотоприемника солнечными лучами. Такое может происходить, когда солнце низко стоит над горизонтом, на закате или рассвете.

Примером многолучевых активных ИК-извещателей служат извещатели ИО209-16-«СПЭК-7» в двух модификациях: ИО209-16/1-«СПЭК-7-2» (формирует два луча с интервалом 350 мм) и ИО209-16/2-«СПЭК-7-6» (формирует шесть лучей с интервалом 70 мм). Излучатели и фотоприемники смонтированы в единых корпусах (колоннах излучателей и фотоприемников). Такие извещатели используются для защиты ворот, калиток, блокирования доступа к окнам и дверям здания снаружи. Кроме того, извещатель ИО-209-16/2-«СПЭК-7-6» способен обнаруживать протянутую через ЗО часть тела человека,

например руку. Оба исполнения извещателя имеют рабочую дальность от 0,4 до 15 м (на открытом воздухе) и четыре значения чувствительности. В ИК-барьере имеется возможность использования до пяти извещателей. Колонны излучателей при таком использовании объединяются специальной линией синхронизации. Колонна фотоприемников может быть как синхронизирована, так и работать каждая со своими собственными настройками.

Достоинства активных ИК-извещателей следующие:

– извещатели нечувствительны к изменению характеристик теплового излучения окружающих объектов (фона) и возникающим тепловым помехам;

– обнаружительная способность не зависит от характеристик теплового излучения человека (нарушителя);

– максимальная эффективность достигается при установке извещателей поверх либо вдоль ровного ограждения, когда извещатель блокирует ограждение от перелаза и пролаза.

Недостатки активных ИК-извещателей следующие:

– высокая стоимость, особенно для эксплуатации на открытых площадках; требуют постоянного обслуживания, уязвимы с точки зрения подготовленного нарушителя;

– формируют только линейную ЗО; отчасти эта проблема может быть решена путем организации поверхностной ЗО за счет применения извещателей, формирующих несколько ИК-лучей, или построения ИК-барьера из нескольких извещателей (при этом размеры ЗО для первого варианта будут небольшими, а второй вариант потребует увеличения финансовых затрат);

– ложные тревоги вызывают мелкие и средние животные, мусор и листья при ветре, растительность, крупные птицы.

Пассивные оптико-электронные средства обнаружения

Пассивные ИК-извещатели предназначены для обнаружения нарушителя, перемещающегося в пределах зоны обнаружения, по инфракрасному излучению самого человека [26; 49]. Принцип действия пассивных ИК-извещателей основан:

– на регистрации разницы интенсивности инфракрасного излучения, исходящего от нарушителя, перемещающегося в ЗО, и фоновой обстановки;

– преобразовании ее в электрический сигнал;

– анализе полученного электрического сигнала с целью выделения признаков проникновения.

В пассивных ИК-извещателях обработка сигнала проводится аналоговыми методами, а в более сложных приборах используется цифровая обработка с помощью встроенного процессора. В качестве ЧЭ в пассивных ИК-извещателях применяют специальные приемники – пироэлементы (активные диэлектрики), преобразующие ИК-излучение в электрические сигналы.

При движении нарушителя в ЗО извещателя в существующем тепловом фоне прочих объектов излучение нарушителя поступает на оптическую систему извещателя и фокусируется на пироэлементе. Кроме того, аналогичным образом на пироэлементе оптической системы фокусируется и фоновое ИК-излучение. Пироэлемент вырабатывает электрический сигнал, пропорциональный разностному ИК-потоку от двух пироплощадок. Далее электрический сигнал поступает в БОС, где формируется извещение о тревоге, если изменение разностного теплового пятна превышает установленный порог.

Основные характеристики пассивных ИК-извещателей в соответствии с ГОСТ [49] следующие:

– диапазон обнаруживаемых скоростей перемещения нарушителя составляет от 0,1 до 5,0 м/с;

– максимальная рабочая дальность действия – максимальное расстояние, на котором извещатель обнаруживает движение нарушителя;

– чувствительность – извещатель должен сформировать извещение о тревоге при перемещении нарушителя на расстоянии не более 3 м.

Пассивные ИК-извещатели при эксплуатации весьма чувствительны к действию множества дестабилизирующих факторов. Для периметральных средств охраны количество и степень влияния таких факторов значительно выше, чем для извещателей в закрытом помещении. Для уменьшения вредного воздействия на извещатели атмосферных осадков и засветок от солнечных лучей применяют защитные козырьки.

Эксплуатация пассивных ИК-извещателей на открытых площадках сопряжена со значительными трудностями:

– высокий уровень ложных тревог. При снижении чувствительности для уменьшения числа ложных тревог происходит снижение обнаружительной способности и повышение вероятности пропуска нарушителя;

– сложности с ориентацией ЗО: необходимо одновременно учитывать как тепловые и оптические помехи, так и вероятное направление перемещения нарушителя;

– высокая трудоемкость работ по эксплуатационно-техническому обслуживанию извещателей.

Преимущество пассивных ИК-извещателей – относительно низкая стоимость.

Недостатки пассивных ИК-извещателей следующие:

– повышенная чувствительность к оптическим засветкам;

– низкая устойчивость к внешним атмосферным факторам;

– дальность действия в условиях тумана или сильного снегопада уменьшается до 30 %;

– импортные пассивные ИК-извещатели в основном отвечают требованиям отечественного национального стандарта, но не в полной мере соответствуют параметрам устойчивости к воздействию низких температур, диапазону обнаруживаемых скоростей и коммутационным параметрам выходных реле.

В целом из-за таких особенностей пассивных инфракрасных ПСО их не рекомендуется применять для защиты открытых площадок и периметров охраняемых территорий.

Вибрационные средства обнаружения

Вибрационные извещатели предназначены для обнаружения нарушителя по создаваемым нарушителем вибрациям (деформациям) защитного ограждения при попытке его преодоления на участке периметра охраняемого объекта [26]. Среди различных типов линейных извещателей вибрационные извещатели – одни из самых эффективных по надежности обнаружения и погонной стоимости. Вибрационные извещатели устанавливаются на «мягкие» ограждения из некапитальных конструкций (рис. 2.8), например на металлическую сетку, колючую проволоку, АКЛ и пр.

Рис. 2.8. Установка вибрационного извещателя

Извещатели этого класса обнаруживают нарушителя при его попытке перелезть через ограждение, при разрушении или демонтаже полотна ограждения. К достоинствам вибрационных извещателей относятся:

– возможность установки ЧЭ с учетом геометрии участков защищаемого периметра. Величина угла поворота ограничена лишь допустимым радиусом изгиба самого ЧЭ;

– размеры ЗО ограничены размерами контролируемого ограждения.

Недостатки и ограничения вибрационных извещателей следующие:

– необходимость регулярного контроля параметров настройки извещателя, так как свойства ограждения могут заметно изменяться при резких повышениях и понижениях температуры, а также при смене сезонов;

– высокие требования, предъявляемые к качеству монтажа как самого ограждения, так и ЧЭ (крепеж кабеля к ограждению, монтаж соединительных муфт и т. д.). Если в пределах одной ЗО ограждение имеет участки с различной чувствительностью (например, с разным усилием натянута металлическая сетка, с разным качеством устойчивости установлены опоры, кронштейны козырька и т. п.), настроить извещатель практически невозможно;

– ограниченность применения, т. е. извещатели используют только на «мягких» (сетчатых) или легких металлических ограждениях; установка этих извещателей на «жестких» ограждениях (железобетонных, кирпичных или конструкциях из пластика) не предусмотрена;

– возможность выдачи ложной тревоги при проезде тяжелой техники вдоль ограждения и ударах по нему камнем, палкой и т. д.;

– недопустимость прямого контакта ЧЭ с ветвями деревьев и больших кустарников.

С помощью такого извещателя можно блокировать жесткие ограждения или оборудовать дополнительные козырьки из металлической сетки или спирали АКЛ. Внутри класса вибрационных извещателей существуют разные типы, различающиеся по вариантам и диапазону определения полезных сигналов, связанных с колебаниями ограждения.

Вибрационные трибоэлектрические средства обнаружения

Чувствительный элемент таких извещателей – трибоэлектрический кабель, преобразующий механические вибрации в электрический сигнал. Кабель крепят либо непосредственно к ограждению, либо к специальному легкому металлическому козырьку над ним [26]. Сигналы с кабеля обрабатываются БОС, который в соответствии с заданным алгоритмом работы формирует тревожные извещения.

Для отечественных извещателей применяется в качестве ЧЭ кабель со спиралевидным центральным проводником (типа КТВ). Кроме того, активно используются экранированные кабели (типа ТПП 10×2×0,5), сохраняющие свои свойства при эксплуатации в уличных условиях в течение всего срока и обладающие «паразитным» трибоэффектом.

Принцип функционирования извещателя следующий. Два проводника размещаются между диэлектриком (полиэтилентерефталатной пленкой) и экраном внутри коаксиального кабеля. При локальных деформациях под воздействием вибрации создается небольшое электрическое поле между центральным проводником и экраном за счет трений диэлектрика и полиэтилентерефталатной пленки. Из-за смещений кабеля сенсорные проводники оказываются под воздействием изменяющегося электрического поля, образуется разность потенциалов, воспринимаемая специальным анализатором. Чувствительность к вибрациям и деформациям, вызванным нарушителем, в специализированном трибоэлектрическом кабеле является нормированным параметром. При этом чувствительность в специализированном кабеле значительно выше и стабильнее, чем в телефонном кабеле ТПП. Это позволяет реализовать монтаж ЧЭ по ограждению высотой от 2 до 3 м за один проход, при этом крепление кабеля к ограждению и прокладка осуществляются в стандартном металлическом коробе, что повышает вандалоустойчивость. Допускается прокладка в этом же коробе как шлейфа самого извещателя, так и прочих кабелей связи и цепей электропитания ПСО.

Для извещателя со стандартным телефонным кабелем («Трезор», «Гюрза», «Мурена», «Микрос-102») рекомендуется проводить двойную, многопроходную (до шести проходов) или «синусоидальную» прокладку ЧЭ по ограждению, что значительно увеличивает трудоемкость монтажных и пусконаладочных работ, а также усложняет проведение обслуживания ПСО.

Длина кабельного ЧЭ ограничена, поэтому такой тип ПСО позволяет защищать участки периметра охраняемой территории из двух независимых частей (плечей) ограждения общей длиной до 500 м при высоте ограждения до 1 м. Однако при повышении высоты ограждения до 2,5 – 3 м длина защищаемого участка периметра территории, блокируемого одним СО, сокращается в два-три раза.

Специализированный извещатель охранный трибоэлектрический «Гюрза-035ПВЗ» отличается от аналогов тем, что оболочка ЧЭ выполнена из специального ПВХ-пластиката. При этом такое изделие может быть использовано для защиты ограждения, расположенного

во взрывоопасных зонах, благодаря применению искробезопасных электрических цепей и специальных кабелей для ЧЭ. Извещатель имеет маркировку «2ExicIIB T6X».

Низкое энергопотребление извещателей типа «Гюрза» различных модификаций – их достоинство: ток в режиме «Охрана» составляет 1,5 мА, в режиме «Тревога» – 0,6 мА; извещатели имеют также и широкий диапазон питающих напряжений – от 8 до 35 В. Срок эксплуатации – не менее 10 лет. Особенность извещателя «Гюрза-070ПЗ» – возможность создания двух зон обнаружения одним извещателем («Вправо – Влево» или «Козырек – Полотно»), при этом длина каждого плеча ЧЭ – до 500 м.

Кроме того, такой извещатель может быть смонтирован на ограждениях различных типов. Он обладает высоким уровнем защиты от воздействия дестабилизирующих факторов, в первую очередь электромагнитных и вибрационных помех. В специальном исполнении извещатель имеет диапазон рабочих температур от –50 до +70 °С.

Основное отрицательное качество трибоэлектрических ПСО – использование в качестве базового принципа действия паразитного эффекта, который вносит существенные ограничения в функциональные возможности извещателя. Диапазон регистрируемых извещателем частот, как правило, не превышает 80 – 400 Гц, в более высокочастотной области присутствует собственный шум анализатора сигналов. Этим объясняется тот факт, что попытка нарушителя перелезть через ограждение (низкочастотное воздействие) отечественными вибрационными ПСО выявляется более надежно, чем механическое воздействие режущим инструментом (высокочастотное воздействие). В силу данного обстоятельства для организации эффективной защиты от разных способов преодоления ограждения, в том числе путем механического воздействия режущим инструментом и разрушения ограждения через создание в нем проломов, рекомендуется при монтаже извещателя укладывать кабели на ограждении зигзагом или выполнять несколько проходов, что значительно снижает дальность защищаемого участка периметра, а также увеличивает трудоемкость монтажных работ.

Вибрационные микрофонные средства обнаружения

Вибрационные микрофонные ПСО предназначены для обнаружения нарушителя по создаваемым им вибрациям капитального по своей конструкции (кирпич, бетон) инженерного ограждения при попытке преодоления ограждения и несанкционированного проникновения на охраняемый объект [26]. Физический принцип действия таких СО основан на регистрации механических вибраций или деформаций полотна ограждения, которые возникают при попытках нарушителя произвести пролом или преодолеть капитальное ограждение. Чувствительный элемент для таких ограждений представляет собой специально разработанный электромагнитный микрофонный кабель, способный преобразовывать механические деформации или вибрации в электрические сигналы. Такой кабель закрепляют непосредственно на ограждении или специальном металлическом козырьке. Сигналы поступают в блок обработки, в котором по заданному алгоритму происходит формирование тревожного извещения.

В микрофонном кабеле проводники размещаются в магнитном поле гибкого магнитного полимера. Локальные деформации, вызванные вибрацией защищаемого ограждения, приводят к перемещению гибкого магнитного полимера относительно проводников кабеля. Такие перемещения и являются причиной возникновения переменного магнитного поля, которое, в свою очередь, индуцирует напряжение в проводниках кабеля.

Общий недостаток таких ПСО – однопроходная схема монтажа кабеля на ограждении защищаемого участка периметра территории объекта. Микрофонный ЧЭ отличается высокой точностью воспроизведения вибраций ограждения и высоким соотношением сигнал/шум из-за малого сопротивления.

Вибрационные средства обнаружения с локализацией места воздействия на основе импульсного рефлектометра

Во всех типовых трибоэлектрических системах защиты ограждений периметров территорий к одному БОС подключается от одного до двух чувствительных элементов. Для этих участков устанавливается единая чувствительность по всей длине [26]. Место проникнове-

ния нарушителя (его воздействие на ограждение) определяется с точностью до зоны, определяемой началом и концом ЧЭ. Основа качественного функционирования всех типов вибрационных периметровых средств – конструктивное качество выполнения ограждения. Чем больше длина защищаемого участка периметра ограждения, тем больше происходит ложных тревог. Одна из главных проблем типовых ЧЭ трибоэлектрических систем, применяемых на некапитальных (гибких) ограждениях, – подверженность их ложным тревогам во время сильных порывов ветра и дождя. Локальное возмущение, вызванное нарушителем, сравнивается с шумом (энергией), аккумулированным по всей длине ЧЭ, а при климатических «возмущениях» уровень шума очень высок.

Конструктивное исполнение ЧЭ в виде коаксиального кабеля позволяет регистрировать попытки преодоления нарушителем ограждения с помощью проводной локации, с использованием принципов работы импульсных рефлектометров. Деформация кабеля приводит к изменению формы зондирующих импульсов рефлектометров. По задержке и изменению формы импульсов в БОС возможно определить характер разрушающих воздействий или способ проникновения, а также локализовать место проникновения.

При отсутствии деформаций на ограждении возвратившийся сигнал формирует картину распределения шумов в кабеле в спокойном состоянии (норма). Это аналогично распределению сигнала от неподвижных объектов, таких как здания, в обычном радаре. В кабельный ЧЭ подается зондирующий импульс, который создает электромагнитное поле внутри специализированного коаксиального кабеля между центральной жилой и оплеткой. В данном поле оказываются сенсорные проводники, расположенные в каналах около внешней оплетки. Любая механическая деформация или вибрация сенсоров приводит к отражению части энергии импульсов обратно в приемник. Временная задержка между началом импульсов и приемом отраженного от деформированного участка сигнала определяет (локализует) расстояние, которое импульсы проходят в кабеле.

Достоинства вибрационных извещателей следующие:

– возможность выявления как преодоления ограждения нарушителем, так и его разрушения;

– отечественные вибрационные СО обладают существенно меньшим энергопотреблением, меньшей стоимостью, лучше подходят для эксплуатации в условиях низких температур, широкого диапазона питающих напряжений, обеспечивают ударостойкость.

Недостатки вибрационных извещателей следующие:

– отечественные вибрационные СО уступают зарубежным аналогам по чувствительности, удобству настройки и наличию сервисных функций;

– дестабилизирующие факторы и природные помехи, воздействующие на ограждение и непосредственно на ЧЭ, могут приводить к формированию ложных тревог;

– опыт эксплуатации показывает, что главные причины ложных срабатываний извещателей – сильный ветер и стаи крупных птиц на ограждениях;

– высокие требования к монтажу ЧЭ, качеству ограждения; качество функционирования вибрационных ПСО прямо зависит от правильного проектирования конструкции ограждения и аккуратности выполнения монтажа; ЧЭ подбирается под ограждение, а ограждение подбирается под ЧЭ;

– диапазон рабочих температур некоторых зарубежных изделий слишком узкий для использования в российских условиях (до –30 °С), что ограничивает их применение.

Волоконно-оптические средства обнаружения

По способу применения и определения нарушителя по физическому воздействию на ЧЭ ВОС аналогичны вибрационным извещателям. Однако типы ЧЭ ВОС по сравнению с обычными кабельными линиями обладают иными характеристиками и потребительскими свойствами. В качестве ЧЭ ВОС используется волоконно-оптический кабель, в котором локальные деформации, возникающие при механических вибрациях, преобразуются в изменение характеристик лазерного излучения, проходящего через оптическое волокно [26]. Кабель при монтаже крепится либо непосредственно к ограждению, либо к специальному легкому металлическому козырьку над ним. Изменение параметров лазерного излучения в кабеле анализируется в БОС, который в соответствии с прописанным алгоритмом формирует тревожное извещение при превышении за-

данного порога. Кроме БОС в состав извещателя входят оптический квантовый генератор и монитор.

К одному концу волоконно-оптического кабеля подключен миниатюрный полупроводниковый лазер. На противоположном конце кабеля установлен фотодиод (приемник), преобразующий оптический сигнал в электрический. Анализатор в БОС сравнивает принимаемый сигнал с эталоном, соответствующим невозмущенному состоянию ЧЭ (норма), и детектирует внешние воздействия на защищаемый участок ограждения периметра (сжатие, смещение, вибрация и пр.).

Волоконно-оптическое средство обнаружения состоит из следующих элементов:

– передатчика (светодиод или лазер);

– волоконно-оптического сенсорного кабеля – ЧЭ;

– волоконно-оптического кабеля связи (нечувствительного к воздействиям);

– приемника;

– процессора для обработки сигнала.

Среди отечественных разработок ВОС можно выделить извещатель «Ворон» производства компании «Прикладная радиофизика». Данный извещатель предназначен для формирования протяженных многозонных и многорубежных ПСО на основе волоконно-оптических кабелей, которые монтируются на деформируемые ограждения различного типа, а также в почву. Такой комплекс состоит из пультового аппаратно-программного оборудования и линейной части.

Принцип работы извещателя «Ворон» показан на рис. 2.9. В качестве ЧЭ в системе «Ворон» использован специальный многомодовый волоконно-оптический кабель типа КДВО-18И. От внешних воздействий кабель защищен полиэтиленовой оболочкой, которая позволяет функционировать извещателю при температурах до –65 ºС. Кабель усилен двумя стальными жилами с прочностью на разрыв 320 Н (32 кг). В модернизированных системах планируется использовать новый кабель КДВО-3Т («трос»), в котором ЧЭ защищен армирующей оплеткой из стальных жил, обеспечивающих прочность на разрыв до 6000 Н (600 кг).

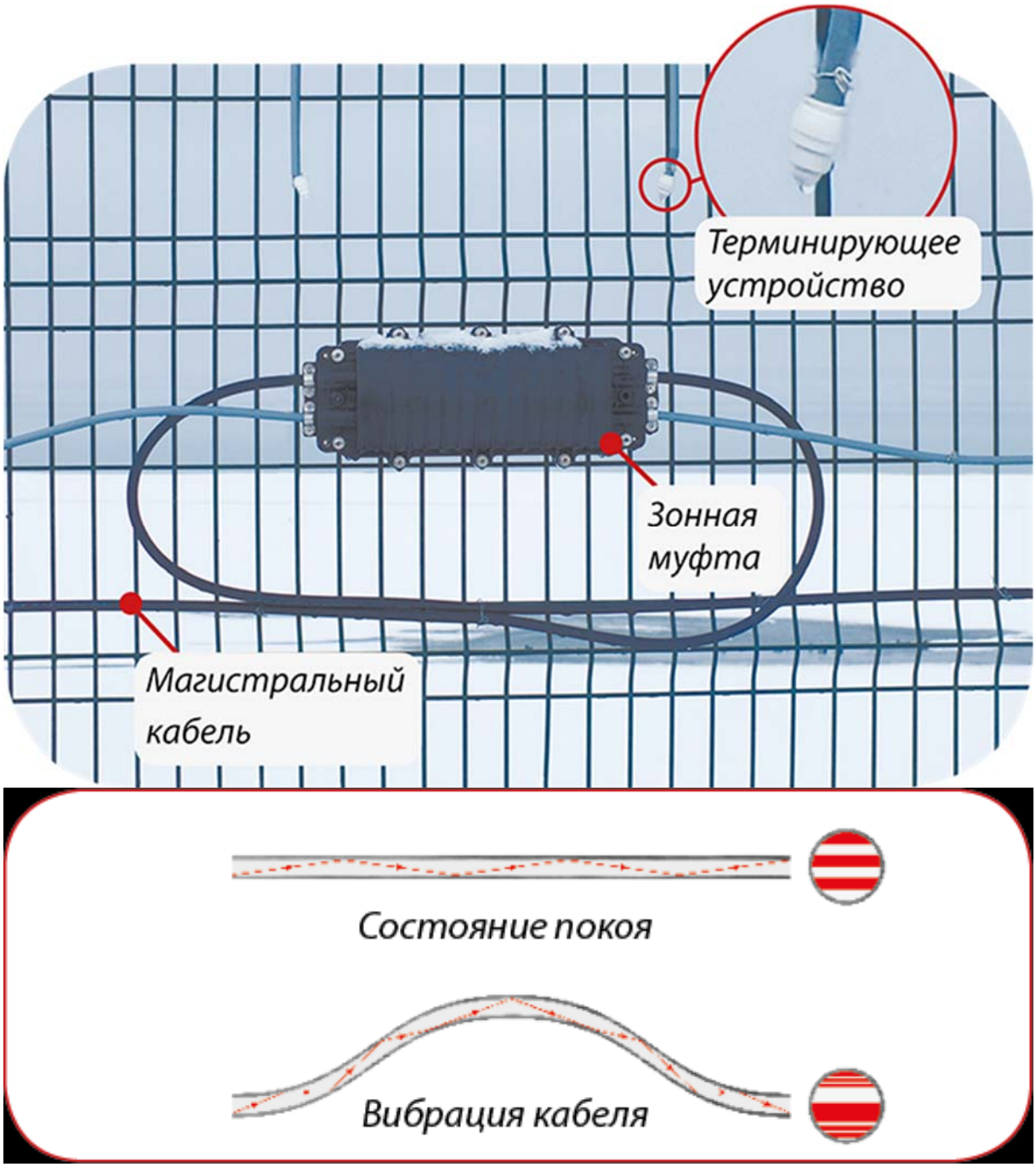


Рис. 2.9. Принцип работы системы «Ворон»

К особенностям системы «Ворон» относится применение волоконно-оптической линии связи кольцевой конфигурации, которая позволяет полностью отказаться от кабелей сигнализации и электропитания, прокладываемых вдоль периметра. В каждой ЗО устанавливается муфта «Ворон-2МС», соединяющая ЧЭ с волоконно-оптическим кабелем связи. Сварка обоих кабелей проводится так, что фазовые

изменения в ЧЭ трансформируются в амплитудную модуляцию в оптическом кабеле связи. Сигналы ЧЭ обрабатываются центральным процессором в БОС, который построен по принципу многопараметрического нейронного анализатора.

Анализатор «обучается» непосредственно в условиях эксплуатации объекта при пусконаладочных работах, обрабатывая и запоминая реальные отклики от ЧЭ, которые соответствуют как сигналам при проникновении нарушителя, так и фоновым сигналам помех. Блок обработки сигналов системы «Ворон» содержит блок приемопередатчиков, распределительные устройства, процессор, компьютер, клавиатуру и блок бесперебойного электропитания; БОС выполнен в виде стандартной стойки.

Достоинства волоконно-оптических ПСО следующие:

– невосприимчивость к электромагнитным и радиочастотным помехам, что позволяет использовать их в зонах с высоким уровнем таких помех;

– возможность применения для защиты не только ограждений, но и неогражденных участков территорий;

– высокая электробезопасность, ЗО с этим ЧЭ применяется на взрывоопасных объектах, а также под водой (пресной или морской);

– легкость монтажа и минимальное время пусконаладки, что позволяет оборудовать протяженные объекты за относительно короткое время;

– отсутствие излучения электромагнитной энергии (трудно обнаружить с помощью поисковой техники);

– минимальное энергопотребление при значительной удаленности от точки измерений;

– возможность эксплуатации в неблагоприятных атмосферных условиях (морской туман, кислотные пары, индустриальные выбросы, песок) и диапазоне температур от –40 до +70 °С. Оболочка ЧЭ обеспечивает защиту оптоволокна от УФ-излучения, влаги и т. п.;

– благодаря значительной длине ЧЭ возможен его монтаж на ограждении в несколько проходов, что позволяет более эффективно организовать охрану периметра, сохранив при этом достаточно протяженную ЗО;

– возможность организации охраны достаточно протяженного периметра с конфигурацией практически любой сложности и скрытой подземной установки;

– высокая коррозионная стойкость и работоспособность в агрессивных внешних условиях;

– высокая технологичность, возможность интегрирования в материал конструкции на стадии изготовления.

Недостатки волоконно-оптических ПСО следующие:

– использование нейросетевых алгоритмов обработки сигналов предполагает наличие персонального компьютера в качестве централизованного БОС большой вычислительной мощности;

– возможная потеря чувствительности при промерзании почвы;

– высокая удельная стоимость при защите периметра небольшой протяженности;

– необходимость использования ЧЭ в защитной оболочке при установке на ограждении, что повышает стоимость системы;

– сложность процедуры сращивания и ремонта ЧЭ в полевых условиях (требуется устройство для сварки волокон);

– высокая зависимость помехозащищенности и обнаружительной способности от качества «обучения» нейросети ПСО при установке, что требует высокой квалификации персонала.

Комбинированные и совмещенные средства обнаружения

Для создания эффективной защиты участков периметров необходимо использовать несколько рубежей охраны и извещатели, основанные на различных физических принципах [26]. Комбинированные извещатели для охраны участков периметров позволяют обнаруживать попытки проникновения нарушителя на защищаемый объект, снизить количество ложных срабатываний, а также выделять сигналы нарушителя на фоне помеховых воздействий (повысить обнаружительную способность ПСО). Достоинство таких извещателей – возможность одновременного обнаружения попыток проникновения нарушителя на охраняемый объект различными способами. Как правило, комбинированные извещатели состоят из двух или более ЧЭ, функционирующих согласно разным физическим принципам, и одного БОС, который имеет каналы обработки поступающих сигналов от каждого ЧЭ. Каждый ЧЭ, в свою очередь, имеет отдельную по конфигурации зону обнаружения.

Например, в совмещенном ПСО «Базальт» ОАО «НПК “Дедал”» используется два физических принципа обнаружения – вибрацион-

ный и емкостный. В состав данного ПСО включены два отдельных извещателя: емкостный «Сигма-07» и вибрационный «Дельфин-МП». Емкостный извещатель охраняет козырек защитного ограждения, а вибрационный – защищает полотно ограждения. Протяженность охраняемого рубежа может составлять от 3 до 250 м, а диапазон рабочих температур – от –50 до +50 °С.

Примером технической реализации комбинированного двухпозиционного извещателя может служить извещатель «ФОРМАТ-100» производства ЗАО «Охранная техника», который состоит из двухпозиционных извещателей: радиоволнового «БАРЬЕР-100» и активного инфракрасного «ИКС-01». Извещение о тревоге выдается при срабатывании обоих каналов обнаружения по схеме «И». Совмещение двух физических принципов обнаружения позволяет уменьшить ширину зоны обнаружения до диаметра ИК-луча, формировать предварительный сигнал тревоги по СВЧ-каналу обнаружения, имеющему более широкую зону. Благодаря характеристикам извещатель «ФОРМАТ-100» успешно применяется для защиты узких участков периметров территорий, расположенных вблизи автодорог. Длина зоны обнаружения извещателя составляет от 10 до 100 м. Извещатель обеспечивает непрерывную круглосуточную работу и сохраняет свои характеристики в температурном диапазоне от –40 до +85 °С.

В комбинированном извещателе «ЦИКЛОП-10/30» объединены радиоволновой однопозиционный извещатель «ЗЕБРА-30» и пассивный инфракрасный извещатель «ИД-12/ИД-40». Угол расходимости луча у извещателя «ЦИКЛОП-10» составляет около 60°, поэтому он выполняет функции защиты широких открытых площадок (например, автостоянок). У извещателя «ЦИКЛОП-30» угол расходимости луча составляет 3°, что позволяет организовать зону обнаружения в форме коридора. Длина зоны обнаружения может быть от 2,5 до 40 м.

Радиоволновой канал извещателя имеет высокие технические характеристики благодаря разделению зоны обнаружения на подзоны с индивидуальной настройкой чувствительности. Извещатель сохраняет свои характеристики при температуре от –40 до +65 °С.

Достоинства комбинированных извещателей состоят в том, что они обладают повышенной помехозащищенностью от воздействия внешних дестабилизирующих факторов.

Недостатки комбинированных извещателей заключаются в том, что для обнаружения и распознавания нарушителя используют одновременно несколько ЧЭ, в результате увеличивается стоимость извещателей и, соответственно, трудоемкость технического обслуживания. Комбинированные ПСО применяют для охраны особо важных объектов.

Быстроразворачиваемые комплексы

Быстроразворачиваемые комплексы относятся к активным средствам раннего обнаружения, так как могут формировать тревожное сообщение не только при попытке преодоления нарушителем основного ограждения защищаемой территории объекта, но и на подступах его к объекту [26]. Данное обстоятельство повышает эффективность реагирования наряда физической охраны на появление угрозы для объекта и позволяет оказать нарушителю достойное противодействие. Альтернативный вариант применения данных систем – временная охрана объектов, не имеющих ограждения и открытых площадок.

Быстроразворачиваемые комплексы имеют все преимущества линейных радиоволновых извещателей, но в то же время обладают большой мобильностью при их перемещении и оперативностью установки (монтажа) на охраняемом участке периметра территории или открытой площадке.

Особенности БРК следующие:

– формирование и выдача сигналов оповещения и их визуализация для оператора;

– развертывание на местности временного периметра охраны протяженностью до 200 м на один комплект;

– стоимость БРК в большинстве случаев превышает стоимость аналогичных по функциональной оснащенности периметровых средств охраны;

– автоматическое круглосуточное наблюдение и обнаружение нарушителя в режиме реального времени;

– передача информации по проводным каналам и (или) нескольким радиочастотным диапазонам на пункт управления;

– ограниченный до нескольких дней срок службы до замены элемента электропитания, при этом применение БРК в условиях низ-

ких температур дополнительно снижает данный параметр, в ряде типов БРК предусмотрено проводное электропитание.

Области применения БРК следующие:

– временная охрана дальних подступов к объекту;

– охрана временных стоянок подвижных объектов;

– создание временной защиты при выходе из строя части стационарных технических средств охраны периметра;

– создание временных рубежей охраны объектов;

– охрана временных объектов, полевых лагерей, локальных зон, площадок караульного помещения, контролируемых участков местности;

– охрана модульных пунктов управления доступом;

– временная организация транспортных шлюзов.

Комплекс охранной сигнализации «Радий-БРК» ЗАО «ЮМИРС», комбинированное устройство охранной сигнализации «Пахра» ООО «Спецмонтаж-безопасность», комплекс «Радиобарьер-МФ» ООО «Полюс-СТ» и другие имеют в своем составе извещатели различных принципов обнаружения, которые могут применяться как отдельно, так и совместно для охраны периметров различных объектов.

Достоинства БРК следующие:

– малозаметность и маскируемость;

– возможность установки на неподготовленной в инженерном отношении местности;

– мобильность, т. е. возможность быстрой установки (изменения конфигурации контролируемой территории) в зависимости от изменений условий эксплуатации;

– отсутствие или минимум технического обслуживания в течение времени работы.

Основной недостаток БРК – то обстоятельство, что они предназначены для охраны отдельных локальных участков территорий или открытых площадок в течение коротких промежутков времени.

Выбор и применение периметровых средств обнаружения

Выбор и применение перспективных ПСО, основанных на различных физических принципах, для охраны участков периметров защищаемых территорий и открытых площадок строятся на следующих основополагающих принципах [26]:

– возможность раннего обнаружения нарушителя, до момента разрушения ограждения и проникновения нарушителя непосредственно на объект;

– точное следование контурам периметра, отсутствие «мертвых», «слепых» зон;

– скрытая (маскируемая) установка ЧЭ;

– независимость параметров обнаружения от сезона (зима, лето) и климатических условий (дождь, ветер, град и т. д.);

– невосприимчивость к внешним дестабилизирующим факторам, таким как индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы;

– устойчивость к электромагнитным помехам в виде грозовых разрядов и источников мощных электромагнитных излучений.

Основные принципы функционального построения системы охраны периметров следующие [26]:

– комплексное или комбинированное обнаружение с использованием функционально законченных извещателей на основе различных физических принципов обнаружения с дополнением их видеонаблюдением;

– многозональность, позволяющая контролировать ограждение периметра территории путем разделения его на локальные участки;

– децентрализованная обработка первичной информации, которая поступает от ЧЭ.

При организации системы охраны периметра решаются следующие задачи:

– обеспечение совместной работы каналов на различных физических принципах в локальном участке периметра территории, а также учет сигналов от других ПСО, смонтированных на данном участке периметра территории;

– выбор ПСО, использующих различные физические принципы обнаружения нарушителя в зависимости от установленного типа ограждения;

– установка дополнительного оборудования для управления параметрами СОП при монтаже и регулировке.

Кроме того, при выборе средств ПСО необходимо организовать передачу информации:

– тревожных извещений с локального участка по двухпроводной линии или радиоканалу с указанием его адреса на местный пункт охраны объекта;

– служебных и тревожных извещений на ПЦН, радиоканал для передачи и обмена (протокол, работа в реальном режиме времени, работа при постановке активных помех, кодирование информации, выбор радиочастот и т. д.);

– с дублированием радиоканала (при необходимости).

Проектирование системы охраны периметра

Проектирование системы охраны периметров охраняемых территорий или открытых площадок объекта заключается в проведении следующих мероприятий [26]:

1) анализ возможных угроз и потенциальных способов преодоления нарушителем рубежей, разработка модели(ей) потенциального нарушителя;

2) обследование местности, анализа почвы (глинистый грунт, песчаный, болотистый, скальный, возможность произвести подкоп);

3) анализ климатических и погодных условий, возможности образования снежных заносов, определение их высоты (прежде всего у ограждения), выявление диапазона изменения температур, вероятности сильных ветров со скоростью более 25 м/с и осадков;

4) уточнение особенностей конструкционных элементов ограждений (материал, высота, повороты, изгибы);

5) оценка электромагнитной «зашумленности» периметра защищаемой территории (наличие различного вида индустриальных помех, близость высоковольтных линий электропередач и т. д.);

6) оценка информации о пересечении периметра подземными и надземными магистралями (канализационные и кабельные коммуникации, трубопроводы, эстакады и т. п.);

7) оценка количества и видов разрывов, пролазов или проломов в ограждении (целостность), а также автомобильных проездов, ворот, калиток, водопропусков и т. п.;

8) формирование требований к маскировке технических средств охраны периметра объекта и эстетических требований к ПСО;

9) оценка возможности физических нарядов службы безопасности по реагированию на тревожные извещения ПСО, квалификации персонала;

10) определение вида и комбинации технических средств охраны периметра объекта;

11) анализ возможностей (вариантов) использования ПСО и выбор наиболее приемлемой по критичному значению (например, степень защищенности или простота конструкции);

12) оценка финансовых возможностей (как правило, принято считать, что стоимость система охраны периметра не должна превышать 10 – 15 % от возможных потерь, вызванных проникновением нарушителя на охраняемый объект).

При выборе и использовании перспективных средств обнаружения, основанных на различных физических принципах, для охраны периметров огражденных территорий и открытых площадок особое значение имеет снижение влияния дестабилизирующих факторов и помех, усложняющих функционирование ПСО, и обеспечение высокой обнаружительной способности ПСО. Помеховыми и дестабилизирующими факторами принято считать следующие:

1) климатические: температура (от –60 до +60 °С), влажность, туман, дождь, гроза, снег, град, наледь, ветер, пыль, песок, солнечная радиация;

2) фауна: насекомые, птицы, животные;

3) флора: трава, кусты, деревья;

4) условия применения:

– дизайн периметра;

– перемещение вблизи периметра людей, животных, автомобилей, поездов и пр.;

– изгибы периметра по горизонтали и вертикали;

– характеристики почвы, конструкция и параметры ограждений (при наличии ограждений);

– наличие луж, ручьев, неровностей почвы, наличие или близость крупных предметов, близость различных коммуникаций;

5) промышленные помехи: мощные электроустановки, линии электропередач, радиостанции, сотовая связь, электрифицированный транспорт и т. д.

На специфических объектах число дестабилизирующих факторов может возрастать (химически активная среда, радиационное излучение и др.).

На разные ПСО, основанные на различных физических принципах, перечисленные факторы влияют по-разному. Например, насекомые никак не влияют на подавляющее большинство извещателей, но могут существенно нарушать нормальную работоспособность инфракрасных приборов, закрывая собой ЧЭ или создавая непрозрачную паутину.

В условиях вечной мерзлоты, постоянной подвижности почвы невозможно установить прочные опоры, не подверженные никаким движениям. Это особенно важно для извещателей, требующих точной юстировки или регулировки усилий натяжения ЧЭ.

Без ограничения доступа животных в ЗО большинства извещателей ПОС эффективность охраны будет очень низкой. Животные могут проникать внутрь или появляться вблизи подавляющего числа охраняемых объектов, особенно там, где есть для них пища. Подлезая под ворота и калитки, собаки или другие животные проникают на объекты. Чаще собаки перемещаются стаями и способны вызвать сигнал тревоги практически у любого средства с ЗО, примыкающей к земле ближе 0,5 м.

Кроме того, воздействие большинства помех и дестабилизирующих факторов может носить вероятностный, случайный характер. Конкретное помеховое воздействие, влияющее на характеристики извещателей ПСО, для данного объекта может происходить раз в год или раз в минуту. Например, если СО будет реагировать на проезд автомобиля, то срабатывание СО раз в месяц не критично. Если СО реагирует на пролет птиц один раз из десяти, а таких пролетов несколько сот в сутки, его установка недопустима. Если помехи происходят днем, когда средство снято с охраны, и отсутствуют вечером и ночью, то ими можно пренебречь. Частый случай, когда СО устанавливается на ограждение между двумя соседними периметральными смежными участками и может реагировать на подход с внешней стороны. Когда СО срабатывает по сравнительно редкому известному событию, например открывание ворот и прочее, этот фактор необходимо учитывать. Как правило, для систем охраны периметров

самыми существенными считаются 5 – 7 факторов помех, не считая погодных условий. С учетом этих факторов и выбирают ПСО.

Вариант применения СО напрямую связан с помеховыми факторами, которые могут влиять на работу ПСО. Наиболее распространенные для защиты участков периметров территорий и открытых площадок – варианты со следующими ПСО [26]:

1) вибрационные, емкостные и инфракрасные СО, защищающие верх ограждения;

2) инфракрасные и радиолучевые СО, установленные на полосе отчуждения;

3) вибрационные СО, смонтированные на сетчатых ограждениях.

Обычно в указанном порядке строят трехрубежные средства охраны периметров. На менее важных объектах применяют какой-либо один вариант, иногда – два.

Необходимые условия эксплуатации извещателей ПСО для применения указанных вариантов следующие:

– для первого: прочный забор, отсутствие примыкающих веток деревьев;

– для второго: выровненная, без ям и бугров, полоса отчуждения вдоль периметра шириной от 3 до 6 м, отсутствие на ней деревьев, кустов и высокой травы;

– для третьего: сетчатое ограждение, отсутствие примыкающих к нему деревьев, кустов и высокой травы.

При оборудовании периметра СО необходимо учитывать наличие ворот и калиток, крыш и стен зданий, переходов трубопроводов и коммуникаций над ограждением и под ограждением. В каждом конкретном случае может потребоваться отдельный подход к поставленной задаче.

Выбор и использование перспективных СО, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок основан на анализе уязвимостей средств обнаружения, вероятности обнаружения, количества ложных тревог, маскируемости, надежности, имитостойкости и универсальности. Опыт использования различных видов и типов СО показывает, что для обеспечения высокой надежности их функционирования при охране периметра каждого конкретного объекта следует приме-

нять наиболее эффективный в данных условиях физический принцип обнаружения.

Разработка проекта системы охраны периметра объекта обычно включает в себя:

– анализ потенциальных угроз и формирование моделей нарушителей;

– выделение на объекте охраняемых зон и участков;

– определение конфигурации системы охраны периметра в целом и ее отдельных компонентов;

– определение функциональных и технологических связей как внутри системы охраны периметра, так и с другими системами безопасности объекта;

– формирование различных вариантов построения системы охраны периметра;

– оценку эффективности вариантов построения системы охраны периметра;

– оценку стоимости вариантов построения системы охраны периметра;

– выбор варианта (вариантов) на основе критерия эффективность/стоимость;

– подготовку технических и конструкторских предложений для включения в техническое задание на создание (модернизацию) системы охраны периметра.

Одни из важнейших составляющих построения системы охраны периметра – модель угроз охраняемому объекту и модели нарушителей. Определение целей несанкционированного доступа на территорию объекта, модели наиболее вероятного нарушителя и наиболее вероятных сценариев его действий, типов проникновения дают возможность сформировать требования к инженерно-техническим средствам системы охраны периметра, при реализации которых возможно ее эффективное противодействие существующим угрозам и выполнение требований нормативных документов. Как правило, к системам охраны периметра объектов высоких категорий, критически важных и опасных объектов предъявляют следующие основные требования:

– каждый рубеж охраны должен состоять не менее чем из двух физических барьеров, каждый из которых оборудован своими средствами обнаружения;

– каждый рубеж должен включать в себя не менее чем два типа средств обнаружения, основанных на различных физических принципах.

Варианты построения системы охраны периметра для функционирования в простых условиях

Простые условия функционирования [26; 36] системы охраны периметра предполагают отсутствие: ограничений по площадям, на которых разворачиваются ПСО, пересечений периметра оврагами, реками, ручьями и так далее, влияния ЛЭП, зданий и сооружений, примыкающих к периметру; вблизи защищаемых участков периметра нет дорог; ПСО расположены на ровной поверхности, очищенной от травы, кустов, деревьев и фоновых металлических предметов; район установки системы охраны периметра малоснежный. Требуемая высота инженерных ограждений составляет не менее 2,5 м.

Физические барьеры ограждения периметра охраны строятся заново. Чувствительные элементы средств обнаружения подключают к БОС, которые размещают в специальных шкафах или в герметичном корпусе на физических барьерах. Кроме того, в специальных шкафах располагаются контроллеры нижнего уровня средств сбора и обработки информации (ССОИ), а также источники питания средств обнаружения.

Расстояние между участковыми шкафами определяется прежде всего:

– характеристиками ССОИ (допустимым расстоянием между контроллерами нижнего уровня);

– допустимой длиной шлейфов сигнализации;

– плотностью установки средств обнаружения;

– наличием дополнительного оборудования.

Расстояние между специальными шкафами составляет от 250 до 500 м. Магистральные линии связи между контроллерами нижнего и верхнего уровней, проходящие вдоль тропы обхода нарядов физической охраны, укладываются в лотки или короба. Типовой вариант размещения элементов СОП на рубеже охраны изображен на рис. 2.10 [36].

Шкафы участковые предназначены для следующих целей:

– размещение приборов и источников питания в условиях открытой местности;

– обеспечение пыле- и влагозащищенности;
– термоизоляция;
– контроль несанкционированного вскрытия;
– грозозащита и кроссировка размещаемого оборудования.

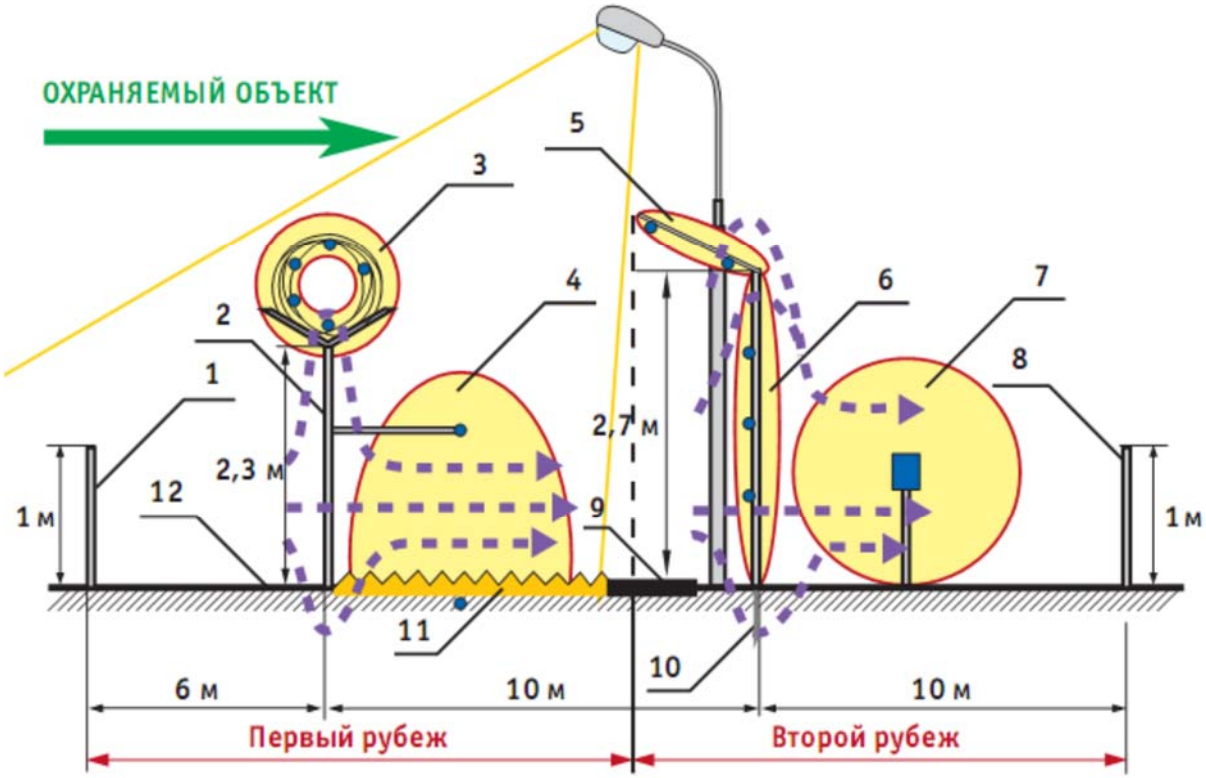


Рис. 2.10. Вариант построения фрагмента СОП, предназначенной для функционирования в простых условиях: *1* – внешнее предупредительное ограждение; *2* – первое основное ограждение с V-образным козырьковым ограждением и объемной АКЛ; *3* – ЗО вибрационного трибоэлектрического извещателя; *4* – ЗО проводноволнового извещателя; *5* – наклонное козырьковое ограждение и ЗО емкостного извещателя; *6* – второе основное ограждение и ЗО трибоэлектрического СО; *7* – ЗО двухпозиционного РВСО; *8* – внутреннее предупредительное ограждение; *9* – тропа наряда; *10* – противоподкопное ограждение; *11* – контрольно-следовая полоса; *12* – зона отчуждения

2.2. Требования по оснащению средствами охранно-тревожной сигнализации зданий и помещений

Техническими средствами охраны должны оборудоваться все места наиболее вероятного проникновения в помещения объекта (окна, двери, люки, вентиляционные короба и т. п.). Объекты (МПХИГ), за исключением класса Г3, рекомендуется оборудовать двумя и более

рубежами охранной сигнализации. Объекты класса Г3 допускается оборудовать одним рубежом ОС.

Требования по оснащению средствами охранно-тревожной сигнализации зданий и помещений соответствуют методическим рекомендациям [6], особо важных объектов и помещений – рекомендациям [27; 29], банкоматов и банковских устройств самообслуживания – рекомендациям [39]. Общие требования к системам охранно-тревожной сигнализации изложены в ГОСТ [30; 31; 53]. Требования к охранным извещателям в зависимости от их типов изложены в ГОСТ [43; 44; 45; 46; 47; 48; 49; 50; 54; 55; 56; 58; 59; 60; 62]. Требования к приемно-контрольным приборам представлены в ГОСТ [52]. Рекомендации по применению охранных извещателей в зависимости от их типов изложены в методических пособиях и рекомендациях [32; 33; 34; 35].

В зависимости от вида предполагаемых угроз объекту (МПХИГ) должна быть предусмотрена блокировка следующих элементов строительных конструкций защищаемого объекта: внешние входные двери – на открывание и разрушение (пролом); некапитальные наддверные проемы – на разрушение (пролом); ворота – на открывание и разрушение (пролом); остекленные конструкции – на открывание, разрушение, разбитие; стены, перекрытия и перегородки, не удовлетворяющие требованиям нормативных документов, или стены, перекрытия и перегородки, за которыми размещаются помещения других собственников, позволяющие проводить скрытые работы по разрушению стены, – на разрушение (пролом); решетки, жалюзи и другие защитные конструкции, установленные с наружной стороны оконного проема, – на открывание и разрушение; вентиляционные короба, дымоходы, места ввода/вывода коммуникаций сечением более 200×200 мм – на разрушение (пролом).

При блокировке входных дверей объектов (МПХИГ) всех классов, за исключением классов В3 и Г3, рекомендуется использовать ТСО, обеспечивающие возможность обнаружения несанкционированных действий на ранних этапах их совершения (извещатели раннего обнаружения). Внутри помещений должна быть предусмотрена защита объема посредством объемных извещателей различного физического принципа действия, обеспечивающих обнаружение проникновения (перемещения).

В помещениях значительных размеров со сложной конфигурацией, в которых для защиты всего внутреннего объема требуется большое количество приборов объемного обнаружения (ПОО), допускается блокировать только места возможного проникновения. Для защиты отдельных особенно ценных предметов (сейфов, металлических шкафов и др.) должны использоваться охранные извещатели, работающие на различных физических принципах обнаружения. В обоснованных случаях допускается блокирование остекленных конструкций с помощью объемных, поверхностных или линейных извещателей различных физических принципов действия.

При невозможности защиты входных дверных проемов (тамбуров) ТСО, обеспечивающими возможность обнаружения несанкционированных действий на ранних этапах их совершения, рекомендуется в дверном проеме между основной и дополнительной дверью устанавливать пассивный оптико-электронный извещатель, обнаруживающий перемещение нарушителя (ПОО с зоной обнаружения типа «штора»). Для исключения формирования возможных ложных сигналов «Тревога» при взятии объекта (МПХИГ) под охрану шлейфы сигнализации устройств оконечных объектовых СПИ должны обеспечивать задержку «на взятие», если устройство взятия/снятия объекта под охрану находится внутри защищаемого помещения.

Рекомендуется блокировать стены, перекрытия и перегородки, с которыми возможно проводить скрытые работы по их разрушению или на которые можно оказывать ударное воздействие, если за ними размещаются помещения других собственников.

Особенности построения рубежей ОС. Для каждого рубежа ОС рекомендуется выделять отдельный шлейф сигнализации, контролирующий отдельную зону или элемент объекта (МПХИГ). Не рекомендуется блокировать одним шлейфом сигнализации более пяти соседних помещений.

Конкретные типы извещателей выбирают после обследования объекта (МПХИГ) в зависимости от класса, на основании анализа особенностей объекта, наиболее вероятных типов криминальных угроз, в зависимости от помех, внешних воздействующих факторов и стоимости. Основные типы извещателей, обеспечивающих защиту помещений объекта (МПХИГ) и его конструкций от предполагаемого (возможного) способа криминального воздействия, приведены в табл. 2.2.

Таблица 2.2

Определение типа извещателей

Способ воздействия	Тип извещателя (принцип действия)
Проникновение через ограждение 2 – 4-го класса защиты следующими способами: разрушение полотна, подкоп, перелаз, отгиб	Комбинированно-совмещенный с четырьмя каналами обнаружения (емкостный, вибрационный, сейсмический, радиоволновой)
Проникновение через неогороженный, слабозащищенный периметр или периметр 1-го класса	Линейный радиоволновой, линейный оптико-электронный (активный инфракрасный)
Проникновение на открытую площадку с материальными ценностями, подход к охраняемому объекту (здание, складское помещение)	Объемный радиоволновый
Проникновение в технологические колодцы, выходы воздуховодов подземных сооружений, туннелей, площадок, огороженных сеткой типа «рабица» или металлическим прутком	Объемный радиоволновой двухпозиционный
Разрушение остекленных конструкций (разбитие, вырезание, выдавливание, выворачивание, терморазрушение)	Поверхностный ударно-контактный, поверхностный звуковой (акустический)
Разрушение остекленных конструкций (разбитие, вырезание, выдавливание, выворачивание, терморазрушение) и проникновение в охраняемое помещение	Поверхностный совмещенный (акустический и пассивный инфракрасный), объемный совмещенный (акустический и пассивный инфракрасный)
Разрушение деревянных конструкций (пролом, выпиливание, сверление, разборка)	Поверхностный вибрационный (пьезоэлектрический)
Разрушение металлических конструкций (разрубание, раздвигание, выкусывание, выпиливание, высверливание, выдавливание, прожигание)	Поверхностный вибрационный (пьезоэлектрический)
Открывание конструкций (дверей, оконных рам)	Точечный магнитоконтактный
Проникновение в помещение через двери, оконные рамы	Поверхностный оптико-электронный (пассивный инфракрасный) – «защитная штора»

Окончание табл. 2.2

Способ воздействия	Тип извещателя (принцип действия)
Перемещение во внутреннем объеме помещения	Объемный ультразвуковой, объемный оптико-электронный (пассивный инфракрасный), объемный радиоволновой, объемный комбинированный: пассивный инфракрасный плюс радиоволновой; пассивный инфракрасный плюс ультразвуковой; пассивный инфракрасный плюс видео
Пересечение во внутреннем объеме помещения ловушек, барьеров	Линейный оптико-электронный (активный инфракрасный), оптико-электронный пассивный
Касание, приближение к картинам (с металлической фольгой на подрамнике), электропроводящим предметам (металлическим шкафам)	Поверхностный емкостный
Проникновение в небольшие замкнутые объемы (витрины, шкафы, киоты и т. п.)	Объемный ультразвуковой
Перемещение персонала и посетителей в зону охраны отдельных предметов и групп предметов	Объемный комбинированный (пассивный инфракрасный плюс радиоволновой) для установки на потолке
Разрушение стенок сейфа взломом, сверлением, выворачиванием	Поверхностный вибрационный (пьезоэлектрический)

Техническими средствами охраны оборудуются все помещения с постоянным или временным хранением ценностей, а также все места вероятного проникновения нарушителя в здания (помещения) объектов (МПХИГ).

Тревожная сигнализация

В целях обеспечения безопасности посетителей и персонала объектов (МПХИГ), а также по заданию и с согласия собственника объекта, с целью обеспечения охраны общественного порядка на охраняемых объектах и прилегающих территориях, недопущения противоправных криминальных действий объекты и МПХИГ оборудуются тревожной сигнализацией. Тревожная сигнализация выполня-

ет задачи формирования сигналов «нападения» для оперативной передачи сообщений на ПЦО (разбойные нападения, хулиганские действия, угрозы и др.). Тревожной сигнализацией оборудуются объекты как в обязательном порядке (согласно требованиям нормативных документов), так и по инициативе собственников объектов.

Требования стандартов к извещателям тревожной сигнализации изложены в ГОСТ и аналитическом обзоре [57; 63]. Тревожная сигнализация при своем функционировании не должна создавать помех (в частности, радиопомех), которые могли бы оказать влияние на работу ТСО и других технических средств и систем на охраняемом объекте. Тревожная сигнализация должна соответствовать требованиям стандартов по обеспечению электромагнитной совместимости. Технические средства тревожной сигнализации на объекте должны устанавливаться:

– в комнатах хранения оружия и боеприпасов, кассах, сейфовых комнатах, хранилищах, кладовых и предкладовых;

– на охраняемой территории в помещении КПП, у центрального и запасных выходах (выездов);

– в торговых залах объектов торговли, где расположены защищаемые ценности;

– кабинетах руководителей объекта по согласованию с собственником;

– на постах и в помещениях охраны, расположенных в здании, строении, сооружении и на охраняемой территории;

– в помещениях консьержей в подъездах жилых домов (по согласованию с собственниками);

– других местах по требованию руководителя (собственника) объекта или рекомендации сотрудников вневедомственной охраны или охранной организации [6].

Кнопки (радиобрелоки) тревожной сигнализации должны подключаться на ПЦО охранной организации отдельным шлейфом без права снятия с охраны. Кнопки тревожной сигнализации на объектах (МПХИГ) рекомендуется устанавливать:

– в районе входной двери для объектов особой важности и категорий А1, А2, А3;

– районе сейфов для хранения огнестрельного оружия, ювелирных изделий и иных ценностей;

– иных местах по требованию собственника или рекомендации сотрудников вневедомственной охраны или охранной организации.

Кнопки тревожной сигнализации (КТС) рекомендуется размещать с учетом удобства их нажатия незаметно для нападающего. Кнопки тревожной сигнализации размещают скрытно, в местах, незаметных (замаскированных) для посторонних лиц, недоступных для детей и домашних животных. Кнопки могут быть ручными, ножными или комбинированными. Например, педали, устанавливаемые под крышкой стола, можно нажимать рукой или коленом. Места хранения ценностей, особо значимых предметов (в квартирах класса В1), драгоценных металлов, камней и изделий из них, денежных средств (металлические шкафы или сейфы, столы операционистов, кассовые аппараты, витрины, лотки, торговые прилавки) рекомендуется оборудовать специальными техническими средствами (СТС, датчики-ловушки), формирующими сигналы тревоги независимо от действий персонала объекта при попытках нарушителя завладеть датчиками. Специальные технические средства должны включаться в шлейфы тревожной сигнализации объекта. Допускается совмещать СТС с химловушками. Перед анализом и выбором вариантов оснащения объектов и МПХИГ оборудованием ТСО необходимо проконтролировать выполнение собственником объекта требований предписания (акта обследования) по инженерно-техническому укреплению элементов строительных конструкций зданий и ограждений территории (при наличии). Выполнение комплекса мероприятий по инженерно-техническому укреплению объектов (МПХИГ) позволяет:

– сократить виды и типы применяемых для обеспечения защиты объекта ТСО;

– уменьшить объем монтажных работ, их трудоемкость.

В случае отказа собственника от проведения мероприятий по изменению интерьера объекта и МПХИГ при прокладке шлейфов сигнализации допускается использование радиоканальных ТСО.

При отказе собственника от выполнения требований по ИТУ конструктивных элементов помещений ему рекомендуется оборудовать помещения дополнительными ТСО раннего обнаружения. В зависимости от класса объекта (МПХИГ), а также наличия помещений повышенного риска (особенно подверженным криминальным посягательствам, кражеопасным) существуют основные типовые варианты

оборудования таких объектов (МПХИГ) ТСО, которые могут быть дополнены в каждом конкретном случае по согласованию с собственником объекта:

– блокировка входной двери на открытие и проникновение отдельным шлейфом сигнализации (соответственно магнитоконтактным и объемным оптико-электронным извещателем с зоной обнаружения типа «штора»);

– блокировка некапитального наддверного проема на пролом путем оплетки с помощью провода марок НВМ, ПЭЛ, ПЭВ;

– блокировка окон, балконной двери на открытие с помощью точечных магнитоконтактных извещателей;

– блокировка окон на разбитие стекол с помощью поверхностных звуковых извещателей или поверхностных ударно-контактных извещателей. Допускается вместо блокировки стекол на разбитие блокировать оконные конструкции на «проникновение» с помощью объемных оптико-электронных извещателей с зоной обнаружения типа «штора»;

– блокировка некапитальных стен, смежных между охраняемыми и неохраняемыми помещениями разных собственников, или межквартирных стен с помощью поверхностных вибрационных извещателей, или охранных объемных оптико-электронных извещателей, или объемных оптико-электронных извещателей с зоной обнаружения типа «штора»;

– блокировка внутреннего объема помещений с помощью объемных оптико-электронных, радиоволновых, ультразвуковых или совмещенных и комбинированных извещателей.

Минимально необходимый типовой состав ТСО объекта представлен в табл. 2.3, для МПХИГ – в табл. 2.4.

Таблица 2.3

Минимально необходимый состав ТСО объекта

Технические средства охраны	Класс объекта				
	А1	А2	А3	Б1	Б2
Количество рубежей охраны объекта	3	2(3)	1	2	1
Охранная сигнализация					
Первый рубеж охраны – периметр объекта (двери, стены, оконные проемы) – с выводом на ПЦО	+/–	+	–	+	–

Окончание табл. 2.3

Технические средства охраны	Класс объекта				
	А1	А2	А3	Б1	Б2
Второй рубеж охраны – внутренний объем – с выводом на ПЦО	+/–	+	–	+	–
Третий рубеж охраны – отдельные предметы – с выводом на ПЦО	+/–	+/–	–	+/–	–
Тревожная сигнализация					
Стационарная КТС	+/–	+	+	+/–	+
Носимая КТС	+/–	+	+	–	+/–

Таблица 2.4

Минимально необходимый состав ТСО для МПХИГ

Технические средства охраны	Класс квартиры			Класс МПХИГ		
	В1	В2	В3	Г1	Г2	Г3
Количество рубежей (шлейфов) охранной сигнализации (не менее)	4	2(3)	1(2)	2(3)	2(3)	1(2)
Охранная сигнализация						
Первый рубеж охраны квартиры (МПХИГ). Первый шлейф ОС (с задержкой на взятие/снятие) – периметр квартиры (МПХИГ)						
Основная входная дверь (на открывание и пролом)	+	+	+	+	+	+
Второй шлейф ОС – периметр квартиры (МПХИГ). Запасные входные двери	+	+	+	+	+	+
Окна и балконные двери (на открывание и разбитие стекла)	+	+/ –	+/ –	+/ –	+/ –	+/ –
Стены, перегородки (на разрушение, ударное воздействие)	+/ –	+/ –	–	+/ –	+/ –	–
Второй рубеж охраны квартиры (МПХИГ). Третий шлейф ОС – внутренний объем помещений	+	+	+/ –	+	+/ –	–
Третий рубеж охраны квартиры (МПХИГ). Четвертый шлейф ОС – охрана отдельных предметов	+	+/ –	–	+/ –	–	–
Тревожная сигнализация						
Стационарная КТС	+	+/ –	+/ –	+/ –	+/ –	–
Носимая КТС	+	+/ –	+/ –	+/ –	+/ –	–

Электропитание ТСО

Общие требования по организации электропитания оборудования ТСО изложены в рекомендациях [6; 27; 36]. Электропитание ТСО допускается осуществлять от распределенной электрической сети объекта, источников электропитания по ГОСТ Р 53560-2009, шлейфов сигнализации или двухпроводных линий (извещатели, которые питаются таким образом), других ТСО, имеющих специально предназначенные для этого выходы, автономных источников электропитания.

Технические средства охраны и безопасности, электропитание которых осуществляется от электрической сети объекта, должны:

– иметь встроенную аккумуляторную батарею или возможность подключения внешней АКБ;

– сохранять работоспособность при отклонении напряжения электрической сети от номинального значения в пределах от –20 до +10 %;

– обеспечивать функционирование в режимах, при которых ток потребления достигает максимального значения (с учетом максимальной допустимой нагрузки выходных цепей) без использования энергии АКБ;

– обеспечивать автоматический заряд АКБ за время не более 12 ч при наличии (восстановлении после пропадания) напряжения электрической сети [6; 27; 36].

Технические средства охраны, электропитание которых осуществляется от вторичных источников электропитания, должны сохранять работоспособность при отклонении напряжения электропитания от номинального значения (12 или 24 В) не более чем ±15 %.

Электропитание технических средств охраны и безопасности для эксплуатации в закрытых помещениях осуществляется, как правило, номинальным напряжением 12 В, 24 В – для ТСО, предназначенных для эксплуатации вне помещений, например на открытых площадках и периметрах территорий.

Вторичные источники бесперебойного электропитания по функциональной оснащенности классифицируют на четыре класса: класс 1 – низкий уровень функциональной оснащенности; класс 2 – средний уровень функциональной оснащенности; класс 3 – повышенный уровень функциональной оснащенности; класс 4 – высокий уровень функциональной оснащенности. Класс источников бесперебойного электропитания по функциональной оснащенности определяют по наихудшему показателю оснащенности.

Ввод питающего напряжения 220 В должен осуществляться от двух независимых вводов согласно представленному в проекте техническому заданию по электроснабжению. В качестве резервного источника питания электроприемников ОТС обычно применяют резервированные источники питания, которые обеспечивают питание электроприемников в дежурном режиме в течение 24 ч и в режиме «Тревога» – не менее 3 ч.

Электропитание ТСО от распределенной электрической сети объекта осуществляется от отдельной выходной группы контактов электрощита дежурного освещения. При отсутствии на объекте электрощита дежурного освещения или отдельной группы на нем собственник должен обеспечить установку отдельного электрощита на соответствующее количество выходных групп, рассчитанного по мощности на потребление систем охраны и безопасности. Помещение, в котором размещены электрощиты, необходимо оборудовать системой охранной сигнализации. Вне охраняемого помещения электрощиты следует располагать в запираемых металлических шкафах, контролируемых охранной сигнализацией. Линии электропитания следует выполнять проводами и кабелями в соответствии с требованиями ПУЭ и СП 5.13130.2009.

Линии электропитания, проходящие через неконтролируемые охранной сигнализацией помещения, должны быть выполнены скрытым способом или открытым способом в трубах, коробах или металлорукавах. Линии электропитания ТСО периметра следует выполнять или кабелями в траншее, подземном коллекторе, или открыто по внутренней стороне бетонного ограждения (стене здания) бронированными кабелями.

В обоснованных случаях допускается прокладка небронированных кабелей (проводов) по внутренней стороне бетонного ограждения (стене здания) в стальных трубах. Допускается прокладка путем подвешивания кабелей на тросе на высоте не менее 3 м или на отдельных участках в охраняемой зоне при условии защиты кабеля от механических повреждений на высоте до 2,5 м. Соединительные или ответвительные коробки должны устанавливаться в охраняемых помещениях.

Защитное зануление электрооборудования автоматизированных установок пожарной сигнализации (АУПС) и автоматических систем

пожаротушения (АСПТ) выполняется в соответствии с требованиями ПУЭ, СНиП 3.05.06-85 «Электротехнические устройства», ГОСТ 12.1.030-81 «Электробезопасность. Защитное заземление. Зануление» и технической документацией завода изготовителя. Сопротивление заземляющей (зануляющей) шины должно быть не более 4 Ом.

Проектирование ТСО

Работы по установке и монтажу технических средств охраны на объектах должны проводиться в соответствии с утвержденной проектно-сметной документацией или актами обследования.

Проектные работы выполняют в соответствии с требованиями документов [1; 2; 12; 13; 14]. Типовые проекты оборудования охраняемых объектов ТСО приведены в методических рекомендациях и типовых рабочих проектах [38; 40; 41].

Трудоемкость работ по проектированию, монтажу и пусконаладке объектовых комплексов ТСО определяется по методическим рекомендациям [66]. Требования к организации работы по снижению количества ложных срабатываний средств ОТС изложены в методических рекомендациях [69].

Производство монтажных работ технических средств охраны и безопасности должно осуществляться в соответствии с документом [2]. Применяют технические средства, входящие в перечень [4].

Проектно-сметная документация должна содержать следующий комплект документов:

– техническое задание на разработку проекта, выполненное в соответствии с требованиями документа [1], или акт обследования [5];

– пояснительную записку;

– планы (схемы закладных) трубопроводов, кабелей, проводов и мест установки технических средств охраны на объекте (по требованию заказчика или монтажной организации);

– поэтажные планы разводки шлейфов сигнализации (двухпроводной линии) и линий связи технических средств охраны (совмещенный или раздельный по каждому типу сигнализации);

– общую структурную схему соединений ТСО (совмещенная или раздельная по каждому виду сигнализации) – скелетную схему;

– схемы электрические подключения технических средств охраны (извещателей, контрольных панелей, УОО СПИ и т. д.);

– схемы установки технических средств охраны в охраняемых помещениях;

– схемы блокировки отдельных конструкций (окон, дверей, воздуховодов, стен и других конструкций, если схемы блокировки не типовые);

– схему размещения ТСО в помещении охраны;

– схему (таблицу) разводки электропитания (по необходимости);

– расчет постоянного тока потребления технических средств охраны и необходимой емкости аккумуляторных батарей вторичного источника бесперебойного питания в режимах «норма» и «тревога» (выбор резервного источника питания);

– кабельный (кроссировочный) журнал (при необходимости или по требованию заказчика);

– спецификацию оборудования;

– таблицу исходных данных для программирования технических средств охраны (в зависимости от типа ТСО);

– чертежи общих видов нетиповых решений, конструкций и оборудования.

Примечания

1. В зависимости от категории объекта, охраняемых ценностей, архитектурных решений, особенностей экспликации помещений, требований заказчика и монтажных организаций состав проектной документации может меняться и дополняться.

2. В пояснительной записке к проекту отражаются принятые технические решения согласно техническому заданию на проектирование.

3. Кабельный журнал не составляется, если вся информация о кабелях и проводах (начало, конец, марка, сечение и длина) приведена в других документах проекта или электронной базе данных автоматизированного рабочего места (АРМ) систем безопасности на объекте.

По актам обследования работы по установке и монтажу технических средств охраны производятся в соответствии с типовыми проектными решениями, за исключением объектов:

– нового строительства подгрупп А1, А2, А3, а также реконструируемых и технически перевооружаемых объектов этих под-

групп, на которых монтажные работы технических средств охраны могут привести к нарушению функционирования других систем;

– находящихся под надзором государственных органов охраны памятников истории и культуры;

– с взрывоопасными зонами.

Примечание: в отдельных случаях по согласованию с государственными органами охраны памятников истории и культуры и/или с собственником объекта допускается выполнение монтажных работ по актам обследования.

При недостаточном уровне инженерно-технического укрепления ограждений периметров, зданий, сооружений, помещений, отдельных строительных конструкций должно оформляться задание по усилению элементов строительных конструкций объекта в форме приложения к акту обследования.

Обоснованные отступления, изменения и исправления в проектную документацию или акт обследования вносятся и допускаются только при наличии разрешений (согласования) заказчика и соответствующих организаций, участвующих в утверждении и согласовании данных документов.

Условно-графическое обозначение элементов систем безопасности определяется в рекомендациях [28].

Основные термины и определения тактики охраны объектов

Под тактикой охраны объекта подразумевается выбор вида охраны, методов и средств его реализации, согласованных с собственником объекта, обслуживающей ТСО организацией и охранной организацией.

В основном тактику охраны определяет охранная организация (монтажная организация при оборудовании объекта ТСО) и обязательно согласовывает все технические решения с собственником объекта. Тактика охраны вырабатывается совместно с собственником при комплексном обследовании объекта. Она определяет:

– вид охраны (автономная или централизованная);

– объектовую аппаратуру, тип СПИ (при централизованной охране определяется охранной организацией);

– канал передачи сообщений на ПЦО (радиоканал, проводные СПИ, ВОЛС, ЛВС), необходимость дублирования канала связи;

– место расположения щита ОТС;

– количество рубежей охраны;

– способ блокирования элементов строительных конструкций и охранные извещатели;

– время охраны объекта;

– способ приема/сдачи объекта под охрану: тактика с открытой или закрытой дверью, автоматическая или ручная тактика (определяется типом СПИ и их оконечных устройств (ОУ)).

Как правило, при использовании оконечных устройств со считывателем последний устанавливается либо со стороны улицы (тактика с закрытой дверью без задержки на вход), либо с внутренней стороны (тактика с открытой дверью с задержкой на вход).

При использовании клавиатурного набора (ОУ с клавиатурой) клавиатура должна быть расположена только внутри охраняемого помещения. Кроме вышеперечисленного тактика охраны объекта определяет:

– помещения, подлежащие оборудованию приборами объемного обнаружения;

– необходимость тревожной сигнализации и помещения, подлежащие оборудованию тревожной сигнализацией;

– необходимость и место установки специальных технических средств тревожной сигнализации для выдачи тревожного извещения независимо от действий персонала объекта;

– используемую на объекте структуру шлейфов сигнализации (радиальная или двухпроводная адресная линия, структура адресной линии и место расположения периферийных устройств адресной линии);

– количество и параметры логических разделов и зон, распределение шлейфов и (или) извещателей по зонам и разделам; количество и распределение ПЦН-выходов через ОУ СПИ на ПЦО, распределение шлейфов (извещателей) зон и разделов по ПЦН-выходам;

– место установки и параметры работы внешних звуковых и световых оповещателей;

– параметры программирования извещателей, приемно-контрольных приборов ТСО и (или) контрольных панелей;

– параметры программирования АРМ систем безопасности (при его наличии), периферийных устройств (релейных модулей, контрол-

леров и др.), элементов двухпроводных адресных линий или интегрированных систем безопасности;

– типы и параметры взаимодействия средств охранной сигнализации с другими системами безопасности и (или) инженерными системами здания (например, очень популярное направление развития инженерного оборудования здания – «умный дом»);

– прочие параметры работы охранной сигнализации.

Принятие решения по организации тактики охраны объекта зависит от следующих факторов:

– характера топологии здания, количества собственников отдельных помещений здания и состояния их охраны (смежные неохраняемые помещения);

– количества и характеристик уязвимых мест объекта;

– удаленности объекта от ПЦО охранной организации;

– общей криминогенной обстановки в регионе;

– характера и состояния строительных конструкций здания, состояния инженерно-технической защиты (укрепленности). Оценка состояния инженерно-технической защиты здания может быть проведена в соответствии с требованиями методических рекомендаций [5; 6] либо других аналогичных документов, если объект по ведомственной принадлежности попадает под действие таких документов (например, объекты Центробанка, Сберегательного банка, Газпрома, объекты культуры и др.);

– наличия и характера несения службы ведомственной физической охраной объекта (наличие физического поста (постов) охраны и время его работы);

– характера материальных, художественных, информационных и других ценностей на объекте, способа их хранения и перемещения, присвоенной группы (категории) объекта;

– режима и времени работы объекта;

– наличия на объекте взрывоопасных и пожароопасных зон, температурного режима и влажности на объекте, электромагнитной обстановки на объекте;

– наличия на объекте других (кроме охранной) систем безопасности (например, охранного телевидения, системы контроля и управления доступом и др.);

– типа и характеристик используемых СПИ охранной организацией;

– организации эксплуатационно-технического обслуживания технических средств охраны на объекте;

– квалификации ответственных лиц за эксплуатацию ТСО на объекте;

– прочих особых характеристик объекта.

Тактику охраны объектов условно можно разделить на следующие составляющие:

– тактика оборудования объекта ТСО;

– тактика приема/сдачи объекта на ПЦО, которая определяется типом СПИ охранной организации;

– тактика передачи тревожных и служебных извещений на ПЦО, которая определяется телефонизацией объекта и типом канала связи СПИ охранной организации;

– тактика действий нарядов охранной организации (алгоритм передачи тревожных сигналов группе реагирования, действия персонала ПЦО и нарядов (групп) задержания (реагирования) при получении с объекта тревожных и служебных сообщений). Данная тактика определяется внутренними документами охранной организации.

Тип шлейфа сигнализации определяет функциональное назначение шлейфа сигнализации. Всего имеется четыре типа шлейфов: охранная сигнализация формирует сигнал о несанкционированном проникновении; пожарная сигнализация формирует сигнал о пожаре; тревожная сигнализация формирует сигнал о нападении; технологические шлейфы контролируют состояние автоматики инженерных систем, назначение последнего типа шлейфов определяется их конкретным использованием в данном приемно-контрольном приборе (ПКП). Иногда пожарные шлейфы также разделяют на два или три типа (ручные извещатели, тепловые и дымовые извещатели с определением двойной сработки, т. е. с временным сбросом питания и формированием извещения «Внимание»).

Шлейф сигнализации с правом (без права) отключения – параметр программирования шлейфа, при котором (если шлейф без права отключения) попытка отключения (снятия с охраны) данного шлейфа на объекте (например, кнопкой отключения на ПКП) приводит к формированию тревожного извещения. Обычно без права

отключения программируют тревожные и пожарные шлейфы сигнализации.

Задержка на вход (на выход) – время на вход определяет задержку в формировании тревожного извещения при срабатывании шлейфа сигнализации, например, входной двери. За время, предоставленное на вход, пользователь должен снять объект с охраны своим паролем (ключом). Если за время задержки на вход никаких действий с ПКП не предпринято (взятие, снятие с охраны), то формируется тревожное извещение о проникновении. Если за данное время объект снят с охраны паролем (ключом) пользователя, то тревожного извещения не формируется. Время на выход – время, аналогичное времени на вход, но необходимое для сдачи объекта под охрану по тактике с открытой дверью. Объект ставится под охрану на ПКП, собственник покидает объект, а шлейфы сигнализации, которые он нарушает, покидая объект, должны иметь задержку на выход. Обычно данные задержки программируются индивидуально для каждого объекта, но рекомендуется устанавливать не более 30 – 40 секунд.

Самовосстанавливающийся шлейф сигнализации – шлейф сигнализации, который после срабатывания и сброса срабатывания на ПКП самостоятельно берется под охрану и не требует никаких дополнительных команд взятия под охрану. Обычно самовосстанавливающимися программируют тревожные и пожарные шлейфы сигнализации.

Обход (байпасирование) шлейфов сигнализации – при разрешении обхода (байпасирования) шлейфа сигнализации он принимается под охрану только при восстановлении своей целостности, при нарушении целостности он не принимается под охрану (обходится) без выдачи извещения о невзятии под охрану. При выключении данной функции шлейф не возьмется под охрану и выдаст извещение о невзятии. Например, при взятии под охрану раздела, объединяющего несколько шлейфов, если обход шлейфов разрешен, раздел возьмется под охрану, даже если будет целостным (закрыты все окна, двери) только один шлейф раздела, остальные шлейфы будут обойдены. При отключении функции обхода при взятии раздела он возьмется под охрану, только если все шлейфы раздела будут целостными. Данной функцией необходимо пользоваться очень осторожно, так как обой-

денные (проигнорированные) шлейфы сигнализации под охрану не ставятся и не выдают тревожного извещения.

Тип контроля шлейфа сигнализации (полноценность шлейфов): шлейф сигнализации считается полноценным, если выдает тревожное извещение и на обрыв, и на короткое замыкание шлейфа. Если контролируется только обрыв, то шлейф считается неполноценным и не должен применяться для охранной сигнализации.

Время интеграции шлейфов сигнализации – минимальное время нарушения шлейфа сигнализации для формирования тревожного извещения. При нарушении шлейфа на время, меньшее времени интеграции, из-за случайных помех или перехода на резервное питание тревожное извещение не формируется. Включение данного параметра повышает помехоустойчивость шлейфов сигнализации. Обычно время интеграции составляет 200 – 300 мс.

Тихая тревога – выдача тревожного извещения ПКП без включения внешних световых и звуковых оповещателей. Данная функция иногда необходима для того, чтобы нарушитель не был информирован о выдаче тревожного извещения. Кроме того, данную функцию используют для шлейфов тревожной сигнализации постов физической охраны, чтобы нарушитель не был информирован о нажатии кнопки тревожной сигнализации на посту охраны.

Громкая тревога – выдача тревожного извещения ПКП с включением внешних световых и звуковых оповещателей.

Тревога по принуждению (проход по принуждению) – вид тревожного извещения с объекта, обозначающий то, что собственник при снятии объекта с охраны воспользовался кодом принуждения. В случае если собственник снимает объект с охраны насильно, под угрозой преступника (под принуждением), в большинстве современных технических средств имеется возможность ввести специально заданный код принуждения. При этом на объекте индикация ПКП и оповещатели отображают снятие объекта, но на самом деле на ПЦО поступает сигнал «Тревога по принуждению». Код принуждения либо специально программируется, либо (для большинства аппаратуры) отличается от истинного кода снятия/взятия на ±1 в последнем разряде.

Время контроля канала для радиоканальных извещателей – минимальное время посылки тестовых сигналов контроля нахожде-

ния извещателя в зоне радиосети. Задается индивидуально (как правило, несколько стандартных значений). При выборе значения времени контроля необходимо помнить, что чем меньше время контроля, тем меньше вероятность саботажа извещателя, но больше расход емкости аккумулятора (время работы аккумуляторной батареи) и выше перегрузка радиосети. Чем больше количество извещателей в системе, тем больше должно быть время контроля канала.

Групповое взятие/снятие – возможность одной командой группового взятия/снятия брать под охрану или снимать с охраны все шлейфы, у которых установлен данный атрибут.

Порядок пересечения зон – установленный порядок пересечения зон (шлейфов) при снятии/взятии объекта с охраны. При соблюдении порядка пересечения зон действует задержка на вход/выход. При нарушении порядка (например, зоны нарушаются не от входной двери к центру здания, а наоборот) формируется без задержек извещение о проникновении.

Понятие логических зон и разделов – программно заданные совокупности шлейфов (извещателей), объединенных по разным признакам (как правило, это топология для группового взятия/снятия, например этажи, части этажей; время работы отдельных структурных подразделений объекта; рубежи охраны или шлейфы, объединенные в ПЦН-выходы; шлейфы или извещатели, объединенные по типу сигнализации шлейфов и др.).

«Временные окна» – программно заданные промежутки времени (включая выходные, праздничные дни, летнее/зимнее время, отпуска сотрудников и др.), в течение которых действуют (или теряют силу действия) права операторов АРМ системы безопасности и пользователей системы безопасности на снятие/взятие под охрану разделов и зон, проходов в определенные помещения и другие действия с системой безопасности в целом и охранной сигнализацией в частности.

Параметры программирования объектовых комплексов ТСО

Различают три основных способа программирования приемно-контрольных приборов, панелей или контроллеров. Первый способ – программирование с помощью dip-переключателей. Прибор вводится в режим программирования, затем последовательной перестановкой

перемычек и нажатием кнопок ПКП по каждому шлейфу сигнализации ПКП программируются параметры шлейфов сигнализации и ПКП в целом. Правильность операций подтверждается частотой и цветом мигания светодиодов. Такой способ очень длительный, трудоемкий, требует точного следования инструкции и в настоящее время почти не применяется.

Второй способ программирования – с помощью внешнего пульта программирования (как правило, это ЖК-пульт с клавиатурой). Подключается пульт по внешнему интерфейсу, принятому в данной линейке технических средств производителя (RS-422; RS-485; «Аргус-диалог» и пр.). Например, таким пультом для оборудования линейки интегрированных средств безопасности «Орион-Про» является пульт контроля и управления типа ПКУ С-2000М.

Третий (наиболее удобный и быстрый) способ программирования заключается в подключении ПКП или контрольной панели ОТС к персональному компьютеру через USB-порт. Если ПКП не имеет выхода на ПК, то используются преобразователи интерфейсов, например С2000-USB (преобразует RS-485 в USB). Многие производители оборудования ТСО для линеек своих технических средств разработали утилиты программирования контрольных панелей. Как правило, параметры программирования ПКП и шлейфов заносятся в таких утилитах в электронную таблицу. Параметры программирования ПКП для каждого вида приборов индивидуальны и определяются их тактико-техническими данными.

2.3. Требования по проектированию внутриобъектовых радиоканальных средств охранно-тревожной сигнализации

В настоящее время появились в эксплуатации современные радиоканальные извещатели, т. е. извещатели, в корпусе которых располагаются передатчики, а шлейф сигнализации представляет собой радиоканал. К таким извещателям помимо типовых технических характеристик по физическому принципу действия предъявляются дополнительные технические требования, относящиеся к радиоканалу:

– дальность действия радиоканала (зависит от мощности передатчика внутри извещателей и составляет от единиц до сотен метров в условиях прямой видимости);

– частота контроля канала каждого передатчика (время, через которое передатчик посылает тестовые сигналы на приемник);

– помехозащищенность и имитостойкость радиоканала (возможность подмены извещателя);

– статическая или динамическая адресация извещателей радиоканала;

– количество адресуемых извещателей в одном помещении;

– возможность контроля уровня сигнала и перехода на резервную частоту;

– ток потребления извещателей, емкость и время работы радиоизвещателей от встроенных аккумуляторов, резервирование аккумуляторов;

– параметры приемников радиоканала (чувствительность, избирательность и др.).

Достоинства радиоканальных извещателей следующие:

– ускорение сроков и упрощение монтажных работ, возможность оборудования объектов, в которых интерьер не позволяет использовать проводную продукцию (объекты культуры и культа, современные офисы с повышенными требованиями к дизайну и др.);

– контроль состояния извещателей в неохраняемое время (снижение вероятности саботажа в неохраняемое время);

– быстрое перепрограммирование тактики охраны системы;

– точность определения срабатывания каждого извещателя, как и в адресной системе.

Недостатки радиоканальных извещателей следующие:

– высокая стоимость;

– необходимость периодической замены батарей (повышение эксплуатационных расходов);

– возможность саботажа радиоканала извещателей;

– ограничение использования извещателей электромагнитной обстановкой на объекте.

Рассмотрим требования по проектированию внутриобъектовых радиоканальных средств (ВОРС) охранно-тревожной сигнализации на примере ВОРС «Стрелец-Про» производства «Аргус-Спектр» (Санкт-Петербург) (https://argus-spectr.ru/streletzpro). Функциональные возможности ВОРС «Стрелец-Про» обеспечивают выполнение следующих функций.

1. Прием и обработка тревожных извещений: сигналов «Нарушен», «Тревога», «Пожар», «Неисправность»; сигналов «Паника» от охранных извещателей, устройств управления и тревожных кнопок; формирование сигнала «Пожар 2» при срабатывании более одного пожарного извещателя или ШС в разделе; прием аналоговых значений от пожарных извещателей и ШС; объединение извещателей и ШС в разделы и группы разделов.

2. Активация выходов по событиям с программируемым типом срабатывания, задержкой и длительностью; объединение выходов в группы выходов.

3. Управление системой: состоянием охраны разделов и групп разделов («Поставить на охрану», «Снять с охраны», «Сбросить пожарные тревоги и неисправности», «Перевзять на охрану»); группами выходов («Включить», «Выключить», «Старт», «Стоп»); формирование сигнала «Снятие под принуждением»; возможность выполнения «Обхода» («Исключения») неисправных извещателей и ШС; задержка постановки на охрану и снятия с охраны; автоматическая постановка на охрану; автоматический сброс пожарных тревог и неисправностей; назначение списка разделов (зон ответственности) для устройств управления.

4. Распределение прав пользователей системы: различные идентификационные признаки пользователей (коды доступа, ключи TouchMemory, карты Proximity); объединение пользователей в группы; настраиваемые права групп пользователей на управление разделами и группами исполнительных устройств.

В состав ВОРС «Стрелец-Про» входит набор устройств из следующих групп:

– устройства приемно-контрольные;
– извещатели пожарные адресно-аналоговые;
– извещатели охранные;
– извещатели технологические;
– устройства исполнительные;
– устройства оповещения;
– устройства управления пожарной автоматикой;
– устройства управления и индикации;
– коммуникационные устройства;
– устройства сетевых интерфейсов;

– устройства сетевой топологии;

– программное обеспечение.

«Стрелец-Про» обеспечивает следующую ёмкость (табл. 2.5).

Таблица 2.5

Емкость «Стрелец-Про»

Компонент	Количество в сегменте, шт.
Устройство	127
Извещатель, шлейф, вход, радиорасширитель	1920
Раздел	512
Группа разделов	128
Реле, выход типа «открытый коллектор», устройство оповещения (выход)	1920
Группа выходов, зона пожарной автоматики, зона оповещения	64
Устройство управления	512
Пользователь	2048
Группа пользователей	512

Характеристики радиоканального интерфейса ВОРС «Стрелец-Про» следующие: частотные диапазоны работы – 864 – 865 МГц, 868 – 868,2 МГц, 868,7 – 869,2 МГц; количество рабочих каналов – 6; автоматическая смена канала при невозможности передачи по основному каналу; максимальная излучаемая мощность – не более 25 мВт; период передачи контрольных сигналов – 2 мин; период контроля связи – 5 мин, 10 мин (программируется); максимальная дальность радиосвязи в открытом пространстве контроллер ↔ контроллер1 – до 2 км, контроллер ↔ ДУ2 – до 1,2 км; сетевая топология контроллеров – многосвязная сеть с динамической маршрутизацией; максимальное количество контроллеров, автоматически подключающихся к родительскому контроллеру, – 31; максимальное количество участков ретрансляции – 10; сетевая топология контроля дочерних устройств «Стрелец-Про» – «звезда»; родительский контроллер выбирается устройством автоматически в зависимости от условий радиосвязи; максимальное количество (коэффициент разветвлённости) дочерних устройств, автоматически подключающихся к контроллеру, – 256; максимальное количество устройств на одном частотном канале в зоне взаимной радиовидимости – не менее 2000; автоматическая подстройка рабочей частоты, автоматическая регулировка мощности; ди-

намическое кодирование информации и механизм динамической двухсторонней аутентификации для исключения возможности постороннего вмешательства в работу радиосистемы и подмены радиоустройств.

В системе функционирует до 127 радиорасширителей (РР), образующих на объекте радиосеть. Центральный контроллер радиоканальных устройств – РР-И-ПРО. Маршруты связи между РР устанавливаются автоматически. Дочерние радиоканальные устройства (ДУ) подключаются к РР, имеющим наилучшие условия связи с РР – координатором радиосистемы (РР-КР). Каждый РР способен непосредственно контролировать 31 дочерний РР и 256 ДУ.

При конфигурировании «Стрелец-Про» один из шести доступных частотных каналов устанавливается в качестве основного рабочего. При невозможности связи по основному каналу оборудование автоматически устанавливает связь по оставшимся резервным каналам. Контроллер радиоканальных устройств РР-И-ПРО возможно подключать к контроллеру сегмента РРОП-И по интерфейсу S2. Также РР-И-ПРО способен самостоятельно выполнять в ИСБ функции контроллера сегмента (с некоторыми ограничениями). РР-И-ПРО имеет интерфейс USB для подключения к ПК, а также интерфейсы S2 (до 2 шт.) для возможности построения кольцевой линии S2 ИСБ. Функции РР выполняют устройства РР-ПРО, а также совмещенные устройства Табло-РР-ПРО, Пульт-РР-ПРО (и аналогичные). Радиорасширитель и совмещенные с ним устройства имеют возможность автоматической активации выходов, входящих в его состав, согласно запрограммированной логике ИСБ. Для управления используются радиоканальные устройства Пульт-РР-ПРО, Пульт-ПРО и Брелок-ПРО.

Определение параметров инсталляции ВОРС «Стрелец-Про»

Перед началом конфигурирования и программирования системы рекомендуется составить проект будущей инсталляции, используя планы помещений и данные технического задания. После изучения документации и основных технических характеристик ВОРС «Стрелец-Про» и при составлении проекта следует определить параметры системы по следующим направлениям.

1. Извещатели и исполнительные устройства: определить типы устройств и места их установки; выбрать тип подключения извещателей и исполнительных устройств (радиоканальные, адресные, неадресные).

2. Устройства управления и индикации: определить места установки устройств управления и индикации (посты наблюдения, места постановки на охрану и пр.); определить помещения, относящиеся к зонам ответственности устройств управления и устройств индикации.

3. Приборы приемно-контрольные: выбрать типы приборов в зависимости от используемых извещателей и исполнительных устройств (РРОП-И, БСЛ240-И, БШС8-И); определить места установки приборов в зависимости от их емкости и радиуса охвата линий связи.

4. Группы разделов: определить количество и состав групп разделов (принцип объединения разделов в группы разделов). При конфигурировании опций автоматической сработки исполнительных устройств обеспечивается одинаковая реакция устройств автоматики на события в разных разделах (например, запуск оповещения при пожарной тревоге во всех разделах здания). При конфигурировании опций индикации обеспечивается укрупнение индицируемой информации (например, до этажа или группы помещений).

5. Разделы: определить количество разделов и их состав. Рекомендуемый принцип организации разделов – географический: извещатели, расположенные в одном помещении, объединяются в один раздел.

6. Срабатывание исполнительных устройств: определить условия срабатывания исполнительных выходов, выбрав их из числа доступных (например, «Звуковое оповещение при пожарных тревогах с задержкой 1 мин и ограничением длительности оповещения 1 час»).

7. Группы пользователей: определить права и необходимое количество групп пользователей. Группы пользователей могут создаваться с функциональными разграничениями (например, «только постановка на охрану», «только стоп групп ИУ» или «неограниченные права») либо с географическими (например, «пользователи комнаты 107»).

8. Пользователи: определить список пользователей и тип их идентификационных признаков (цифровой код, ключ ТМ или карта Proximity).

2.4. Требования по проектированию ПЦН-выходов и рубежей сигнализации централизованно охраняемых объектов

Автоматические охранные извещатели в зависимости от дополнительных функций подразделяют на классы 1, 2, 3 и 4 в соответствии с ГОСТ [51]. Извещатели класса 1 в дополнение к основной функции назначения должны:

– обнаруживать попытку несанкционированного доступа путем вскрытия корпуса (если корпус разборный), позволяющего обеспечить доступ к органам управления, подключения, регулировки, индикации и монтажным элементам;

– обнаруживать неисправность в виде полного отсутствия напряжения электропитания;

– иметь не менее одного информационного выхода для формирования не менее двух видов извещений.

Извещатели класса 2 в дополнение к основной функции назначения должны:

– обнаруживать попытку несанкционированного доступа путем вскрытия корпуса (если корпус разборный), позволяющего обеспечить доступ к органам управления, подключения, регулировки, индикации и монтажным элементам;

– обнаруживать неисправность в виде полного отсутствия напряжения электропитания или снижения напряжения электропитания до значения, установленного в стандарте на извещатели конкретного вида или конкретного типа;

– иметь не менее двух информационных выходов для формирования не менее трех видов извещений.

Извещатели класса 3 в дополнение к основной функции назначения должны:

– обнаруживать попытку несанкционированного доступа путем вскрытия корпуса (если корпус разборный), позволяющего обеспечивать доступ к органам управления, подключения, регулировки, индикации и монтажным элементам;

– обнаруживать попытку нарушения нормального функционирования путем отрыва от монтажной поверхности, изменения положения в пространстве или иного внешнего воздействия;

– обнаруживать неисправность в виде полного отсутствия напряжения электропитания или снижения напряжения электропитания до значения, установленного в стандарте на извещатели конкретного вида или конкретного типа;

– обеспечивать автоматический контроль параметров окружающей среды, влияющих на параметры обнаружения;

– иметь не менее трех информационных выходов для формирования не менее четырех видов извещений.

Извещатели класса 4 в дополнение к основной функции назначения должны:

– обнаруживать попытку несанкционированного доступа путем вскрытия корпуса (если корпус разборный), позволяющего обеспечить доступ к органам управления, подключения, регулировки, индикации и монтажным элементам;

– обнаруживать попытку нарушения нормального функционирования путем отрыва от монтажной поверхности, изменения положения в пространстве или иного внешнего воздействия;

– обнаруживать неисправность в виде полного отсутствия напряжения электропитания или снижения напряжения электропитания до значения, установленного в стандарте на извещатели конкретного вида или конкретного типа;

– обеспечивать автоматический контроль параметров окружающей среды, влияющих на параметры обнаружения;

– иметь не менее трех информационных выходов для формирования не менее четырех видов адресных извещений;

– обеспечивать возможность удаленного контроля функционирования.

Основные виды несанкционированных воздействий на технические средства охранной сигнализации и способы защиты

Анализ практики охраны различных объектов, обобщение опыта работы территориальных подразделений вневедомственной охраны, расположенных в различных субъектах РФ, позволяет выделить наиболее часто используемые нарушителями способы саботажа охранных извещателей для обхода рубежей сигнализации с целью незаконного проникновения на охраняемый объект.

Данные статистики посягательств на защищаемые объекты показывают, что случаи умышленного нарушения функционирования (саботажа) ТСО на объектах высоких классов (А1, А2) распространены в 9,7 раза чаще, чем попытки саботажа ТСО на объектах более низких классов (Б1, Б2), поэтому на объектах высоких классов необходимо применять ТСО с функцией защиты от саботажа (маскирования) и ТСО, обладающие высокой имитостойкостью.

Наибольшее распространение имеет саботаж извещателей при помощи маскирования (37 % от числа всех попыток), который чаще всего происходит на объектах в неохраняемое время, когда к извещателям и другим средствам ТСО может иметься доступ посторонних лиц. В ряде случаев (7 %) магнитоконтактные извещатели были заблокированы внешним магнитом во время нахождения объекта под охраной.

Наиболее уязвимы для саботажа (умышленного нарушения функционирования) звуковые, инфракрасные оптико-электронные пассивные и магнитоконтактные извещатели. Для решения этой проблемы рекомендуется применять пассивные ИК-извещатели с функцией антимаскирования («Фотон-16», «Астра-5» исп. АМ, «Фотон-22») и антисаботажными зонами обнаружения, звуковые извещатели с функцией антимаскирования («Стекло-4») и магнитоконтактные извещатели с функцией защиты от саботажа («Кенар»).

Для защиты внутреннего пространства помещений особо важных объектов высоких категорий наряду с пассивными оптико-электронными ИК-извещателями рекомендуется устанавливать активные ультразвуковые, радиоволновые или комбинированные извещатели. Для блокировки остекленных конструкций рекомендуется устанавливать звуковые извещатели с функцией защиты от маскирования, совместно осуществляется блокировка оконного проема или витрины пассивными оптико-электронными ИК-извещателями, имеющими зону обнаружения типа «штора» и функцию защиты от маскирования.

Нарушителями также может быть использован саботаж путем переориентации извещателей с целью изменения направления зоны обнаружения. Для защиты от этого в помещениях с доступом посторонних лиц следует использовать извещатели, устанавливаемые непосредственно на стену или потолок (с ЗО в форме конуса) без ис-

пользования кронштейна или обладающие чувствительностью к переориентации («Астра-5» исп. АМ, «Фотон-16», «Фотон-22»).

Повреждение периметровых средств обнаружения происходит примерно в 10 % случаев от всех случаев саботажа извещателей. В связи с этим для защиты периметров объектов следует использовать периметровые средства обнаружения, выдающие тревожное сообщение в случае повреждения чувствительного элемента, линии связи либо при вскрытии блока обработки сигналов.

Внесение изменений в настройки извещателей при их пусконаладке или перепрограммировании происходит в 5 % случаев саботажа работы ТСО. Для борьбы с подобными случаями тактика охраны объекта должна предусматривать возможность круглосуточной передачи на ПЦН извещения о вскрытии корпуса извещателя, в том числе когда объект не стоит на охране.

На объектах высоких категорий (А1 и А2) известны ситуации, когда саботаж осуществлялся путем демонтажа технических средств охраны. В таких случаях следует использовать вибрационные и совмещенные с ними извещатели раннего обнаружения, обладающие функцией контроля механического контакта с охраняемой поверхностью («Шорох-2», «Шорох-3») или работающие в круглосуточном режиме.

Вместе с тем следует учитывать, что большинство (60 %) случаев саботажа приходится на средства передачи извещений. При этом наиболее распространено:

– нарушение антенно-фидерных устройств (45 %, при этом из них 60 % случаев саботажа происходило на объектах класса Б2);

– имитация сигнала оконечного устройства (15 %, при этом из них 40 % попыток саботажа ТСО происходило на объектах классов А1, А2);

– отключение электропитания СПИ (15 %);

– постановка радиочастотной помехи для блокировки СПИ, функционирующей с использованием радиоканала (10 %);

– подмена объектового оборудования СПИ (10 %).

Организация передачи информации о срабатывании сигнализации

Передача извещений о срабатывании охранной сигнализации с объекта на ПЦО может осуществляться с приемно-контрольного прибора малой емкости, внутреннего пульта охраны или устройств око-

нечных СПИ. Требования государственных стандартов к системам передачи извещений изложены в ГОСТ и методических рекомендациях [22; 30; 37; 42]. Требования к ПЦО изложены в ГОСТ и методических рекомендациях [61; 68]. Методические рекомендации по применению СПИ по различным каналам связи содержатся в обзорах [64; 65; 67].

Количество рубежей охранной сигнализации, выводимых на ПЦО отдельными номерами, определяется совместным решением руководства объекта и подразделения вневедомственной охраны исходя из категории объекта, на основе анализа риска и потенциальных угроз объекту, возможностей интеграции и документирования ПКП (внутренним пультом охраны или оконечным устройством) поступающей информации, а также согласно порядку организации дежурства персонала охраны на объекте. Минимально необходимое количество рубежей охранной сигнализации, выводимых на ПЦО со всего охраняемого объекта, должно быть: для подгруппы Б2 – один объединенный рубеж (периметр); для подгруппы Б1 и выше – два объединенных рубежа (первый – периметр и второй – объем). Кроме того, при наличии на объекте специальных помещений (сейфовые, оружейные комнаты и другие помещения, требующие повышенных мер защиты) выводу на ПЦО подлежат также и рубежи охранной сигнализации этих помещений.

Как правило, все одноименные рубежи охранной сигнализации всех подгрупп охраняемых помещений (кроме специальных помещений), имеющихся на объекте, объединяются в соответствующие рубежи и выводятся на отдельные пультовые номера ПЦН ПЦО. Точное количество ПЦН-номеров определяется договором на централизованную охрану объекта. Объединение рубежей происходит с помощью пультов внутренней охраны, многошлейфных (2 и более) ПКП и оконечных устройств.

При наличии на объекте поста внутренней охраны с круглосуточным дежурством собственной службы безопасности или частного охранного предприятия на ПЦО выводятся: один общий сигнал, объединяющий все рубежи охранной сигнализации объекта, за исключением рубежей специальных помещений объекта; рубежи охранной сигнализации (периметр и объем) специальных помеще-

ний. При этом должна быть обеспечена регистрация всей поступающей информации каждого рубежа охраны помещений на внутреннем пульте охраны.

При охране только отдельных устройств (банкоматы, игровые автоматы, распределительные шкафы и другие аналогичные устройства) на ПЦО выводится один рубеж охранной сигнализации (блокировка на «разрушение» и «вскрытие»). При отсутствии на охраняемом объекте технической возможности вопросы вывода рубежей охранной сигнализации решаются индивидуально охранной организацией и собственником в каждом конкретном случае.

Рубежи охранной сигнализации должны выводиться на ПЦО с внутреннего пульта охраны, ПКП или оконечного устройства, обеспечивающих запоминание тревожного состояния и его фиксацию на выносном световом (звуковом) оповещателе или индикаторе. Для объектов жилого сектора допускается применение оконечных устройств и объектовых блоков без соответствующего запоминания тревожного состояния и его фиксации. Извещения от шлейфов тревожной сигнализации одним объединенным сигналом выводятся на ПЦО непосредственно или через ПКП, оконечное устройство СПИ или внутренний пульт охраны.

Для исключения доступа посторонних лиц к извещателям, ПКП, разветвительным коробкам, другой установленной на объекте аппаратуре охраны должны приниматься меры по их маскировке и скрытой установке.

Крышки клеммных колодок данных устройств должны быть опломбированы (опечатаны) электромонтером или инженерно-техническим работником охранной организации с указанием фамилии и даты в технической документации объекта. Распределительные шкафы, предназначенные для кроссировки шлейфов сигнализации, должны закрываться на замок, быть опломбированы и иметь блокировочные (антисаботажные) кнопки, подключенные на отдельные номера внутреннего пульта охраны «без права отключения», а при отсутствии внутреннего пульта охраны – выводиться на ПЦО в составе тревожной сигнализации. Согласно методическим рекомендациям [5], к системам передачи извещений предъявляются следующие требования, представленные в табл. 2.6.

Таблица 2.6

Выбор канала передачи информации на ПЦО с объектов (квартир, МПХИГ)

Канал передачи информации			Класс объекта					Класс квартир			Класс МПХИГ		
			А1	А2	А3	Б1	Б2	В1	В2	В3	Г1	Г2	Г3
Количество каналов передачи информации			2	1/2	1/2	1/2	1/2	2	1/2	1/2	1/2	1/2	1/2
Количество шлейфов в оконечном объектовом устройстве (не менее)			4	4	2	4	2	4	4	2	4	4	2
Среда передачи информации		Организация передачи информации											
Проводная среда передачи информации	Традиционные линии связи	По абонентской телефонной сети общего пользования или специально выделенной линии оператора связи	+	+	+	+	+	+	+	+	+	+	+
	Проводные линии связи, интернет-провайдер	По открытому каналу сети Интернет	–	–	–	–/+	–/+	–	–/+	–/+	–/+	–/+	–/+
		По каналам закрытой сети Ethernet на базе ВОЛС	+	+	+	+	+	+	+	+	+	+	+
Беспроводная среда передачи информации	Радиосистемы передачи извещений	Выделенная частота УКВ-радиодиапазона	+	+	+	+	+	+	+	+	+	+	+
	Каналы передачи данных сетей сотовых операторов	GSM(GPRS)-каналы передачи данных сетей сотовых операторов	–	–/+	–/+	–/+	+	–	–/+	+	–/+	–/+	+

Контрольные вопросы

1. Назовите физический принцип действия, достоинства и недостатки использования емкостных и радиоволновых технических ПСО.
2. Назовите физический принцип действия, достоинства и недостатки использования проводноволновых и сейсмических технических ПСО.
3. Назовите физический принцип действия, достоинства и недостатки использования манометрических и оптико-электронных (пассивных и активных) технических ПСО.
4. Назовите физический принцип действия, достоинства и недостатки использования вибрационных и волоконно-оптических ПСО.
5. Что является рубежом охраны? Сколько существует рубежей охраны? Что они защищают? Какие извещатели используются в рубежах охраны?
6. Что защищает 1-й рубеж охраны? Какие извещатели используются в этом рубеже охраны и для каких строительных конструкций? Как они защищают, как устанавливаются?
7. Что защищает 2-й рубеж охраны? Какие извещатели здесь используются? Что и как они защищают? Как устанавливаются?
8. Что защищает 3-й рубеж охраны? Какие извещатели используются в этом рубеже охраны? Что и как они защищают? Как устанавливаются?
9. Назовите основные требования по установке и способы блокирования дверей охранными извещателями.
10. Назовите основные требования по установке и способы блокирования оконных конструкций охранными извещателями.
11. Назовите основные требования и способы блокирования внутреннего объема помещения охранными извещателями.
12. Назовите основные требования к проектированию тревожной сигнализации.
13. Назовите требования по проектированию ПЦН-выходов и рубежей сигнализации централизованно охраняемых объектов.
14. Назовите требования по организации электропитания технических средств охранно-тревожной сигнализации.
15. Назовите основные виды несанкционированных воздействий на технические средства охранной сигнализации и способы защиты.

Глава 3. ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Основные термины, определения и сокращения

Аутентификация – процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

Биометрическая идентификация – преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие, например, в виде математического ожидания и дисперсий контролируемых параметров или, например, в виде параметров обученной сети искусственных нейронов.

Биометрический образ – образ человека, полученный с выходов первичных измерительных преобразователей физических величин, подвергающийся далее масштабированию и иной первичной обработке с целью извлечения из него контролируемых биометрических параметров человека.

Вещественный код – код, записанный на физическом носителе (идентификаторе).

Временной интервал доступа (окно времени) – временной интервал, в течение которого в данной точке доступа устанавливается заданный режим доступа.

Динамический биометрический образ – биометрический образ, изменяемый человеком по своему желанию, например рукописный образ слова-пароля.

Доступ – перемещение людей (субъектов доступа), транспорта и других объектов (объектов доступа) в (из) помещения, здания, зоны и территории.

Запоминаемый код – код (кодовое слово, пароль), вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

Зона доступа – здание, помещение, территория, транспортное средство, вход и (или) выход которых оборудованы средствами контроля и управления доступом (КУД).

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, – это предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и другие подобные устройства).

Идентификация – процесс опознавания субъекта или объекта по присущему или присвоенному ему идентификационному признаку. Под идентификацией понимается также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Контроллер доступа (КД) – прибор приемно-контрольный доступа (ППКД), аппаратное устройство в составе средств управления СКУД.

Контроль и управление доступом – комплекс мероприятий, направленных на предотвращение несанкционированного доступа.

Копирование – действия с идентификаторами, цель которых – получение копии идентификатора с действующим кодом.

Манипулирование – действия с устройствами контроля доступа, находящимися в рабочем режиме, без их разрушения, цель которых – получение действующего кода или приведение в открытое состояние устройств преграждающих управляемых (УПУ). Устройства контроля доступа могут продолжать правильно функционировать во время манипулирования и после него; следы такого действия не будут заметны. Манипулирование включает в себя также действия над программным обеспечением и по съему информации с каналов связи и интерфейсов устройств доступа.

Наблюдение – действия с устройствами контроля и управления доступом без прямого доступа к ним, цель которых – получение действующего кода.

Несанкционированные действия – действия, цель которых – несанкционированное проникновение в зону доступа через УПУ.

Несанкционированный доступ – доступ субъектов или объектов, не имеющих права доступа.

Пользователь СКУД – субъект, в отношении которого осуществляются мероприятия по контролю доступа.

Правило двух (и более) лиц – правило доступа, при котором доступ разрешен только при одновременном присутствии двух или более лиц.

Принуждение – насильственные действия над лицом, имеющим право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.

Пропускная способность – способность средства или системы КУД пропускать через заданную точку доступа определенное количество субъектов или объектов доступа в единицу времени.

Саботаж – преднамеренно созданное состояние системы или ее компонентов, при котором нарушается работоспособность, ухудшаются параметры, происходит повреждение системы.

Санкционированный доступ – доступ субъектов или объектов, имеющих права доступа.

Система контроля и управления доступом – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Средства управления (СУ) – аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации.

Средства контроля и управления доступом (средства КУД) – механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

Точка доступа – место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные необходимыми средствами).

Уровень доступа – совокупность временных интервалов доступа (окон времени) и точек доступа, которые назначаются определен-

ному лицу или группе лиц, имеющим доступ в заданные точки доступа в заданные временные интервалы.

Устойчивость к взлому – способность конструкции противостоять разрушающему воздействию.

Устройства преграждающие управляемые – устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (турникеты, шлюзы, проходные кабины, двери и ворота, оборудованные исполнительными устройствами СКУД, а также другие подобные устройства).

Устройства исполнительные (УИ) – устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические, электромагнитные замки, электромагнитные защелки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

Устройство считывающее, считыватель – устройство, предназначенное для считывания (ввода) идентификационных признаков.

Требования к функциональным характеристикам средств СКУД

Требования к функциональным характеристикам элементов СКУД изложены в ГОСТ [71; 72]. Устройства преграждающие управляемые в закрытом состоянии должны обеспечивать физическое препятствие доступу в соответствии с классификацией по виду перекрытия проема:

– частичное перекрытие (турникеты, шлагбаумы);

– полное перекрытие (полноростовые турникеты, специализированные ворота);

– сплошное перекрытие (сплошные двери, сплошные ворота);

– блокирование объекта в проеме (шлюзы, кабины проходные).

Устройства преграждающие управляемые в рабочем режиме могут быть нормально открытыми или нормально закрытыми. Нормально открытые УПУ должны быть оснащены датчиком приближения субъекта и объекта доступа, обеспечивать свободный проход при санкционированном доступе и переходить в закрытое состояние, если доступ несанкционирован.

Нормально закрытые УПУ должны открываться при санкционированном доступе. Устройства преграждающие управляемые с ча-

стичным перекрытием проема при необходимости должны быть оснащены средствами сигнализации, срабатывающими при попытке обхода преграждающего устройства. Устройства преграждающие управляемые при санкционированном доступе должны переходить в открытое состояние при подаче управляющего сигнала от устройства управления.

Нормально закрытые УПУ при необходимости должны быть оборудованы средствами звуковой сигнализации, которая включается после их открывания и при отсутствии прохода в течение установленного времени, и иметь средства для возврата в закрытое состояние. Устройства преграждающие управляемые при необходимости должны иметь защиту от прохода через них одновременно двух или более человек.

Устройства преграждающие управляемые должны иметь возможность механического аварийного открывания в случае пропадания электропитания, возникновения пожара или других чрезвычайных ситуаций. Аварийная система открывания должна быть защищена от возможности использования ее для несанкционированного проникновения.

В конструкции УПУ должны быть предусмотрены меры по защите внешних электрических соединительных цепей от несанкционированных воздействий (подачи напряжений, обрыва, короткого замыкания), приводящих к открыванию УПУ. Устройства преграждающие управляемые могут иметь дополнительно средства специального контроля (металлодетекторы, обнаружители радиоактивных веществ и др.), встроенные или совместно функционирующие. Устройства исполнительные должны обеспечивать приведение УПУ в закрытое или открытое состояние.

Устройства исполнительные могут быть самостоятельными изделиями или выполненными как часть конструкции УПУ.

Считыватели должны обеспечивать:

– ввод запоминаемого кода;

– считывание идентификационного признака с идентификаторов;

– введение биометрической информации (для считывателей биометрической информации);

– преобразование введенной информации в электрический сигнал;

– передачу информации на контроллер СКУД.

Считыватели должны иметь световую индикацию работоспособности и состояния доступа. Рекомендуемый режим работы – непрерывное свечение индикатора красного цвета при закрытом доступе и непрерывное свечение индикатора зеленого цвета при открытом доступе. Допускается в режиме экономии электропитания световую индикацию работоспособности и состояния доступа отображать кратковременными вспышками соответствующего цвета.

При необходимости считыватели должны иметь звуковой сигнализатор. Параметры звуковых сигналов и события, которые они индицируют, должны быть описаны в документации на изделия. Допускается в считывателе не иметь индикации, в этом случае должно быть оговорено в документации, что такие считыватели должны использоваться с контроллерами СКУД, которые обеспечивают управление внешними световыми и звуковыми индикаторами.

Считыватели должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды и степень защиты должны быть указаны в стандартах и (или) нормативных документах на устройства конкретного типа.

Считыватели при взломе и вскрытии, а также в случае обрыва или короткого замыкания подходящих к ним цепей не должны вызывать открытие УПУ. При этом автономные системы должны выдавать звуковой сигнал тревоги, а системы с централизованным управлением дополнительно должны передавать сигнал тревоги на пункт управления. Идентификаторы должны иметь уникальный идентификационный признак (код, номер), который не должен повторяться. В случае если такое повторение возможно, в документации на изделия должны быть указаны условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами. Идентификаторы должны обеспечивать хранение идентификационного признака в течение всего срока службы при эксплуатации.

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов. Аппаратные средства управления (контроллеры) должны обеспечивать прием информации от считывателей, обработку информации и

выработку сигналов управления на исполнительные устройства. Контроллеры в системах с централизованным управлением и универсальных должны обеспечивать: обмен информацией по линии связи между контроллерами и средствами централизованного управления; сохранность данных в памяти при обрыве линий связи со средствами централизованного управления, при отключении питания и переходе на резервное питание; контроль линий связи между контроллерами и средствами централизованного управления.

Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также имитостойкость и защиту информации (для систем повышенной и высокой устойчивости). Виды и параметры протоколов и интерфейсов должны быть установлены в стандартах и других нормативных документах на контроллеры конкретного типа. Контроллеры должны иметь входы для подключения цепей сигнализации состояния УПУ, кнопки запроса на выход, контакты вскрытия корпуса, контакты отрыва от стены. Контроллеры СКУД дополнительно могут иметь входы для подключения шлейфов охранной сигнализации. Контроллеры должны иметь выходы для подключения цепей управления исполнительными устройствами, выходы управления световой индикацией состояния доступа по каждому направлению, выходы управления световой и звуковой индикацией тревожных состояний.

Сетевые СКУД должны иметь средства централизованного управления, в качестве которых могут использоваться средства вычислительной техники (СВТ) общего назначения или специализированные компьютеры. Основной компонент средств управления сетевых СКУД – программное обеспечение (ПО). Программное обеспечение сетевых СКУД должно обеспечивать:

– эргономичный экранный интерфейс с пользователем (оператором СКУД);

– занесение кодов идентификаторов в память системы;

– задание характеристик точек доступа;

– установку временных интервалов доступа (окон времени);

– установку уровней доступа для пользователей;

– протоколирование текущих событий;

– протоколирование тревожных событий;

– ведение и поддержание баз данных;

– регистрацию прохода через точки доступа в протоколе базы данных;

– сохранение баз данных и системных параметров на резервном носителе;

– сохранение баз данных и системных параметров при авариях и сбоях в системе;

– приоритетный вывод информации о нарушениях.

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

- отключение питания аппаратных средств;
- программный рестарт аппаратных средств;
- аппаратный рестарт аппаратных средств;
- случайное нажатие клавиш на клавиатуре;
- случайный перебор пунктов меню программы.

После указанных воздействий и перезапуска программы должны сохраняться работоспособность системы и установленные данные. Указанные воздействия не должны приводить к открыванию УПУ и изменению действующих кодов доступа.

Требования к функциональным характеристикам СКУД

Требования к функциональным характеристикам автономных СКУД [71; 72] представлены в табл. 3.1, систем с централизованным управлением и универсальных СКУД – в табл. 3.2.

Таблица 3.1

Функциональные характеристики автономных систем

Функциональная характеристика	Класс		
	1	2	3
Установка уровней доступа	–	–	+
Установка временных интервалов доступа	–	+	+
Возможность регулирования времени открывания УИ	–	+	+
Возможность идентификации по двум признакам	–	–	+
Защита от повторного использования идентификатора для прохода в одном направлении	–	–	+
Ввод специального идентификационного признака для открывания под принуждением	–	–	+
Подключение считывателей различных типов	–	+	+

Окончание табл. 3.1

Функциональная характеристика	Класс		
	1	2	3
Доступ по правилу двух (и более) лиц	–	–	+
Световая индикация состояния доступа	+	+	+
Контроль состояния УПУ	–	+	+
Световое и/или звуковое оповещение о попытках НСД	–	–	+
Регистрация и хранение информации о событиях в энергонезависимой памяти	–	+	+
Количество событий, хранимых в энерго-независимой памяти, не менее	–	64	256
Ведение даты и времени возникновения событий	–	+	+
Возможность подключения устройства для вывода информации о событиях	–	+	+
Возможность передачи информации о событиях на ЭВМ	–	–	+
Возможность интегрирования с системой охранной сигнализации на релейном уровне	–	+	+
Возможность интегрирования с системой охранного телевидения на релейном уровне	–	–	+

Примечание. Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «–» означает отсутствие функции.

Таблица 3.2

Функциональные характеристики систем с централизованным управлением и универсальных СКУД

Функциональная характеристика	Класс системы		
	1	2	3
Число уровней доступа, не менее	16	64	256
Число временных интервалов доступа, не менее	16	64	256
Защита от повторного использования идентификатора для прохода в одном направлении:			
– локальная	–	+	+
– глобальная	–	–	+
Возможность двойной идентификации	–	+	+
Поддержка биометрической идентификации	–	–	+
Ввод специального идентификационного признака для открывания под принуждением	–	+	+

Окончание табл. 3.2

Функциональная характеристика	Класс системы		
	1	2	3
Подключение считывателей различных типов	–	+	+
Доступ по правилу двух (и более) лиц	–	+	+
Число событий, сохраняемых в энергонезависимой памяти контроллеров, не менее	1000	5000	10000
Возможность интегрирования с системами охранной и пожарной сигнализации на релейном уровне	+	–	–
Возможность интегрирования с системой видеоконтроля на релейном уровне	+	–	–
Возможность интегрирования с системами охранной и пожарной сигнализации и видеоконтроля на системном уровне	–	+	+
Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т. п.)	–	–	+
Обеспечение изображения на экране ЭВМ плана объекта и (или) помещений объекта с указанием мест расположения средств контроля доступа, охранной и пожарной сигнализации, средств видеоконтроля; графическое отображение тревожных состояний в контрольных точках на плане	–	+	+
Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	–	–	+
Ведение баз данных на пользователей	–	+	+
Поддержание фотографических данных пользователей в базе данных	–	–	+
Контроль за перемещением и поиск пользователей	–	–	+

Примечание. Знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «–» – отсутствие функции.

Системы КУД должны также иметь следующие характеристики:

– максимальное количество точек доступа, зон доступа, пользователей, обслуживаемых системой;

– максимальное количество точек доступа, обслуживаемых одним контроллером;

– максимальное количество контроллеров в системе;

– количество считывателей на один контроллер системы;

– количество и вид временных интервалов доступа, уровней доступа;

– количество типов считывателей, используемых в системе;

– время реакции системы на заявку на проход;

– максимальную длину линии связи с контроллерами и допустимые параметры линии связи;

– максимальное расстояние действия считывателя (для бесконтактных считывателей);

– максимальное время хранения информации о событиях в памяти системы;

– максимальную пропускную способность для системы в точках доступа;

– вероятность несанкционированного доступа, ложного задержания (для СКУД с биометрической идентификацией);

– показатели по уровням устойчивости к НСД.

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

Требования по устойчивости средств и систем КУД к НСД

Требования по устойчивости к НСД неразрушающего воздействия устанавливаются для средств КУД в зависимости от функционального назначения [71; 72] и включают в себя:

– устойчивость к вскрытию для УПУ и исполнительных устройств (замков и запорных механизмов);

– устойчивость к манипулированию;

– устойчивость к наблюдению для считывателей с запоминаемым кодом (клавиатуры, кодовые переключатели и т. п.);

– устойчивость к копированию идентификаторов.

Показатели устойчивости по данным требованиям и методы их испытаний должны быть установлены в стандартах и (или) технических условиях на средства КУД конкретного типа. Программное обеспечение сетевых систем должно быть защищено от несанкционированного доступа. Требования по защите программных средств систем КУД должны обеспечиваться средствами ограничения и администрирования доступа операционных систем управляющего компьюте-

ра СКУД и разграничением доступа к ПО СКУД. Рекомендуемые уровни защиты доступа к ПО с помощью паролей с разделением по типу пользователей следующие:

– первый («администратор») – доступ ко всем функциям;

– второй («дежурный оператор») – доступ только к функциям текущего контроля;

– третий («системный оператор») – доступ к функциям конфигурации программного обеспечения, без доступа к функциям, обеспечивающим управление УПУ.

Количество знаков в пароле должно быть не менее шести. При вводе пароля в систему знаки не должны быть видны на средствах отображения информации. После ввода в систему пароли должны быть защищены от просмотра средствами операционных систем ЭВМ.

Требования к надежности

На средства и системы КУД конкретного типа устанавливают такие показатели надежности [71], как средняя наработка на отказ (ч), среднее время восстановления работоспособного состояния (ч), средний срок службы (годы). При установлении показателей надежности должны быть указаны критерии отказа. Показатели надежности средств КУД устанавливаются исходя из необходимости обеспечения надежности системы в целом. По требованию заказчика на конкретные средства и системы могут быть установлены дополнительно другие требования по надежности.

Требования к электропитанию

Основное электропитание средств и систем КУД [71] должно осуществляться:

– от однофазной электросети переменного тока с номинальным напряжением 230 В (по ГОСТ 29322-2014), с отклонением напряжения в пределах от –20 до +10 % от номинального значения;

– источников электропитания постоянного тока с номинальным напряжением 12, 24 В, с отклонением напряжения не более ±15 % от номинального значения.

Электропитание отдельных средств КУД допускается осуществлять от других источников с иными параметрами выходных напряже-

ний, требования к которым устанавливаются в нормативных документах на конкретные типы средств. Средства и системы КУД должны иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервного источника питания может использоваться резервная сеть переменного тока или источники питания постоянного тока. Номинальное напряжение резервного источника питания постоянного тока выбирается из значений 12 или 24 В. Переход на резервное питание должен происходить автоматически, без нарушения установленных режимов работы и функционального состояния средств и систем КУД. Последние должны быть работоспособны при допустимых отклонениях напряжения резервного источника от –15 до +10 % от номинального значения. Резервный источник питания должен обеспечивать выполнение основных функций системы при пропадании напряжения в сети на время не менее 0,5 ч для систем первого и второго класса по функциональным характеристикам и не менее 1 ч – для систем третьего класса.

Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы и т. п.). При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания и иметь системные средства индикации аварии электропитания. При использовании в качестве источника резервного питания аккумуляторных батарей должен выполняться их автоматический заряд, также рекомендуется иметь индикацию разряда батареи ниже допустимого предела. Для автономных систем индикация разряда может быть световая или звуковая, для сетевых систем сигнал разряда батарей может передаваться на пункт управления. Химические источники питания, встроенные в идентификаторы или обеспечивающие сохранность данных в контроллерах, должны поддерживать работоспособность средств КУД в течение не менее 3 лет.

Выбор варианта оборудования объекта средствами КУД

Выбор варианта оборудования объекта средствами КУД следует начинать с его обследования [5]. При обследовании определяют характеристики значимости помещений объекта, его строительные и архитектурно-планировочные решения, условия эксплуатации, режи-

мы работы, ограничения или, наоборот, расширения права доступа отдельных сотрудников, параметры установленных (или предполагаемых к установке на данном объекте) средств, входящих в СКУД. По результатам обследования устанавливают тактические характеристики и структуру СКУД, а также составляют техническое задание на оборудование объекта СКУД. В техническом задании [1] указывают:

– описание системы и размещение составных частей системы;

– условия эксплуатации средств КУД;

– основные технические характеристики, такие как:

- пропускная способность в охраняемые зоны, особенно в час пик;
- максимально возможное число пользователей на один считыватель;
- максимальное число и виды идентификаторов;

– требования к маскировке и защите средств КУД от вандализма;

– оповещение о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;

– возможность работы и сохранения данных без компьютера или при его отказе;

– алгоритм работы системы КУД в аварийных и чрезвычайных ситуациях;

– программное обеспечение системы;

– требования к безопасности;

– требования к электропитанию;

– обслуживание и ремонт системы;

– требования к возможности включения системы КУД в интегрированную систему безопасности.

Архитектурно-планировочные и строительные решения. В ходе изучения чертежей, обхода и осмотра объекта, а также проведения необходимых измерений определяют:

– количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т. п.);

– материал строительных конструкций;

– количество отдельно стоящих зданий, их этажность;

– количество открытых площадок;

– количество отапливаемых и неотапливаемых помещений и их расположение.

Условия эксплуатации. Учитывать вредное воздействие окружающей среды следует лишь для исполнительных устройств, считывателей и контроллеров (совмещенных со считывателями в одном конструктивном блоке), предназначенных для работы вне отапливаемых закрытых помещений либо в особых условиях (запыленность, повышенная влажность, отрицательная температура, агрессивная среда и т. п.). Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удаленность считывателей и контроллеров от управляющего центра, заземление составных частей системы и т. п.

Дополнительные требования и методические рекомендации по выбору и применению СКУД при организации централизованной охраны банковских устройств самообслуживания (банкоматов, платежных терминалов) приведены в документе [39].

Сетевые СКУД предназначены для оборудования крупных объектов, таких как банки, крупные учреждения и офисные здания. Несомненное достоинство этих систем – возможность практически неограниченного расширения. Такие системы позволяют обслуживать десятки тысяч пользователей. Эффективность работы сетевых СКУД обусловлена возможностью создавать разветвленные, достаточно многочисленные соединения контроллеров и управляющих компьютеров в единую систему. Модульность построения данных систем обеспечивает:

– гибкость конфигурации;

– простоту монтажа, технического обслуживания и ремонта;

– возможность расширения системы;

– соотношение цена – качество;

– легкость сопряжения с устройствами сервисной автоматики (управление лифтом, освещением, системами кондиционирования и т. д.).

Соединение контроллеров между собой и подключение контроллера к различным периферийным устройствам, входящим в состав системы, обеспечиваются при помощи различных модулей. К одному контроллеру может быть подключено до восьми считывателей различных типов, например считыватель магнитных карточек,

считыватель бесконтактных карточек, клавиатура (кодонаборное устройство) и др. Подключение считывателей осуществляется через соответствующий считывающий модуль, работающий с двумя считывающими устройствами. Помимо считывателей он также контролирует датчики состояния дверей и кнопки их открывания, другие вспомогательные устройства. Информация о состоянии иных внешних устройств поступает в контроллер через модуль входа/выхода. Посредством этого же модуля контроллер управляет работой исполнительных устройств, устройством выдачи тревожных извещений. Модуль связи обеспечивает объединение контроллеров в единую систему протяженностью до 1 км с помощью интерфейса RS-485, а также при необходимости объединение контроллеров и управляющего компьютера в компьютеризированную систему с помощью интерфейса RS-232. Один контроллер может обслуживать до 10 000 пользователей. Для увеличения числа пользователей может применяться модуль расширения памяти.

При создании компьютерной сети контроллеры в количестве до 32 единиц могут быть объединены в одну ветвь. В этом случае модуль связи включается в первый по порядку контроллер ветви. Через него осуществляется связь этого контроллера с компьютером по интерфейсу RS-232. Обмен информацией между контроллерами происходит по интерфейсу RS-485. Кроме того, модуль связи осуществляет преобразование формата RS-232/RS-485. Каждый контроллер в ветви имеет свой адрес. Дальнейшее наращивание системы возможно путем организации нескольких (до 10) ветвей контроллеров. Модуль связи первого контроллера преобразовывает, с одной стороны, поток данных, посылаемых с управляющего компьютера на контроллер, а с другой – поток выходных данных, параллельно подаваемых на адресные модули связи в ветвях. Каждый адресный модуль связи обменивается данными с контроллерами в ветвях и другими модулями связи. Такая расширенная сеть позволяет обслуживать до 320 контроллеров и 2048 контролируемых точек.

В качестве исполнительных устройств могут использоваться электрозамки дверей, исполнительные устройства шлагбаумов, турникетов, устройства тревожного оповещения и освещения, телевизионные камеры и т. д. Логическое устройство (процессор) контроллера

позволяет производить необходимую установку параметров доступа в каждой контрольной точке при помощи программного обеспечения, т. е. конфигурирует систему. Системный оператор может задавать параметры (замкнутое/разомкнутое состояние контактов реле или кнопок, состояние и режим работы счетчиков, состояние регистров, временные интервалы регистраторов событий и т. д.) прямо с клавиатуры компьютера. Это дает возможность реализовывать различные варианты организации контроля и управления доступом, гибко меняя их в соответствии с текущими требованиями.

Программа предоставляет большие сервисные возможности оператору и выводит на экран разнообразную информацию. Например, на дисплее компьютера может отображаться план одного или нескольких помещений с обозначенными на нем контролируемыми точками, индикация несанкционированных проникновений (если требуется – со звуковым сопровождением). На экран могут выводиться многочисленные сообщения, например полные или краткие отчеты о зарегистрированных событиях, имеется возможность их распечатки на принтере.

Размещение технических средств СКУД на объекте

Общие рекомендации по выбору и применению СКУД приведены в методических рекомендациях [70]. Типовые проектные решения по размещению технических средств СКУД на защищаемом объекте приведены в документе [73].

Устройства центрального управления (персональные компьютеры), являющиеся «мозгом» СКУД, рекомендуется устанавливать в отдельных служебных помещениях, защищенных от доступа посторонних лиц, например в помещении службы безопасности или поста охраны объекта.

Основные положения, в соответствии с которыми разрабатываются режимы работы всей системы безопасности, определяются руководящим составом службы безопасности исходя из общей концепции обеспечения безопасности объекта. Управляющие программы загружаются в центральный управляющий и вспомогательные компьютеры или контроллеры и запираются секретными кодами.

Персонал охраны, а также других служб, которые подключены к общей компьютерной сети, не должен иметь доступа к программным средствам и возможности влиять на установленные режимы работы, исключение составляют лица, ответственные за данные работы.

При объединении компьютеров в сеть целесообразно распределять функциональные возможности среди пользователей сети и в соответствии с этим размещать компьютеры в помещениях объекта.

Устройства контроля и управления. Ведущие контроллеры и контроллеры, работающие на несколько устройств заграждения, рекомендуется размещать в специальных запираемых металлических шкафах или нишах на высоте, удобной для технического обслуживания. При этом следует дверцы данных шкафов или ниш блокировать охранной сигнализацией на возможное открытие или пролом. Контроллеры, совмещенные в одном корпусе с исполнительными или считывающими устройствами, рекомендуется оборудовать антисаботажными кнопками, предотвращающими несанкционированное вскрытие корпуса. Корпус данных контроллеров должен быть выполнен из ударопрочного материала для предотвращения актов вандализма. Контроллеры, управляющие работой считывателей или исполнительных устройств одной двери в двух направлениях, рекомендуется устанавливать с внутренней стороны охраняемого помещения.

Во избежание выхода контроллеров из строя или сбоев в работе не рекомендуется подключать их к источнику питания, от которого одновременно питается исполнительное устройство с большой индуктивностью обмоток, приводящее к броску напряжения по цепи питания. Для исключения этих нежелательных последствий необходимо предусматривать установку специальных демпфирующих устройств или элементов, гасящих импульсные помехи, вызванные ЭДС самоиндукции обмотки исполнительного устройства.

При работе устройств контроля и управления в сетевом режиме необходимо учитывать возможность появления помех и сбоев в работе из-за неправильного монтажа соединительных линий и нарушения ограничений по их длине.

Для нормальной работы СКУД рекомендуется:

– для шины RS-485 использовать высококачественный экранированный кабель «витая пара»;

– при значительной длине соединительного кабеля подключать к шине оконечные и согласующие элементы. Необходимое точное значение параметров этих элементов зависит от характеристик кабеля;

– заземлять устройства и экранированные оплетки кабелей в одной точке (во избежание возникновения блуждающих токов), желательно у ведущего контроллера. При большой длине кабелей заземление можно делать в разных точках, но при этом обязательно использовать специальные методы и устройства защиты от помех;

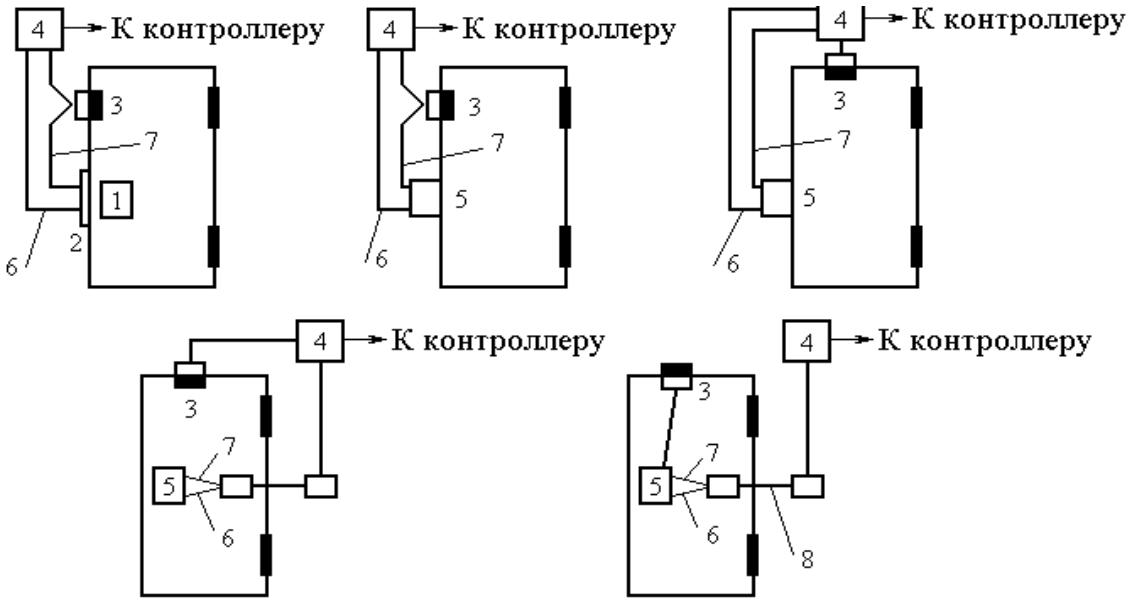
– использовать шинные усилители при большой длине кабеля.

Считыватели и исполнительные устройства

В зависимости от типа считывателей и исполнительных устройств, пропускной способности и организации системы безопасности объекта в целом считыватели и УИ могут устанавливаться как вблизи устройств заграждения, так и непосредственно на них. При их размещении необходимо учитывать условия эксплуатации, удобство монтажа, надежность и вандалостойкость [70; 71].

Считыватели «Proximity» удобнее всего размещать на стене, скрытно в стене, перед устройствами заграждения или даже с внутренней стороны устройства заграждения, например на внутренней стороне неметаллической двери, если ее толщина не превышает 10 см. При монтаже считывателя на металле рекомендуется, чтобы между основанием считывателя и металлической поверхностью расстояние было не менее 25 мм.

В случае, когда стена, за которой установлен считыватель, оказывается слишком толстой или изготовлена из металла (содержит металлическую арматуру), считыватель допускается устанавливать на расстоянии, на котором должна быть обеспечена необходимая защита от возможного несанкционированного прохода. Варианты размещения исполнительных устройств на дверных конструкциях представлены на рисунке.



Варианты размещения исполнительных устройств на дверных конструкциях: *1* – механический замок; *2* – электромагнитная защелка; *3* – магнитоконтактный датчик открытия двери (СМК); *4* – соединительная коробка; *5* – электромеханический или электромагнитный замок; *6* – кабель питания замка (для дверей из сгораемого материала двойная изоляция ПХВ или металлорукав); *7* – цепи управления и контроля; *8* – гибкий переход (кабелепровод)

Считыватели магнитных, Виганд-карточек, электронных ключей и клавиатуры также рекомендуется размещать на стене или непосредственно на устройстве заграждения на высоте, удобной для пользования. Считыватели магнитных карточек (за исключением совмещенных с исполнительными устройствами) во избежание помех или выхода их из строя не рекомендуется устанавливать в непосредственной близости от мощных исполнительных устройств, создающих сильные электромагнитные поля (соленоидные, магнитные замки и т. п.).

Электромагнитные защелки рекомендуется монтировать в косяк дверной коробки. Данная установка позволяет блокировать ригель замка, установленного в двери, при закрывании двери и разблокировать замок при подаче сигнала от контроллера. Кроме того, такая установка защелки позволяет полностью сохранить замочно-скобяную фурнитуру двери.

Электромеханические замки рекомендуется устанавливать на деревянных и металлических дверях массой до 100 кг при условии средней нагруженности (до 100 – 200 проходов в день). Применение этих замков для дверей с высокой нагруженностью неэффективно по причине высокого механического износа и, как следствие, снижения надежности и срока службы. Чаще всего электромеханические замки устанавливают на двери (накладной или врезной замок), но иногда и на дверной коробке.

Электромагнитные замки рекомендуется устанавливать на деревянных и металлических дверях массой до 650 кг в условиях высокой нагруженности (более 200 проходов в день). Отсутствие деталей, подверженных трению и износу, делает этот замок практически вечным. Особенность данного замка – необходимость постоянной подачи тока на обмотку его электромагнита, так как при пропадании напряжения питания, например при аварии или умышленном обрыве проводов, замок открывается. В связи с этим для надежной работы необходимо дублирование его механическим замком или применение дополнительного резервного питания. При совместном использовании магнитоконтактных извещателей (типов ИО 102-4, ИО 102-5, ИО 102-6, ИО 102-14, ИО 102-15/1, ИО 102-20) в качестве датчиков положения двери с электромагнитными и электромеханическими замками они должны быть разнесены друг от друга как можно дальше.

При установке исполнительных устройств (замки, доводчики, приводы и т. п.), требующих для своей работы подводки электропитания, необходимо использовать специальные устройства и кабели, обеспечивающие электро- и пожаробезопасность (особенно на сгораемых конструкциях), а также защиту от повреждений при открытии/закрытии дверей (гибкие кабелепроводы).

Электропроводка технических средств СКУД

Электропроводка технических средств СКУД представляет собой совокупность кабельных линий и линий проводов электрических соединителей, трубопроводов и коробов, проложенных и закрепленных на элементах зданий и сооружений, устройств их крепления и защиты от механических повреждений [70; 71]. Следует помнить, что при большой длине электропроводки (более 50 м) для борьбы с электромагнитными помехами необходимо использовать экранированные

кабели и провода, витые пары. Сечение (диаметр) проводников выбирается исходя из длины электропроводки и нагрузки. Кроме того, выбор видов электропроводки, проводов, кабелей, труб и коробов с проводами и кабелями и способов их прокладки должен осуществляться с учетом требований электро- и пожарной безопасности.

Электропроводка СКУД подразделяется:

– на проводные линии (цепи сигнализации и управления, шины данных, интерфейсные шины), обеспечивающие связь между исполнительными устройствами, считывателями, контроллерами и компьютерами;

– низковольтные цепи питания (12/24 В постоянного тока);

– высоковольтные цепи питания (230/400 В переменного тока частотой 50 Гц).

Монтаж электропроводок должен выполняться в соответствии с проектом (актом обследования и типовыми проектными решениями) и с учетом требований ПУЭ, СП 76.13330.2016. При открытой параллельной прокладке проводов или кабелей линий связи и силовых линий питания и освещения расстояние между ними должно быть не менее 0,5 м, в противном случае должна быть обеспечена защита от наводок. Это требование относится и к низковольтным цепям питания, если они запитывают мощные индуктивные нагрузки (электромагниты, соленоиды и т. п.) устройств заграждения. Трассы проводок необходимо выбирать наикратчайшими, с учетом расположения электроосветительных, радиотрансляционных сетей, водопроводных и газовых магистралей, а также других коммуникаций. Прокладка проводов и кабелей по стенам внутри охраняемых зданий должна проводиться на расстоянии не менее 0,1 м от потолка и, как правило, на высоте не менее 2,2 м от пола. При прокладке проводов и кабелей на высоте менее 2,2 м от пола должна быть предусмотрена их защита от механических повреждений [70].

Электропроводки, проходящие по наружным стенам на высоте менее 2,5 м или через помещения, которые не подлежат защите, должны быть выполнены скрытым способом или в металлических трубах. При пересечении силовых и осветительных сетей кабели и провода СКУД должны быть защищены резиновыми или полихлорвиниловыми трубками, концы которых должны выступать на 4 – 5 мм с каждой стороны перехода. При пересечении кабели большей емко-

сти должны прилегать к стене, а меньшей емкости – огибать их сверху. Кабели меньшей емкости допускается пропускать под кабелями большей емкости при прокладке их в штробах. Не допускается прокладка по стенам распределительных кабелей емкостью более 100 пар.

При выполнении скрытой проводки в полу и междуэтажных перекрытиях кабели должны прокладываться в каналах и трубах. Заделка кабелей в строительные конструкции наглухо не допускается. На прокладку скрытой проводки составляется акт. При прокладке кабелей в местах поворота под углом 90° (или близких к нему) радиус изгиба должен быть не менее семи диаметров кабеля. Кабели и провода должны крепиться к строительным конструкциям при помощи скреб или скоб из тонколистовой оцинкованной стали, полиэтиленовых эластичных скоб. Установка крепежных деталей должна проводиться с помощью шурупов или клея. При прокладке нескольких проводов по одной трассе допускается располагать их вплотную друг к другу.

Для соединения и ответвления провода и шин рекомендуется применять распределительные и соединительные коробки. Расстояние от кабелей и изолированных проводов, прокладываемых открыто, непосредственно по элементам строительной конструкции помещения, до мест открытого размещения (хранения) горючих материалов должно быть не менее 0,6 м. При пересечении проводов и кабелей с трубопроводами расстояние между ними «в свету» должно быть не менее 50 мм, а с трубопроводами, содержащими горючие или легковоспламеняющиеся жидкости и газы, – не менее 100 мм. При параллельной прокладке расстояние от проводов и кабелей до трубопроводов должно быть не менее 100 мм, а до трубопроводов с горючими или легковоспламеняющимися жидкостями и газами – не менее 400 мм.

Прокладка электропроводки в трубах

Применяемые для электропроводки стальные трубы должны иметь внутреннюю поверхность, исключающую повреждение изоляции проводов при их затягивании в трубу. Стальные трубы, прокладываемые в помещениях с химически активной средой, внутри и снаружи должны иметь антикоррозийное покрытие, стойкое в условиях

данной среды. В местах выхода проводов из стальных труб следует устанавливать изоляционные втулки. Для ответвления и соединений стальных трубных проводок как открытых, так и скрытых следует применять коробки, ящики и т. п. Расстояние между протяжными коробками (ящиками) не должно превышать:

– 50 м (при наличии одного изгиба труб);

– 40 м (при наличии двух изгибов труб);

– 20 м (при наличии трех изгибов труб).

Расстояние между точками крепления открыто проложенных стальных труб как на горизонтальных, так и на вертикальных поверхностях не должно превышать:

– 2,5 м (для труб с условным проходом до 20 мм);

– 3 м (для труб с условным проходом до 32 мм);

– 4 м (для труб с условным проходом до 80 мм);

– 6 м (для труб с условным проходом до 100 мм).

Расстояние между точками крепления металлорукавов не должно превышать:

– 0,25 м (для металлорукавов с условным проходом до 15 мм);

– 0,35 м (для металлорукавов с условным проходом до 27 мм).

Трубы с электропроводкой должны быть закреплены на опорных конструкциях на расстоянии от ввода:

– в приборы – не далее 0,8 м;

– соединительные и протяжные коробки – не далее 0,3 м;

– гибкие металлические рукава – 0,5 – 0,75 м.

Приваривать стальные трубы к металлоконструкциям не допускается. Прокладку проводов и кабелей в неметаллических (пластмассовых) трубах следует выполнять в помещениях при температуре воздуха не ниже –20 и не выше +60 °С.

Применяемые для защиты электропроводки от механических повреждений трубопроводы должны изготавливаться из негорючих, трудносгораемых материалов с нагревостойкостью не менее 105 °С согласно требованиям ГОСТ 8865-93 (МЭК 85-84). Неметаллические трубы, прокладываемые открытым способом, должны крепиться так, чтобы было возможно их свободное перемещение при линейном расширении или сжатии в результате изменения температуры окружающей среды. Крепление следует выполнять скобами, хомутами и

накладками. Расстояние между точками крепления открыто проложенных полимерных труб не должно превышать:

– 1 м (для труб диаметром 20 мм);

– 1,1 м (для труб диаметром 25 мм);

– 1,4 м (для труб диаметром 32 мм);

– 1,6 м (для труб диаметром 40 мм);

– 1,7 м (для труб диаметром 50 мм).

Изменение направлений защитных труб осуществляется изгибом. При изгибе труб, как правило, следует применять нормализованные углы поворота (90, 120 и 135°) и нормализованные радиусы изгиба (400, 800 и 1000 мм).

Прокладка электропроводки напряжением 220 В

Для электроснабжения технических средств СКУД допускается использовать следующие провода и кабели:

– провода марок ПВ, АПВ, ПРГ: прокладываются в металлических трубах и металлорукавах;

– провода марки ППВ: прокладываются открыто по несгораемым основаниям, а по сгораемым основаниям – с подкладкой листового асбеста толщиной 3 мм;

– провода марки АППВ: прокладываются скрыто в слое штукатурки;

– кабели марок ВРГ, ВВГ, АВГ, АВРГ: прокладываются внутри помещений, в каналах, тоннелях, агрессивной среде, при отсутствии механических воздействий. Кроме того, допускается использовать провода и кабели, входящие в комплект поставки, если это не противоречит противопожарным нормам.

При монтаже электропроводки не допускается:

– применять неизолированные электрические провода;

– использовать кабели и провода с поврежденной изоляцией;

– объединять слаботочную и сильноточную электропроводку в одной защитной трубе;

– перекручивать, завязывать провода; заклеивать участки проводов и кабелей бумагой (обоями); использовать плинтусы, оконные и дверные деревянные рамы.

Соединение, ответвление и оконцевание жил проводов и кабелей должны проводиться при помощи опрессовки, сварки, пайки или

сжимов (винтовых, болтовых и т. п.). В местах соединения, ответвления и присоединения жил проводов или кабелей должен быть предусмотрен запас провода (кабеля), обеспечивающий возможность повторного соединения, ответвления. Соединение и ответвление проводов и кабелей, за исключением проводов, проложенных на изолирующих опорах, должны выполняться в соединительных и ответвительных коробках, внутри корпусов технических средств. Не допускается применение винтовых соединений в местах с повышенной вибрацией или влажностью. В местах прохождения проводов и кабелей электроснабжения технических средств СКУД через стены или перекрытия должны быть предусмотрены огнестойкие уплотнения (асбест, шлаковата, песок и т. п.). Прокладка кабелей в сооружениях подземной канализации должна проводиться в соответствии с проектом и оформляться актом. Марки, сечения и число прокладываемых проводов и кабелей, а также размеры труб в каждом отдельном случае определяются проектом в зависимости от материала труб, способа их прокладки и окружающей среды. Электропроводка в трубах может состоять из одной или нескольких электрических цепей и прокладываться на значительном протяжении по совместной трассе. Работы по монтажу электропроводки в трубах выполняются в определенной технологической последовательности.

Затягивание проводов в трубы происходит с помощью проволоки или троса. Перед этим удаляют со свободных концов труб пробки и заглушки, проверяют трубопровод продуванием воздуха, вдувают в него тальк (для уменьшения трения провода о стенки труб) и затягивают протяжную стальную ленту, или стальную спираль с шариком на конце, или стальную проволоку диаметром 1,5 – 3,5 мм с петлей на конце. Протяжную проволоку проталкивают в трубу со стороны одной из коробок или с конца трубы, а протяжной трос затягивают с помощью специального гибкого шланга. На конец трубопровода устанавливаются втулки для предохранения изоляции проводов от повреждения. Провода с большими сечениями затягиваются в трубы с помощью специальных захватов, небольших лебедок, универсального электромонтажного привода и других приспособлений (рычажных, пневматических). Для облегчения затягивания проводов в протяженные трубопроводы с большим числом изгибов дополнительно устанавливаются соединительные коробки или ящики. В вертикально

проложенные трубы провода затягивают снизу вверх и закрепляют изоляционными клипсами или зажимами (при сечении проводов 50 мм^2 – через 30 м, при сечениях 70 – 150 мм^2 – через 20 м и при сечениях 185 – 240 мм^2 – через 15 м).

Контрольные вопросы

1. Приведите классификацию СКУД по техническим и функциональным признакам.
2. Опишите принцип функционирования одной точки прохода.
3. Перечислите требования по проектированию и размещению в защищаемых помещениях элементов СКУД.
4. Какие действия с носителями идентификационных признаков могут привести к несанкционированному преодолению СКУД?
5. Какова защищенность и уязвимость различных типов идентификаторов от несанкционированного доступа?
6. Назовите разновидности и принципы действия бесконтактных идентификаторов.
7. Какие формы передачи данных распространены в СКУД?
8. На чем основаны биометрические методы идентификации?
9. Опишите способы идентификации на основе квазидинамических признаков.
10. Перечислите основные требования к исполнительным устройствам СКУД.
11. Перечислите основные требования к устройствам идентификации доступа.
12. В чем заключается специфика построения СКУД для автономного режима работы? Приведите типовой состав оборудования СКУД.
13. В чем заключается специфика построения СКУД для сетевого режима работы? Приведите типовые структурные решения таких систем.
14. Охарактеризуйте исполнительные устройства, применяемые для контроля доступа людей в помещения.
15. Назовите основные требования к обеспечению электропитания элементов СКУД.

Глава 4. ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ВИДЕОНАБЛЮДЕНИЯ

Общие положения

Выбор варианта оборудования объекта СОТ следует начинать с его обследования [5]. При этом определяются характеристики значимости объекта, его строительные и архитектурно-планировочные решения, условия эксплуатации СОТ, параметры установленных (или предполагаемых к установке на данном объекте) систем сигнализации и управления доступом. По результатам обследования выявляются тактические характеристики и структура СОТ, а также технические характеристики ее компонентов. При определении категории значимости объекта или его частей (зон) принимаются во внимание:

– производственное назначение объекта в целом и его отдельных зон (помещений, открытых площадок и т. п.);

– характер размещения и сосредоточения предметов преступных посягательств (денежных средств и ценностей, оружия и боеприпасов, наркотических веществ и т. п.);

– степень тяжести возможных финансовых, политических либо социальных последствий несанкционированного проникновения или разбойного нападения на объект.

Архитектурно-планировочные и строительные решения. В ходе изучения чертежей, обхода и осмотра объекта, а также в ходе проведения необходимых измерений определяются:

– конфигурация границ (периметра) объекта;

– количество отдельно стоящих зданий, их этажность;

– количество открытых площадок;

– количество отапливаемых и неотапливаемых помещений;

– геометрические размеры (площадь, линейные размеры, высота потолков и т. п.) помещений, открытых площадок, сторон периметра.

Условия эксплуатации. Учитывать воздействие внешних факторов следует лишь для передающей части СОТ, предназначенной для работы вне отапливаемых закрытых помещений либо в особых условиях (запыленность, повышенная влажность, электромагнитные помехи и т. п.). Кроме того, необходимо знать местоположение зон объекта на местности (ориентация в осях север – юг, запад – восток),

чтобы избежать прямых засветок камер солнечным светом. При интегрировании СОТ с системами сигнализации и управления доступом следует учитывать:

– возможность их совместимости;

– интеграции на релейном, а также программно-аппаратном уровнях;

– организации интерфейсов RS-232 и RS-485 (при значительной удаленности панелей систем сигнализации и управления доступом);

– состояние выходов тревоги средств сигнализации и управления доступом в различных режимах. Отечественные и большинство зарубежных средств охранной сигнализации имеют в дежурном режиме замкнутые контакты, которые размыкаются при тревоге.

Общие технические требования к охранным телевизионным системам изложены в ГОСТ [79]. Типовые проектные решения по организации СВН на охраняемом объекте приведены в документе [74], для тепловизионного оборудования – в документе [75]. Рекомендации по организации передачи телевизионных изображений по различным каналам связи на ПЦО приведены в документе [76]. Применение охранных телевизионных систем в условиях действия дестабилизирующих факторов и плохой видимости описано в рекомендациях [78]. Типовые проектные решения по оснащению объектов системами охранного телевидения изложены в документе [77]. Правильный выбор камер – принципиально самый важный момент при проектировании системы, так как именно характеристики камер определяют в конечном счете характеристики других компонентов. При выборе телекамеры и места ее установки учитываются:

– значимость зоны наблюдения и геометрические размеры зоны;

– необходимость идентификации наблюдаемого предмета и ориентация зоны наблюдения на местности;

– освещенность объекта наблюдения и расположение уязвимых мест (окон, дверей, люков и т. п.);

– условия эксплуатации и тип наблюдения (скрытое или открытое).

Требования к техническим параметрам камер следующие:

– разрешение черно-белых камер должно быть не менее 420 ТВЛ;

– разрешение цветных камер должно быть не менее 380 ТВЛ;

– для внешних камер (особенно при охране периметра протяженных объектов) желательно использовать низкоуровневые камеры (чувствительность свыше 0,1 лк при количестве кадров не менее 25 в секунду на канал), поскольку уровень освещенности на объекте может быть резко снижен в результате ухудшения погодных условий или диверсии против системы освещения;

– в перспективных системах должны использоваться мегапиксельные матрицы с прогрессивной разверткой.

Камеры с прогрессивной разверткой изображение по кадрам выводят сразу, в отличие от обычных камер, которые выводят изображение по полукадрам. В настоящее время камеры с прогрессивной разверткой создают чаще всего на базе CMOS-матрицы. К сожалению, мегапиксельные матрицы на базе прибора с зарядовой связью (ПЗС) разрабатывают только в единичных случаях для использования в специальных приложениях.

Примечание. CMOS-матрицы обладают большими шумами и низкой чувствительностью по сравнению с ПЗС-матрицами. К положительным чертам первых матриц следует отнести мегапиксельный формат (переход на структуру CMOS позволяет производить такие матрицы относительно просто и дешево), возможность высокоскоростной съемки (порядка 500 кадров в секунду), вывод изображения сразу по целому кадру. Геометрические размеры зоны определяют угол зрения камеры. В охране входной двери, помещений, открытых площадок применяются широкоугольные камеры с углом зрения 60 – 90° либо камеры с меньшими углами зрения, устанавливаемые на поворотных платформах. В охране периметров используют камеры с малыми углами зрения. Угол зрения камеры можно определить по формуле $\alpha = 2\text{arctg}(\frac{h}{2f})$, где α – угол зрения по горизонтали; h – размер матрицы и f – фокусное расстояние объектива.

В таблице приведены усредненные значения углов зрения камер с различными форматами матриц и объективами с разными фокусными расстояниями. (Следует заметить, что углы зрения изделий разных фирм могут несколько отличаться от приведенных в таблице.)

Усредненные значения углов зрения камер с различными форматами матриц и объективами с разными фокусными расстояниями

Тип исполнения матрицы / Фокусное расстояние, мм	1/3”	1/2”	2/3”	1”
2,8	98°	–	–	–
4	64	86°	–	–
6	42	58	–	–
8	33	42	55°	–
12	2	30	–	–
16	17	23	30	43°
25	11	14	19	28
50	5,5	7	10	15
75	3,6	5	6,6	10
100	–	–	5	–
150	–	–	–	4,9
235	–	–	–	3,1
350	–	–	–	2,1

Идентификация наблюдаемого предмета. На объектах особой важности, как правило, требуется идентификация личности или номера автомобиля при входе или несанкционированном проникновении в важные зоны, такие, например, как банковские хранилища, помещения для хранения оружия либо наркотиков, боксы для инкассаторских машин, стоянки служебного автотранспорта и т. п. С этой целью применяют камеры с повышенным разрешением либо камеры, оснащенные длиннофокусными объективами и имеющие малые углы зрения. Для получения более полной информации об объекте наблюдения (например, идентификация цвета автомобиля, глаз, волос, одежды и т. п.) используются камеры цветного изображения. Основное требование, предъявляемое к цветным камерам, – правильная передача цветов. Для компенсации искажений цветопередачи при изменении источников света в камерах применяются специальные схемы баланса белого. В большинстве камер регулировка баланса белого осуществляется автоматически. В хороших камерах, как правило, имеются регулировки для адаптации к разным источникам света. Если в соответствии с геометрическими размерами зоны уже выбран требуемый

угол зрения камеры, то минимальный размер объекта (детали объекта) можно определить так: $S = 150L\text{tg}\left(\frac{0{,}5\alpha}{R}\right)$, где L – расстояние от камеры до наблюдаемого объекта, м; α – угол обзора камеры; R – разрешение камеры, ТВЛ.

На практике может оказаться, что камера с выбранным углом зрения не позволяет получить требуемую для идентификации объекта наблюдения детализацию даже при использовании камеры с повышенным разрешением, а применение камеры с меньшими углами зрения может оставить часть зоны без наблюдения. Это характерно для больших помещений и открытых площадок (например, автостоянок), а также периметров большой протяженности. В таких случаях применяют камеры с вариообъективами, позволяющими изменять фокусное расстояние и угол зрения. В нормальном режиме, когда в зоне нет нарушения, устанавливается малое фокусное расстояние объектива, камера имеет широкий угол зрения и под наблюдением находится вся зона. При возникновении тревожной ситуации в зоне (либо по желанию оператора) фокусное расстояние объектива увеличивается, что позволяет «приближать» интересующий предмет (ZOOM-функция) настолько, чтобы можно было его идентифицировать. Для правильного выбора вариообъектива необходимо определить границы изменения его фокусного расстояния. Нижняя граница $f_{\min}$ выбирается исходя из требуемого угла зрения камеры в нормальных условиях. Верхнюю границу фокусного расстояния $f_{\max}$ можно определить так: $f_{\max} = \frac{75Lh}{SR}$.

Следующая важная для идентификации объекта характеристика камеры – возможность компенсации заднего света (Back Light Compensation), которая позволяет получить, например, качественное изображение лица человека, стоящего спиной к источнику света, в то время как обычная камера даст только темный силуэт. Вся автоматика в таких камерах ориентируется не на среднюю освещенность всего кадра, а на центральную часть экрана (в очень дорогих камерах размер и положение этой области программируется специальным образом). Развитие этой идеи привело к использованию метода дифференциального усиления. Он позволяет получить одинаково хорошее изображение даже в резко различающихся ярких и темных областях кадра (например, различить лицо человека на переднем плане и лица или фигуры людей на заднем плане). В последние годы все чаще вме-

сте с видеонаблюдением используется и аудионаблюдение, что позволяет идентифицировать объект по голосу. Некоторые современные камеры имеют встроенный микрофон либо микрофон и динамик, что обеспечивает организацию соответственно симплексного или дуплексного канала аудиосвязи.

Аудиоканал позволяет прослушивать охраняемую зону, что может оказаться важным при возникновении в ней тревожной ситуации. Если видеоизображения предполагается использовать для целей криминалистических исследований:

– необходимо учитывать, что структура построения СОТ, подбор ее функциональных возможностей, а также выбор параметров функциональных узлов, входящих в СОТ, вопросы установки СОТ, освещенность охраняемой зоны должны оцениваться с точки зрения качества записываемого изображения;

– изображения, получаемые при помощи СОТ, должны отображать максимально возможное число признаков, идентифицирующих объекты;

– СОТ с цифровым видеонакопителем должна аппаратно обеспечивать получение кадра на выходе системы с разрешением не ниже 704×576 пикселей;

– СОТ должна обеспечивать запись на видеонакопитель не менее 256 градаций серого;

– недопустима недостаточная или избыточная освещенность объекта (блики, резкие тени), что делает невозможным выявление на изображении индивидуализирующих признаков объекта. Указанное требование необходимо учитывать при монтаже системы и организации освещения охраняемой зоны и наблюдаемых объектов;

– телекамеры СОТ необходимо устанавливать по возможности максимально близко к горизонтальной визирной линии по отношению к фиксируемому объекту наблюдения, т. е. отклонение СОТ от горизонтальной визирной линии должно составлять не более 15°;

– значение разрешения системы должно составлять не менее 450 ТВЛ для цветных камер;

– значение разрешения системы должно составлять не менее 500 ТВЛ для черно-белых камер;

– быстрота реакции системы должна обеспечивать включение камеры до появления объекта в охраняемой в зоне (например, при подаче сигнала тревоги от охранного датчика);

– режим записи должен быть 25 кадров в секунду по каждому каналу;

– при монтаже системы и установке режимов работы необходимо учитывать скорости перемещения объектов, находящихся в зоне видимости камеры, с тем чтобы исключить появление нерезких смазанных изображений на записанных видеокадрах.

Освещенность на объекте

Освещенность наблюдаемого объекта может быть различной и, кроме того, может изменяться произвольным образом. Она зависит от времени суток, погоды, прозрачности воздуха. При выборе камеры важно знать такие параметры объекта, как минимальная освещенность и диапазон изменения освещенности. Исходя из значения минимальной освещенности выбирают камеру с соответствующей чувствительностью. Однако здесь могут возникнуть сложности, вызванные тем, что приводимая в паспорте на камеру характеристика чувствительности трактуется неоднозначно. Во-первых, может быть приведена освещенность, при которой камера даст приемлемое либо нормальное изображение. Эти значения могут различаться в 2 – 4 раза. Во-вторых, ряд фирм проводит измерения без специального фильтра ИК-отсечки, что завышает чувствительность камеры. И, наконец, в одних случаях приводится освещенность на объекте ($E_{об}$), а в других – на матрице ($E_{матр}$). Эти величины связаны между собой выражением $E_{матр} = \frac{E_{об}R}{\pi F^2}$, где R – коэффициент отражения объекта; F – относительное отверстие объектива. Разница между значениями этих величин существенная: первая может превышать вторую в 10 раз.

Такая неоднозначность может привести к серьезной ошибке при выборе камеры, поэтому перед приобретением необходимо выяснить, какая из величин указана в документации, а более правильное решение – получить подробную консультацию у специалиста. Следует отметить, что освещенность объекта сильно влияет на разрешение, поэтому для объектов с очень низкой освещенностью следует выбирать камеры с повышенными чувствительностью и разрешающей способностью. Применять сверхвысокочувствительные камеры, представляющие собой комбинацию обычной камеры и прибора ночного видения и имеющие чувствительность в 100 – 10 000 раз выше обыч-

ных, следует с большой осторожностью (а лучше отказаться от них) из-за высокой цены, низкой надежности и очень сложной и неудобной эксплуатации. В частности, их нельзя применять днем (и рекомендуется даже закрывать их объектив в дневное время).

Кроме обычного (видимого) освещения для подсветки объектов используют осветители инфракрасного спектра. Современные матрицы камер имеют спектральную характеристику, существенно сдвинутую в область ближнего ИК-излучения, что позволяет использовать ИК-подсветку, невидимую человеческим глазом. В большинстве современных ИК-осветителях используются ИК-светодиоды, пришедшие на смену прожекторам на основе галогенных ламп накаливания с дисперсионными фильтрами из ИК-стекла, которые поглощают видимую часть спектра. В ИК-осветителях используют светодиоды со световым излучением 850 – 880, 920 – 930 и 940 – 950 нм. Наиболее эффективно применение осветителей с более короткой длиной волны. Это связано с большей чувствительностью матриц в этом диапазоне. Питание ИК-осветителей следует производить от стабилизированных источников постоянного напряжения или можно использовать ИК-осветители, имеющие встроенные стабилизаторы. При работе с ИК-подсветкой следует обратить внимание на то, что коэффициент отражения различных предметов и объектов в ИК-области значительно отличается от коэффициентов отражения при дневном освещении. Так, растения, косметика, материалы одежды, окраска зданий и машин могут создавать значительные искажения в полученном изображении. Этому способствует и монохромный характер излучения ИК-осветителя. Следует учесть, что при ИК-свете изменяется фокусное расстояние объектива видеокамеры. Это может привести к размытости изображения, поэтому необходимо проверять качество фокусировки объектива как в дневное время, так и при ИК-свете.

При использовании телекамер со встроенными ИК-светодиодами в кожух камеры может наблюдаться отражение ИК-излучения от защитного стекла кожуха, крупных частиц пыли и снега, находящихся перед объективом, что отрицательно сказывается на контрастности изображения, поэтому использование внешних ИК-излучателей предпочтительно. В СОТ необходимо применять источники освещения с резервным питанием и возможностью увеличения светового потока

при неблагоприятных условиях не менее чем в 3 раза. Диапазон изменения освещенности необходимо учитывать, как правило, при выборе камер для наружного наблюдения. Для этих целей в системах общего применения выбирают камеры с электронным затвором или электронной диафрагмой, позволяющими компенсировать 1000- или даже 2000-кратные превышения освещенности (диапазон регулирования 1/50 – 1/50 000 или 1/50 – 1/100 000).

Размещение камеры в наблюдаемой зоне

Важную роль в обеспечении нормальной работы камеры играет место установки камеры на объекте [74; 77]. При этом нужно обратить внимание на два момента. Во-первых, следует по возможности исключить засветки объектива прямым или отраженным солнечным светом либо мощными источниками искусственного освещения, например прожекторами. И, во-вторых, нужно ориентировать камеру таким образом, чтобы в поле зрения попадали все уязвимые места (окна, двери, люки и т. п.), а размеры непросматриваемой зоны не позволяли нарушителю проникнуть через нее. Если уязвимые места не просматриваются одной камерой (угол зрения которой по горизонту не должен превышать 90º), то необходимо установить несколько телекамер. Для того чтобы избежать засветок, рекомендуется:

– не ориентировать камеру в южную сторону;

– устанавливать камеру на потолке либо на стене или в углу с наклоном её вниз (если предполагается использовать запись с данной камеры для проведения криминалистической экспертизы, то угол наклона к горизонту не должен превышать 15º);

– использовать корпус или кожух с защитным козырьком и фильтром;

– не направлять камеру на блестящие, хорошо отражающие свет предметы (зеркала, лужи и т. п.), окна.

Если не удается уменьшить размеры непросматриваемой зоны до такой степени, чтобы в ней не мог перемещаться человек, камеру следует устанавливать в таком месте, чтобы в эту зону не попадали уязвимые места (окна, двери и т. п.). Кроме того, при размещении камеры нужно стремиться к тому, чтобы длина питающих и сигнальных кабелей была минимальной.

Требования к аппаратуре постов управления и каналам передачи видеосигнала

Информация от камер по каналам передачи видеосигнала поступает на пост управления, где она коммутируется, обрабатывается, отображается и регистрируется с помощью специальных аппаратных и программных средств [75; 76]. Таких постов в системах высшего и среднего классов может быть несколько, включая и удаленные на значительные расстояния (в системах общего применения, как правило, такая структура не требуется). Точные параметры аппаратуры поста управления, аппаратный состав, функциональные возможности, электрические характеристики и тому подобное можно определить, только учитывая требования заказчика и результаты обследования объекта. При выборе аппаратуры следует обратить особое внимание на следующее:

– вся аппаратура должна соответствовать одним и тем же стандартам черно-белого и цветного телевидения;

– разрешающая способность АПУ должна быть выше, чем у камер, используемых в системе.

С развитием СОТ состав показателей их работы, функциональные возможности и другие характеристики могут изменяться. Видеоусилители применяют для компенсации затухания видеосигнала в линиях при передаче его на большие расстояния. При выборе видеоусилителя необходимо знать его входное и выходное сопротивления, а также коэффициент усиления, так как их значения обусловливают тип линии передачи и максимальное расстояние, на которое можно передать видеосигнал. Видеораспределители используют при необходимости трансляции видеосигнала нескольким потребителям. Основные характеристики видеораспределителей – входное и выходное сопротивления, количество выходов (количество возможных потребителей), амплитудно-частотная характеристика (АЧХ), фазочастотная характеристика (ФЧХ), полоса пропускания видеотракта. Для видеоусилителей важный показатель – возможность и количество независимых регулировок усиления по частоте в диапазоне передачи видеосигнала.

Электропитание СОТ

Электропитание всей СОТ должно быть организовано таким образом, чтобы обеспечивать работоспособность системы в автономном режиме, т. е. при пропадании напряжения сети переменного тока [74; 79]. С этой целью питание компонентов осуществляют от источников бесперебойного питания UPS или специализированных, снабженных аккумуляторами блоков питания. Для питания мониторов и других компонентов СОТ также часто используют инверторы – приборы, преобразующие постоянный ток напряжением 12 В в переменный ток напряжением 220 В и частотой 50 Гц. При построении СОТ ее компоненты следует выбирать таким образом, чтобы номенклатура питающих напряжений и потребляемая мощность (ток) были минимальными.

Организация питания телекамер – одна из проблем в системах с беспроводными каналами связи. С одной стороны, можно подавать питание камерам по проводам, но тогда проблема прокладки проводов остается. С другой – можно питать камеры от аккумуляторов, однако из-за большого потребления даже у современных камер (200 – 400 мА) приходится часто заменять элементы питания.

Заземление оборудования и устройств СОТ должно выполняться в соответствии с требованиями СНиП, ПУЭ, технической документации предприятий-изготовителей на оборудование. При отсутствии резервного внешнего электропитания (дополнительного сетевого фидера) необходимо обеспечить автономное электропитание СОТ от бензогенератора (дизель-генератора). Мощность бензогенератора должна обеспечить как питание СОТ, так и дежурное освещение, необходимое для нормальной работы внешних и внутренних телекамер.

Технические решения, использованные при заземлении, во многом определяют качество работы СОТ. При организации заземления следует руководствоваться следующими принципами:

– все сигнальные цепи СОТ и устройства грозозащиты должны иметь одну точку заземления. Лучше осуществлять такое заземление на приемной части оборудования;

– должно осуществляться заземление, а не зануление, т. е. общая точка заземления СОТ должна быть подключена на земляную шину, а не на «нуль» сети;

– если корпус видеокамеры имеет контакт с экраном линии связи или разъем подключения закреплен на металлическом кожухе, т. е. избежать заземления на передающей части невозможно, то необходи-

мо обеспечить гальваническую развязку передающего и приемного видеооборудования (для этого используют изолирующие трансформаторы, оптоэлектронные приборы развязки и т. д.). Приборы гальванической развязки включаются в разрыв кабельной линии связи и тем самым разрывают паразитный контур заземления;

– питание всех элементов СОТ желательно осуществлять от одной и той же фазы силовой сети.

Использование для передачи видеосигнала оптоволокна полностью исключает наводки на видеосигнал. Это одно из достоинств оптоволоконной линии связи.

Основное назначение грозозащиты – защитить аппаратуру и человека от воздействия грозового разряда. Как правило, грозовой разряд воздействует на аппаратуру путем наведенной ЭДС, которая в среднем имеет напряжение 5 кВ при длительности воздействия 50 мкс. Разряд молнии характеризуется чрезвычайно быстрым нарастанием тока до пикового значения, как правило, достигаемого за время от 1 до 80 мкс, и последующим падением тока обычно за 3 – 200 мкс после пикового значения. Это и определяет выбор времени воздействия расчетного импульса – 50 мкс. Следует учесть, что амплитуда наводимого напряжения от разряда молнии может значительно превышать 5 кВ, поскольку зависит от расстояния между линией связи и местом удара молнии.

Таким образом, данное воздействие характеризуется высоким напряжением и быстротой, поэтому используется многоступенчатая защита, которая обычно состоит из грозоразрядника и полупроводниковых приборов защиты. Грозоразрядник обеспечивает снижение уровня опасного напряжения в линии до 90 – 350 В и отводит на землю импульсный ток до 10 кА. Кроме того, на основе полупроводниковых приборов (диодов, варисторов и т. д.) обеспечивается дальнейшее снижение уровня напряжения до значения, безопасного для аппаратуры и человека, при этом отводимый импульсный ток может составлять до десятка ампер. Таким образом, любое устройство грозозащиты характеризуется определенной отводимой импульсной мощностью разряда, от значения которой зависит вероятность защиты аппаратуры от выхода из строя. От прямого удара молнии ни одно устройство грозозащиты не может защитить аппаратуру. Обычно при этом происходят пробой изоляции в кабелях и проводах и массовые замыкания радиоэлементов на землю в

аппаратуре. Однако устройство грозозащиты и качественное заземление должны обеспечить защиту обслуживающего персонала от поражения электрическим разрядом. Отсюда так важно соответствие качества заземления нормативным требованиям.

Типы структур СВН. Параметры выбора СВН

Типовые структурные схемы систем видеонаблюдения [74; 77] приведены на рис. 4.1 – 4.4.

Рис. 4.1. Структурная схема системы видеонаблюдения
на базе аналогового видеорегистратора

Рис. 4.2. Гибридная структурная схема системы видеонаблюдения
на базе цифрового видеорегистратора

В зависимости от вида применяемого оборудования охранные системы видеонаблюдения разделяют на аналоговые и цифровые. *Аналоговые системы видеонаблюдения* были первопроходцами на

рынке охранного видеонаблюдения, но сегодня в чистом виде мало применяются. Аналоговые системы видеонаблюдения можно смело отнести к прошедшему этапу истории охранного теленаблюдения, хотя и на данный момент можно найти их почитателей.

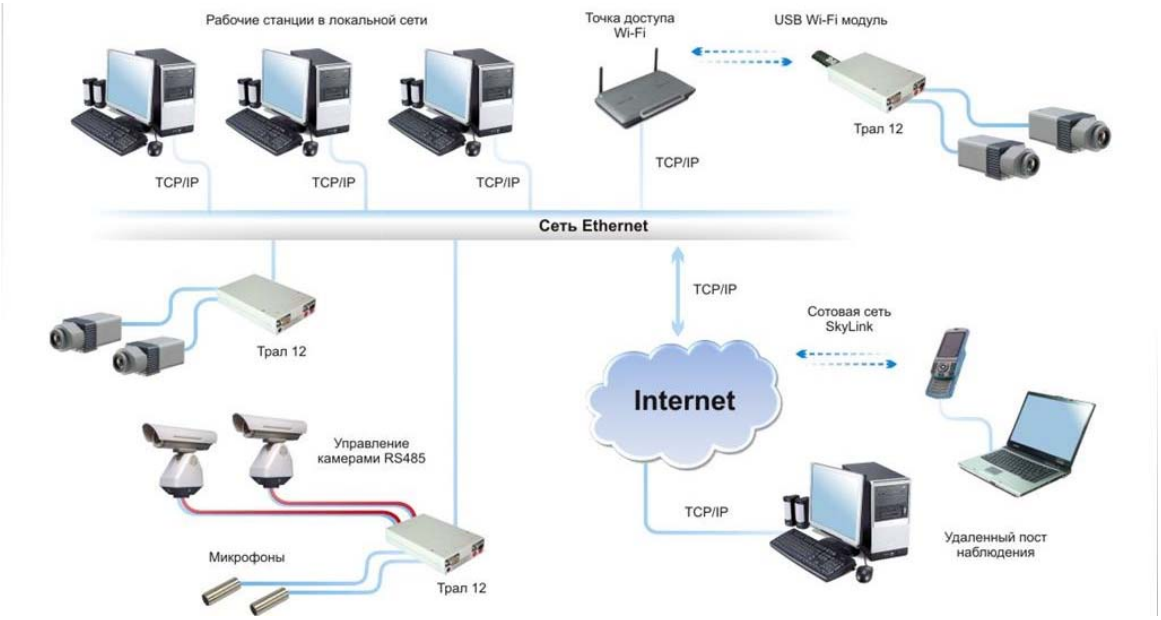


Рис. 4.3. Структурная схема системы видеонаблюдения на базе локальной компьютерной сети учреждения

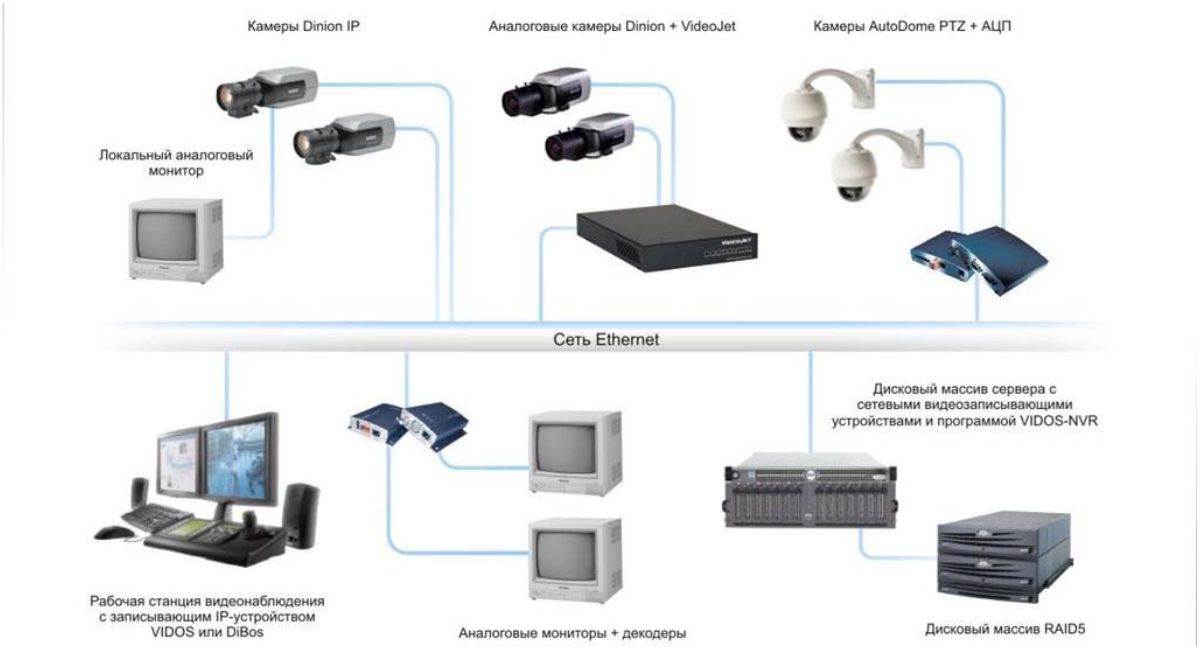


Рис. 4.4. Структурная схема рабочей станции управления видеонаблюдением с записывающим IP-устройством

Перед тем как приступить к закупке аппаратуры и оборудованию объекта, желательно хотя бы ориентировочно оценить сложность будущей системы. Для этого сначала определяют необходимое количество камер, а затем систему условно относят к соответствующей группе: системы, содержащие до 8 камер; системы, содержащие от 9 до 16 камер; системы, содержащие более 16 камер.

При установке телевизионной камеры (ТК) следует руководствоваться следующими принципами [74; 77]:

– камеру следует располагать на местности так, чтобы избежать возможных прямых засветок объектива яркими источниками света (солнце, фары машин и др.);

– размещать ТК так, чтобы размеры «мертвой» зоны были минимальными (рис. 4.5).

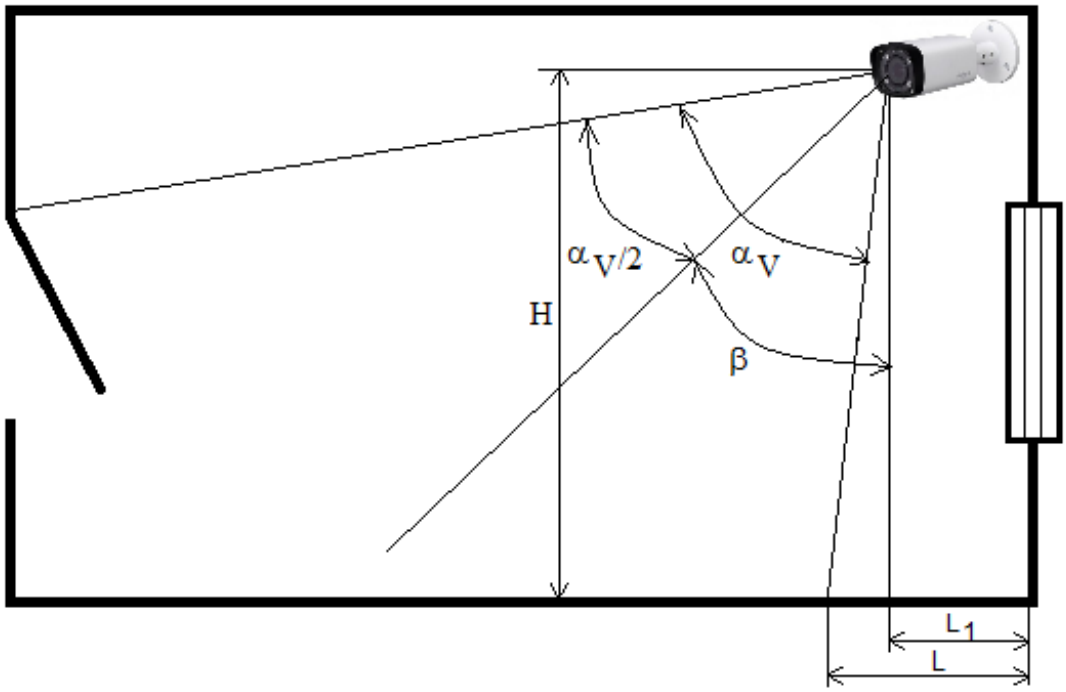


Рис. 4.5. «Мертвая» зона ТК (вид сбоку)

Размер «мертвой» зоны определяют по формуле $L = L_1 + H \times$ $\times \operatorname{tg}(\beta - \frac{\alpha_V}{2})$,, где L_1 – расстояние от стены до объектива ТК, м; H – высота установки ТК, м; β – угол между вертикальной осью и осью ТК (угол наклона ТК); α_V – угол зрения объектива ТК по вертикали. Указанный расчет проводят для каждой выбранной зоны видеоконтроля. Затем рассчитывают общее число камер в СОТ.

Варианты оборудования объектов

Многообразие помещений и территорий различных объектов не позволяет дать однозначные рекомендации по размещению ТК на объекте [74; 77]. Рассмотрим некоторые стандартные помещения (комната, коридор, лестница) и территории (периметр, стоянка автомобилей), которые могут быть на большинстве объектов, и приведем рекомендации по размещению ТК. В любом случае варианты оборудования объектов должны выбираться индивидуально для каждого объекта на стадии его обследования и согласовываться с заказчиком.

Для рис. 4.6 – 4.10 введены следующие обозначения: *A, B* – длина и ширина зоны видеоконтроля, м; *V* – поле зрения ТК по горизонтали, м; *H* – поле зрения ТК по вертикали, м; *h* – высота установки ТК, м; $\alpha_г$, $\alpha_в$ – углы зрения ТК по горизонтали и вертикали. Расчеты минимально различимой детали (МРД) проведены для ТК обычного разрешения (380 ТВЛ).

Помещения. При охране помещений с помощью СОТ (см. рис. 4.6) возможно выполнение следующих задач: общее наблюдение за текущей обстановкой в помещении; контроль за входной дверью; наблюдение за всеми проемами (двери, окна) помещения.

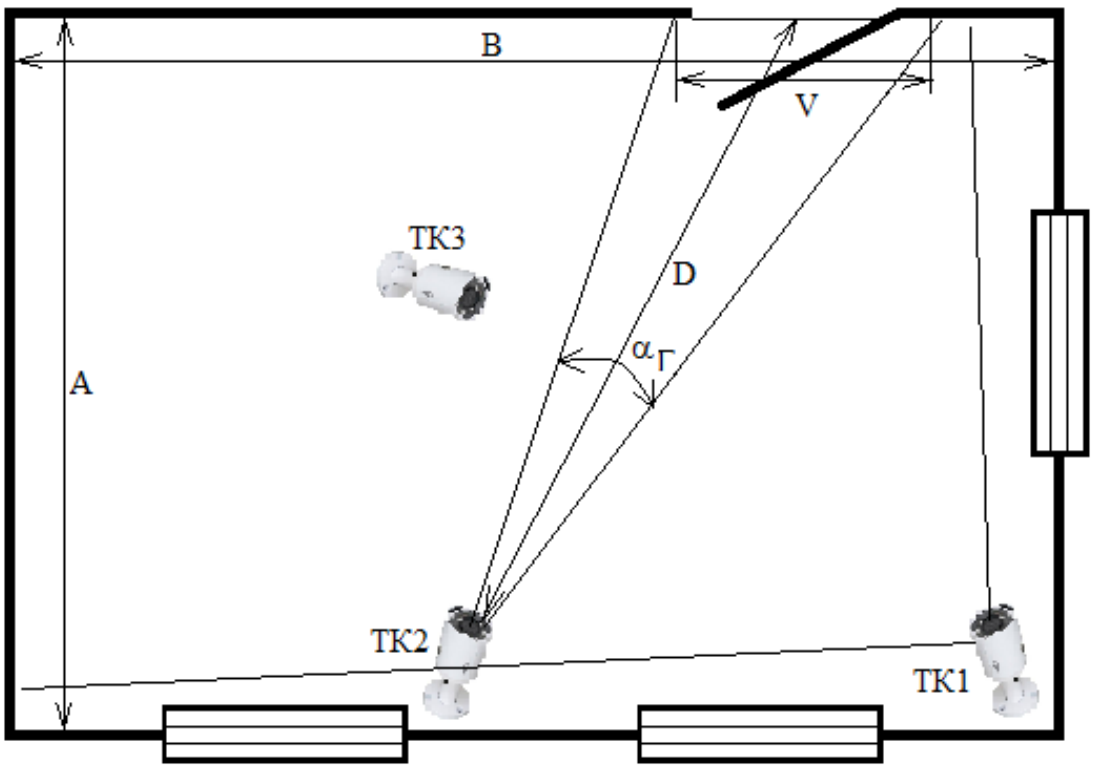


Рис. 4.6. Схема охраны помещения

Размеры помещения: A = 3 м, B = 4 м. Общее наблюдение осуществляет ТК1, обладающая широким углом зрения (до 100°), а следовательно, охватывающая всю площадь помещения. Минимальная различимая деталь (изображения) на дальней границе зоны видеоконтроля при этом $S_н$ = 31 мм. С помощью ТК1 возможно выполнение только целевой задачи обнаружения. Для контроля всех входящих в помещение используется ТК2, которая имеет малый угол зрения. Выбирают камеру с углом зрения по вертикали, исходя из высоты двери или роста человека (т. е. поле зрения по вертикали H равно примерно 1,8 м). Минимальная различимая деталь (изображения) при этом $S_н$ = 4 мм. С помощью этой ТК возможно выполнение целевой задачи различения объекта контроля. Для идентификации объекта контроля применяют ТК высокого разрешения (R = 600 ТВЛ). Для наблюдения за всеми проемами помещения используется расположенная на потолке на поворотном устройстве ТК3, оборудованная объективом с трансфокатором и имеющая предустановки на окна и двери.

Коридоры. Для охраны коридора, как и для охраны комнаты, возможно решение следующих задач: наблюдение за всеми лицами, выходящими в коридор из кабинетов; контроль всех лиц, входящих в коридор через входную дверь (например, с лестничной клетки). Решить эти задачи можно с помощью одной ТК, оборудованной объективом с трансфокатором, или с помощью двух ТК с большим и малым углами зрения ($\alpha_{г1}$ и $\alpha_{г2}$) (см. рис. 4.7).

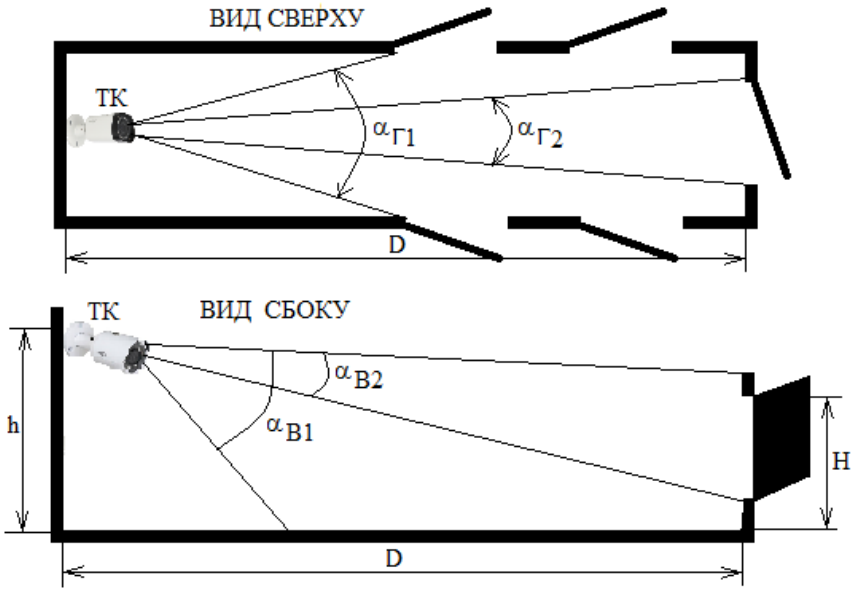


Рис. 4.7. Схема охраны коридора

При длине коридора 10 м, ширине 2,5 м и расположении первой двери на расстоянии 3 м от ТК имеем на дальней границе зоны контроля $S(\alpha_{г1})$ = 21 мм; $S(\alpha_{г2})$ = 6 мм. С помощью таких ТК можно выполнять целевую задачу обнаружения и различения. Если применяют объектив с трансфокатором, его увеличение должно быть не менее 3× при минимальном угле обзора $\alpha_{г2}$ = 15°. Для выполнения задачи по идентификации входящих в торцевую дверь лиц используют ТК высокого разрешения.

Лестницы и входные двери. Наблюдение лестничных пролетов первого и второго этажа (см. рис. 4.8) рекомендуется вести с промежуточных площадок между этажами (выше второго этажа устанавливать ТК нецелесообразно). На указанных площадках под потолком рекомендуется разместить по две камеры, направленные соответственно вверх и вниз по лестнице.

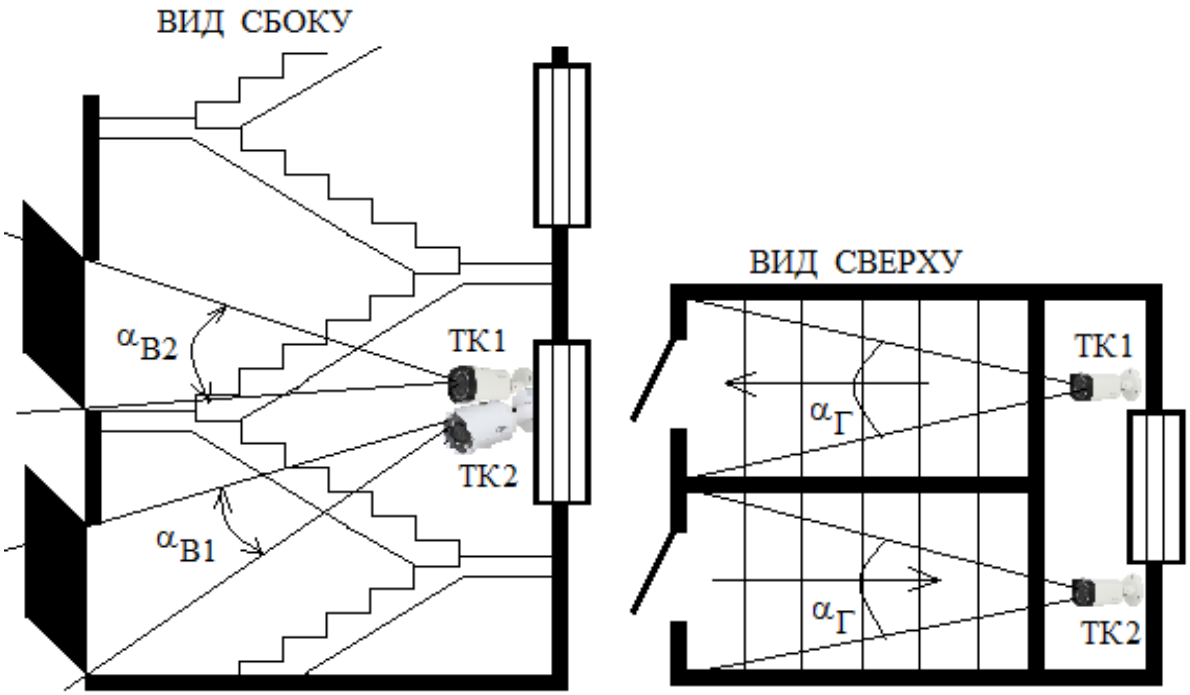


Рис. 4.8. Схема охраны лестничных пролетов

Периметр. При охране периметра территории объекта вдоль забора выделяют зону отторжения (не менее 2 м), в которой не должны находиться посторонние предметы, деревья, кустарники, высокая трава и другие преграды. Весь периметр разбивают на прямолинейные участки и устанавливают размеры контролируемых зон (см. рис. 4.9).

Телевизионную камеру, контролирующую участок периметра, располагают на поворотном/наклонном устройстве и оборудуют объективом с трансфокатором. Минимальное фокусное расстояние выбирают исходя из условия уменьшения «мертвой» зоны под ТК, а максимальное – так, чтобы обеспечить поле обзора ТК, равное ширине зоны отторжения (V) на дальней границе зоны контроля. При длине контролируемого периметра D = 100 м, ширине зоны отторжения V = 2 м и объективе (с трансфокатором) с увеличением не менее 6× и максимальным углом зрения 45° имеем на дальней границе зоны контроля: при максимальном угле зрения S = 218 мм; при минимальном угле зрения S = 32 мм. То есть на дальней границе зоны контроля ТК с указанными параметрами возможно выполнение целевой задачи обнаружения. Для большей детализации объекта контроля необходимо применять ТК более высокого разрешения и объектив с большим увеличением.

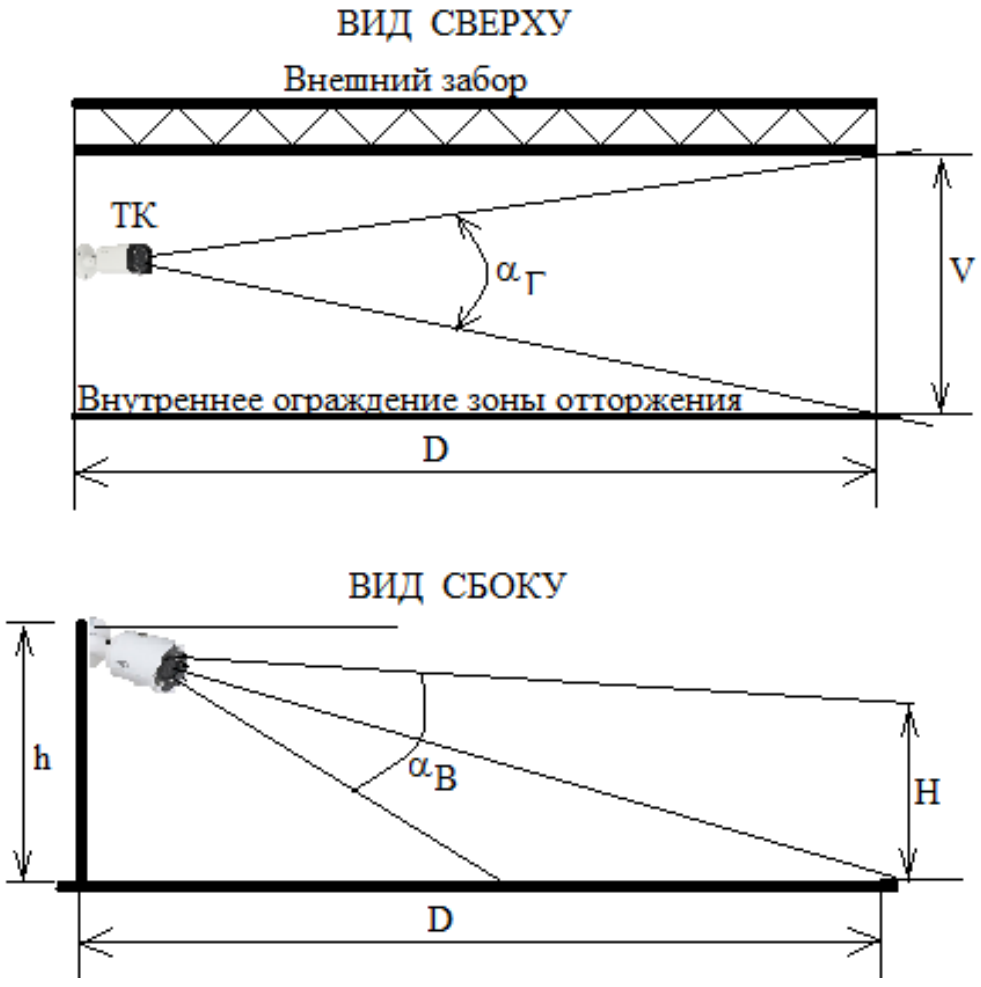


Рис. 4.9. Схема охраны периметра

Открытые площадки. Для охраны открытых площадок (например, стоянок автомобилей) применяют ТК на поворотном/наклонном устройстве и объектив с трансфокатором (см. рис. 4.10). При минимальном фокусном расстоянии объектива проводится обзор всей площади стоянки. При максимальном фокусном расстоянии возможно определение номера автомобиля, въезжающего/выезжающего на/со стоянку(и). Телевизионная камера может быть подключена к системе распознавания номеров автомашин. Объектив (с трансфокатором) с увеличением 10× и максимальным углом зрения 45° при длине и ширине открытой площадки, равных 100 м, дает результат $S(\alpha_{min}) = 13$ мм, т. е. при минимальном угле зрения объектива возможно различение номера автомобиля на экране монитора. Применение ТК высокого разрешения дает результат $S(\alpha_{min}) = 9$ мм, т. е. камеры высокого разрешения позволяют определить номер автомобиля на большем расстоянии.

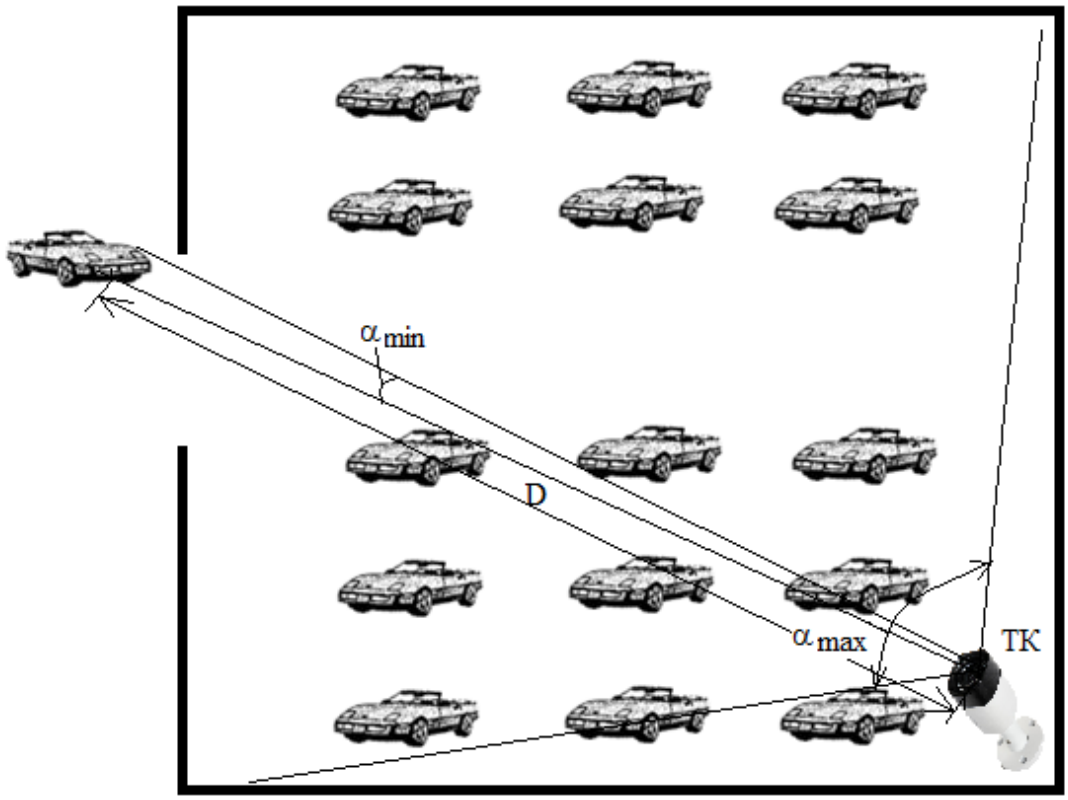


Рис. 4.10. Схема охраны стоянки автомобилей

При организации видеоконтроля на стоянках автотранспорта следует учитывать то, что в темное время суток въезд автомобиля на

стоянку происходит с включенными фарами, на фоне которых номер автомобиля может стать неразличимым. Из этой ситуации есть два выхода: на въезде на стоянку автотранспорта применять дежурное освещение, компенсирующее свет фар; использовать ТК с функцией инверсии белого.

Базовые требования по монтажу СВН

При монтаже систем видеонаблюдения необходимо знать определенные правила, которые помогут избежать неприятностей, связанных с некачественным изображением на мониторе или помехами, которые присутствуют на экране.

1. Необходимо использовать радиочастотный кабель с волновым сопротивлением 75 Ом и плотностью навивки экранирующего чулка не менее 80 %.

2. Необходимо использовать радиочастотные разъемы, не ухудшающие волновое сопротивление кабеля. Разъемы с креплением центральной жилы винтом или обжим радиокабеля до такой степени, что он сплющивается, приводят к непредсказуемому поведению видеосигнала в этом месте.

3. Необходимо следить за тем, чтобы оплетка видеокабеля, включаемого в камеру, не имела гальванической связи с местом крепления кронштейна. Основная масса видеокамер имеет такую связь, а это прямой путь для блуждающих токов 50 Гц в обратный провод (оплетку) и на экран монитора.

4. Наращивание строительной длины радиокабеля должно выполняться только с использованием специальных переходников, соединяющих два конца кабеля, оформленных разъемами.

5. Любое соединение по длине кабеля должно быть заизолировано с помощью термоусаживающихся трубок.

6. Радиус изгиба радиочастотного кабеля должен быть не меньше требуемого по ТУ на данный тип кабеля или составлять не менее 10 внешних диаметров кабеля.

7. Не следует забывать, что по длине питающего кабеля происходят значительные потери напряжения и выбор правильного сечения может устранить многие проблемы.

8. При передаче видеоинформации от камер на большие расстояния необходимо позаботиться о компенсации потерь амплитуд ви-

деосигнала. Первый способ компенсации потерь – использование радиокабеля большего диаметра. Второй способ – установка видеоусилителей. Обычно их размещают перед монитором, но в большинстве случаев это позволяет восстановить только контраст изображения. Мелкие детали на нем таким способом не восстановить. Правильно решить эту задачу можно, установив видеоусилитель непосредственно после видеокамеры и перед монитором, причем усилитель должен иметь высокочастотную коррекцию, настраиваемую на реальную длину кабеля.

9. Если используются видеокамеры с низковольтным питанием постоянным током и блок питания размещен на посту охраны, то на экране во многих случаях появляются пульсации 50 Гц. Это связано с принципом работы стабилизатора постоянного напряжения, который отслеживает пульсации только на своем выходе. На другой стороне питающего кабеля пульсации могут иметь любое значение. В кабель, проложенный по стене, могут наводиться «блуждающие» токи 50 Гц.

10. Питание всех устройств должно осуществляться от одной фазы сети. Следует избегать фаз, от которых питаются лампы дневного света, тиристорные регуляторы и сильноточные устройства.

11. Проектировщики систем, а тем более монтажные организации совершенно не уделяют внимания устройствам защиты от перенапряжений по цепям питания, управления и видеосигнала (в обиходе – грозозащита). В нашей стране устройства защиты от перенапряжений, к сожалению, совершенно новое направление в проектировании различных систем. Как показывает мировая практика, материальные средства, вложенные в системы защиты от перенапряжений, в процессе эксплуатации систем окупаются сторицей. Грозовые разряды и удары молний создают в атмосфере мощные электромагнитные поля. Эти поля, пересекая кабельные коммуникации, наводят в них высокие значения ЭДС, которые в виде потенциалов прикладываются к оконечному оборудованию, выводя его из строя. Для снижения наведенных ЭДС до допустимых значений в кабельных коммуникациях и используются системы защиты от перенапряжений.

12. Если видеокамеры установлены на больших расстояниях от поста наблюдения, то следует рассмотреть целесообразность прокладки кабелей и проводов по заборам или воздушным путем. Значи-

тельно дешевле использовать радиоканал для передачи видеосигнала и управления видеокамерами.

13. Необходимо заземлять оборудование поста видеоконтроля только стандартной системой защитного заземления. Не следует пользоваться сомнительными устройствами заземления. Сечение заземляющего проводника от поста видеоконтроля до электрощита необходимо выбирать в соответствии с требованиями ПУЭ.

Контрольные вопросы

1. Каким образом определяются угол зрения и фокусное расстояние видеокамеры?
2. Каким образом определяется минимальный размер объекта на экране монитора?
3. Какими должны быть размеры изображения для задач обнаружения?
4. Какими должны быть размеры изображения для задач идентификации?
5. Какими должны быть размеры изображения для задач распознавания?
6. Как определяется размер «мертвой» зоны видеокамеры?
7. Назовите основные способы расстановки видеокамер.
8. Назовите особенности расстановки видеокамер при охране периметра и открытых площадок.
9. Назовите особенности расстановки видеокамер при охране коридоров.
10. Назовите базовые требования при монтаже видеокамер.
11. Назовите устройства управления в системах видеонаблюдения.
12. Назовите способы сжатия изображений.
13. Назовите устройства передачи видеосигналов, их основные характеристики и требования по проектированию.
14. Назовите устройства управления режимом отображения, их основные характеристики и требования по проектированию.
15. Назовите общие требования к организации электропитания СВН.

Глава 5. ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ И БЕЗОПАСНОСТИ В СОСТАВЕ ИНТЕГРИРОВАННЫХ КОМПЛЕКСОВ СИСТЕМ БЕЗОПАСНОСТИ

Общие положения

В целях повышения технической защищенности охраняемых объектов в настоящее время активно внедряются интегрированные системы безопасности. Общие требования к ИСБ описаны в ГОСТ Р 57674-2017 «Интегрированные системы безопасности. Общие положения». Как правило, с помощью таких интегрированных систем обеспечивается защита объектов особой важности [29]. Данные системы интегрируют на разных уровнях различные подсистемы безопасности, в том числе совместно функционирующие подсистемы охранной и тревожной сигнализации, пожарной сигнализации (автоматические установки пожарной сигнализации) и пожарной автоматики, охранного телевидения, контроля и управления доступом, а также ряд вспомогательных подсистем для обеспечения защиты объекта от разных видов угроз. В основном ИСБ применяют для защиты очень больших, протяженных, а также особо важных объектов. Использование ИСБ позволяет подразделениям вневедомственной охраны и частным охранным организациям решать задачи обеспечения безопасности граждан и охраны защищаемых ценностей на качественно новом уровне.

Наряду с задачами непосредственно по защите объектов, ИСБ (при включения в их состав подсистем автоматизации обслуживания зданий) позволяют максимально эффективно решать следующие задачи:

– при аварийных и нештатных ситуациях (НСД в охраняемые помещения, пожар, прорывы труб коммуникаций, утечка воды и т. д.) оперативно реагировать и более качественно принимать решения по обеспечению локализации ситуации;

– оптимизировать количество постов физической охраны и инженерных диспетчерских служб для сокращения расходов по содержанию персонала, уменьшить влияние человеческого фактора;

– обеспечить энергосберегающий режим управления инженерным оборудованием здания с целью сокращения затрат по использо-

ванию энергоресурсов (электроэнергии, тепла, горячей и холодной воды, воздуха и т. д.);

– за счет автоматического документирования работы оборудования проводить объективный анализ действий диспетчерских служб, обслуживающих системы жизнеобеспечения здания, а также оценивать качество функционирования службы охраны при нештатных ситуациях, качество решений, принимаемых обслуживающим персоналом.

Наибольшее распространение на объектах, охраняемых подразделениями вневедомственной охраны, нашли следующие российские ИСБ: «Орион-Про», «Рубеж», «Кодос-А-20», «Пахра» и др [4].

Эти ИСБ обеспечивают:

– возможность использования для взятия под охрану и снятия с охраны дистанционных идентификаторов, например карт и электронных ключей;

– видеонаблюдение и видеорегистрацию тревожных ситуаций;

– модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие, распределенные объекты;

– защищенный протокол обмена по каналам связи, имитостойкие шлейфы сигнализации;

– контроль и управление доступом через точки входа (двери, турникеты, шлюзы, шлагбаумы);

– управление установками пожарной автоматики;

– отображение состояний зон, разделов, точек доступа, приемно-контрольных приборов, считывающих устройств, видеокамер на графических планах помещений с подробными текстовыми пояснениями;

– управление инженерными системами здания (системы кондиционирования, отопления, вентиляции, оповещения, аварийной сигнализации);

– разграничение полномочий дежурных, операторов, администраторов за счет многоуровневой системы паролей и возможность подключения биометрических систем ограничения доступа к программам АРМ;

– речевое предупреждение дежурного о тревожных событиях, возможность записи и воспроизведения речевых сообщений;

– протоколирование всех событий, происходящих в системе;

– развитую диагностику работоспособности всех блоков и устройств системы.

Основной критерий классификации для ИСБ – количество реализованных функций в зависимости от состава подсистем ИСБ. Например, для ИСБ основные функции – это охранная сигнализация, тревожная сигнализация, пожарная сигнализация и пожаротушение, контроль и управление доступом, охранное телевидение. Для систем «интеллектуального здания», в которые в качестве подсистемы входит ИСБ, должны быть определены функции управления жизнеобеспечением и диспетчеризации здания (объекта). Иногда может добавляться функция по управлению производственным процессом. Таким образом, при выборе конкретной ИСБ для объекта необходимо определиться с количеством и типом функций, которые должна выполнять ИСБ для специфики данного объекта, с необходимой степенью автоматизации объекта, а также учитывать экономические соображения.

Интеграция подсистем ИСБ может быть выполнена на разных уровнях взаимодействия подсистем. Аппаратная интеграция – интеграция на проектном уровне, когда комплексирование подсистем осуществляется на этапе проектирования данных подсистем для каждого конкретного объекта и условий его функционирования. Такие работы проводят проектно-монтажные организации. Как правило, в этом случае применяют разнородные подсистемы (системы) различных производителей. Объединение (интеграция) этих подсистем осуществляется путем установки оборудования управления подсистемами (системами) в общем помещении – ПЦО. Взаимодействие между подсистемами происходит на уровне операторов подсистем без автоматического процесса передачи информации между подсистемами, т. е. без автоматизации. Это самый минимальный уровень интеграции, ему присущи известные недостатки: сложность обслуживания, разнородность аппаратуры, «человеческий фактор», параллельность прокладываемых коммуникаций, отсутствие автоматизации и т. д.

Разновидность такого типа интеграции – интеграция на релейном уровне, когда для передачи информации между отдельными подсистемами ИСБ используются контакты реле. Достоинство метода – простота оборудования, невысокая стоимость, возможность объеди-

нения подсистем (систем) различных производителей. Однако такой подход имеет весьма серьезные недостатки:

– ограниченность типов передаваемой информации, которой могут обмениваться подсистемы ИСБ;

– отсутствие визуализации информации передаваемых сообщений о состоянии системы в целом;

– очень низкая информативность, а по мере роста количества реле и линий связи – повышение стоимости реализации.

Современные ИСБ создаются с использованием информационных технологий и структурно представляют собой локальные сети различного уровня сложности, состоящие из специализированных вычислительных устройств и специализированных контроллеров. Взаимодействие ИСБ может осуществляться на четырех уровнях сетевого взаимодействия.

Первый (высший) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети Ethernet с протоколом обмена TCP/IP и/или его разновидностями, с использованием сетевых операционных систем Windows или других. Выбор операционных систем профессионального класса обусловлен тем, что необходима высокая надежность и защита от НСД.

Второй уровень представляет собой связь между контроллерами и компьютерами подсистем (вертикальный уровень связи) и между однородными контроллерами в каждой из подсистем (горизонтальный уровень связи). На вертикальном уровне наиболее часто используется интерфейс USB. На горизонтальном уровне – интерфейс RS-485 (RS-422) или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными. В контроллерах некоторых ИСБ возможен прямой выход на первый уровень в протоколе TCP/IP.

Третий уровень представляет собой связь между контроллерами и считывателями систем доступа. Здесь, как правило, применяются интерфейсы RS-485, USB или ставшие уже стандартом интерфейсы считывателей Wigand-26. На этом уровне располагаются также средства управления оповещением, адресные блоки управления с релейными и потенциальными выходами.

Четвертый уровень представляет собой шлейфы контроля состояния извещателей подсистем и входные цепи управления (сбалансированные и несбалансированные радиальные шлейфы, адресные шлейфы, входные цепи для контроля датчиков различных подсистем управления). Как правило, здесь применяют нестандартные специализированные интерфейсы и протоколы от производителей оборудования.

Среди других общих принципов построения ИСБ можно отметить следующие:

– масштабируемость как возможность первоначального развертывания системы в минимальном варианте с последующим наращиванием в процессе эксплуатации как количественных характеристик, так и функциональных возможностей;

– расширяемая модульная архитектура аппаратных средств (возможность наращивания аппаратных средств);

– возможность добавления модулей и расширения их функций для программного обеспечения;

– наличие в составе ПО упрощенного специализированного языка программирования для добавления пользователем собственных реализаций взаимодействия компонентов;

– автономная работа контроллеров подсистем при нарушении связи с центром управления;

– удаленный доступ с использованием каналов связи для построения территориально распределенных систем;

– интеграция подсистем не должна приводить к снижению общей надежности системы и входящих подсистем;

– для распределенных систем со связью с удаленными компьютерами или модемной связью – криптографическая защита данных (при необходимости);

– высокая живучесть системы (сохранение работоспособности системы при выходе из строя отдельных подсистем и блоков, а также сохранение работоспособности в пределах своих функций отдельных подсистем при выходе из строя оборудования или потере связи с центром управления);

– защита программного обеспечения от несанкционированного доступа, разграничение доступа по уровням полномочий пользователей.

В самом типовом варианте средства ИСБ предназначены для решения следующих задач:

– обнаружение НСД на охраняемые объекты (территории, зоны, здания и помещения);

– обнаружение несанкционированных действий на охраняемых объектах (территориях, зонах, зданиях, помещениях);

– выявление признаков пожара, управление системой эвакуации при пожаре;

– контроль и управление доступом персонала и посетителей на охраняемые объекты (территории, зоны, здания, помещения).

Система охранной сигнализации имеет следующий состав: средства обнаружения проникновения – автоматические и неавтоматические охранные извещатели; средства сбора и обработки информации – ПКП, блоки, устройства и модули; СПИ и ПЦН.

Еще один компонент ИСБ, который обязательно присутствует в составе любой из подсистем (систем), – подсистема оповещения в виде световых и звуковых оповещателей, световых табло, мониторов компьютеров и т. д. Однако в ряде случаев система оповещения может представлять собой отдельную техническую систему, например систему речевого оповещения (СОУЭ – система оповещения и управления эвакуацией), выполненную на основе радиотрансляционной сети и специализированной аппаратуры. В состав ИСБ или подсистемы (системы) СОС может входить подсистема защиты от краж отдельных предметов.

Перечень технических систем, комплексов и средств, составляющих ИСБ, может дополняться при необходимости другими средствами и системами для повышения уровня безопасности охраняемого объекта [29]. При невозможности объединения отдельных подсистем в ИСБ на программно-аппаратном уровне в одно АРМ ИСБ допускается самостоятельное развертывание указанных подсистем на отдельных АРМ. Однако при этом интеграция с целью повышения эффективности защиты объекта обеспечивается организационными мерами.

Подсистемы ИСБ должны обладать следующими техническими возможностями:

– выдача тревожных сигналов оператору и дежурному составу сил охраны о проникновении или попытках проникновения нарушителей на территорию (с территории) объекта через рубежи охраны и доступа в охраняемые зоны, здания, сооружения, помещения;

– непрерывная работа с учетом проведения регламентного технического обслуживания;

– выполнение установленного режима доступа людей и транспорта на объект, во внутренние зоны, охраняемые здания, сооружения и помещения;

– дистанционный контроль работоспособности периферийной аппаратуры, самотестирования программного обеспечения и аппаратных средств;

– управление режимами работы подсистем (систем) ИСБ с рабочих мест операторов, наделенных соответствующими полномочиями;

– дистанционное наблюдение за состоянием выбранных внутренних и внешних зон охраняемых объектов;

– регистрация и документирование сигналов от средств обнаружения, распоряжений и команд, отдаваемых начальствующим составом сил охраны и службы безопасности, а также сообщений и докладов охранников и командиров тревожных групп сил охраны;

– управление (при помощи средств связи) оперативными действиями личного состава дежурных сил охраны и службы безопасности при выполнении задач по охране и обороне объекта, а также контроль за исполнением команд и приказов;

– защита программных и аппаратных средств ИСБ от несанкционированного доступа;

– бесперебойное электропитание аппаратуры ИСБ.

Подсистемы (системы) ИСБ должны обеспечивать необходимую функциональную и аппаратную надежность, пожарную безопасность, помехоустойчивость [29]. В подсистемах (системах) ИСБ должны использоваться аппаратные средства, которые сертифицированы по безопасности, а также имеют сертификат, подтверждающий основные технические характеристики. Средства ИСБ рекомендуется применять только те, которые включены в перечень [4].

Для создания необходимого уровня безопасности объекта и его персонала допускается применять подсистемы (системы) ИСБ совместно с другими системами (средствами) обеспечения безопасности (пожарной, автоматизации и диспетчеризации технологического оборудования и т. п.). В этом случае функции совместно действующих систем должны дополнять друг друга, не оказывая взаимного мешающего влияния на работоспособность составных частей. В совместно

действующих системах должны обеспечиваться алгоритмическая совместимость и раздельная регистрация поступающих от них служебных и тревожных сигналов. Условия совместного применения систем должны быть оговорены в техническом задании на проектирование и эксплуатационной документации. Приоритетными для выполнения являются требования, обеспечивающие безопасность жизни людей и пожарную безопасность объекта.

Технические средства управления и контроля интегрированных подсистем ИСБ определяются целевым назначением подсистем. Допускается как ручное, так и автоматическое управление и контроль. Дублирование функций управления и контроля – необходимое условие обеспечения эксплуатационной надежности систем в целом. Кроме того, данные средства должны иметь защиту от возможных ошибок в действиях персонала.

Аппаратные средства подсистем ИСБ должны иметь типовые протоколы и интерфейсы для обмена информацией с целью обеспечения заданной имитостойкости, помехоустойчивости и скорости информационного обмена. Необходимые требования подсистем ИСБ по данным параметрам должны быть описаны в технических условиях и эксплуатационной документации на конкретные технические средства подсистем ИСБ для определения их эксплуатационной совместимости.

Для возможности совместной работы в локальной вычислительной сети программно-математическое обеспечение должно поддерживать совместимость различных подсистем ИСБ.

В соответствии с ГОСТ 28195-89 программное обеспечение ИСБ должно быть устойчиво к случайным или преднамеренным воздействиям следующего вида:

– случайное нажатие клавиш на клавиатуре;

– программный сброс аппаратных средств;

– отключение питания аппаратных средств;

– аппаратный сброс технических средств и подсистем;

– случайный перебор пунктов меню.

После указанных воздействий ПО АРМ ИСБ должно сохранять работоспособность ИСБ и целостность записанных и обрабатываемых данных.

Программное обеспечение должно быть защищено от преднамеренных воздействий с целью изменения установок в системе, несанкционированного копирования и обеспечивать резервное сохранение записанных и обрабатываемых данных, а также системных установок.

Программное обеспечение АРМ ИСБ должно по своей структуре быть клиент-серверным приложением и обеспечивать функционирование нескольких АРМ в одной локальной сети с поддержкой функций разделений операторов АРМ подсистем ИСБ по правам доступа, полномочиям. Программное обеспечение АРМ ИСБ должно иметь возможность назначения индивидуальных прав доступа каждому из операторов с защитой от НСД к АРМ ИСБ.

Программные средства АРМ ИСБ должны обеспечивать операторам в зависимости от их уровня доступа: просмотр информации, управление системой, администрирование. В подсистемах ИСБ должны быть приняты меры по защите информации в аппаратных средствах подсистем ИСБ от НСД внешних и внутренних нарушителей, а также меры по защите информации о функционировании подсистем ИСБ в АРМ ИСБ от НСД.

Технические механизмы защиты информации для обеспечения внутренней безопасности подсистем ИСБ должны предусматривать:

– антивирусную защиту и восстановление информации, разрушенной вирусными воздействиями;

– защиту информации от аварийных ситуаций;

– регистрацию и учет работы пользователей;

– кодирование или шифрование информации (при необходимости);

– ограничение доступа в помещения центральных и локальных пультов управления комплексом ТСО;

– идентификацию пользователей системы;

– разграничение прав пользователей по доступу к информации;

– контроль вскрытия аппаратуры.

Для защиты информации разрабатываются и реализуются административные и организационно-технические меры по подготовке ИСБ к эксплуатации. В частности, к таким мерам относятся:

– отделение функций технического обслуживания и ремонта от основных функций подсистем ИСБ;

– ограничение количества должностных лиц, допущенных к работе с АРМ ИСБ;

– установка технических средств ИСБ в режимных помещениях;

– периодическая смена паролей для входа в систему;

– постановка на учет носителей конфиденциальной информации и документации по подсистемам ИСБ;

– проверка отсутствия посторонней аппаратуры в помещениях с установленными техническими средствами ИСБ;

– защита аппаратуры подсистем ИСБ от электромагнитного излучения и наводок (при необходимости);

– периодическая проверка системы контроля вскрытия аппаратуры.

Программное обеспечение ИСБ защищается от НСД. Для доступа к программному обеспечению АРМ ИСБ должно быть реализовано не менее трех уровней доступа. В частности, первый уровень («администратор или инсталлятор») осуществляет доступ ко всем функциям; второй уровень («оператор») – доступ только к функциям текущего контроля состояния подсистем АРМ ИСБ; третий уровень («системный оператор») имеет доступ к функциям конфигурации программного обеспечения без доступа к функциям, обеспечивающим управление УПУ части подсистем АРМ ИСБ.

Данные уровни определяются либо техническим заданием на разработку программного обеспечения АРМ ИСБ, либо производителем программного обеспечения ИСБ. Требования к паролям, периодичность их смены и прочие вопросы защиты от несанкционированного доступа к программному обеспечению АРМ ИСБ обусловливаются принятой политикой информационной безопасности в организации.

При вводе пароля в систему знаки не должны быть видны на средствах отображения информации АРМ ИСБ. После ввода в систему пароли должны быть защищены от просмотра средствами операционных систем аппаратуры вычислительной техники, средствами ПО локальной распределенной вычислительной сети организации, а также средствами защиты программного обеспечения АРМ ИСБ.

Требования к системе охранной и тревожной сигнализации

На объектах, защищаемых подразделениями вневедомственной охраны, технические средства охранной и тревожной сигнализации должны удовлетворять требованиям документа [3]:

– обнаруживать проникновение нарушителя и выдавать тревожное сообщение о несанкционированном проникновении;

– обеспечивать возможность оперативной подачи сигнала тревоги персоналом объекта (тревожная сигнализация) при возникновении на объекте опасной для персонала объекта ситуации (нападение и др.);

– выдавать извещение о неисправности или отказе технических средств или каналов связи СПИ охранной сигнализации;

– не выдавать ложных срабатываний при переходе источников электропитания с основного на резервный и обратно.

Технические средства охраны для обнаружения проникновения (охранные извещатели) должны обеспечивать обнаружение НСД и/или несанкционированных действий нарушителя с целью проникновения на территорию или в помещения защищаемого объекта. При обнаружении в защищаемой зоне нарушителя либо физическом воздействии на защищаемые извещателем элементы строительных конструкций здания (ограждения) извещатель должен выдавать тревожный сигнал по проводному шлейфу или беспроводному каналу (радиоканалу) связи. Охранные извещатели характеризуются следующими функциональными параметрами:

– видом зоны обнаружения (точечная, линейная, поверхностная, объемная, комбинированная);

– размерами зоны обнаружения;

– чувствительностью;

– помехоустойчивостью;

– вероятностью обнаружения.

Охранные извещатели (ОИ) должны иметь защиту от саботажа нарушителем.

Средства сбора и обработки информации в составе ТСО должны обладать следующими функциональными параметрами:

– помехозащищенность линии (канала) связи приемно-контрольного прибора (контроллера) с извещателями;

– степень защищенности приемно-контрольного прибора (контроллера) ТСО от НСД к функции управления взятием (снятием с охраны) помещений объекта под охрану;

– время приема извещения от извещателей (максимально допустимое время контроля всех извещателей, подключенных к приемно-контрольному прибору), т. е. время опроса извещателей;

– информационная емкость, т. е. количество контролируемых шлейфов сигнализации, охранных извещателей или зон охраны;

– контроль состояния канала связи с извещателями (время обнаружения нарушений канала связи, предельные значения параметров линии связи, при которых должен выдаваться сигнал неисправности линии) как для объектовых шлейфов (двухпроводной линии), так и для каналов связи СПИ;

– информативность, т. е. количество передаваемых (принимаемых) служебных и тревожных извещений на системы передачи извещений с объекта;

– параметры и характеристики интерфейса канала связи приемно-контрольного прибора (контроллера) СПИ.

Система передачи извещений должна обеспечивать передачу всех видов извещений (тревожных, информационных, служебных) с охраняемого объекта (от средств сбора и обработки информации) на ПЦН, входящий в состав СПИ. Последняя обладает следующими функциональными характеристиками:

– тип и количество команд передачи/приема телеуправления (при наличии обратного канала передачи данных от ПЦН до охраняемого объекта);

– тип и количество передаваемых извещений (извещение о проникновении, извещение о пожаре, служебные и контрольно-диагностические сообщения и другие, если они имеются в системе);

– алгоритмы установки приоритетов для передачи тревожных извещений;

– вид канала передачи данных от объекта на ПЦН;

– время доставки тревожного извещения;

– время доставки других видов извещений.

По физическому типу каналы передачи информации с объекта на ПЦН могут быть следующими:

1) выделенные каналы (проводные, оптоволоконные и пр.);

2) каналы по линиям телефонной сети общего пользования, в том числе переключаемые, занятые телефонной связью, с использо-

ванием частотного выделения служебных сигналов, с использованием аппаратуры автоматического набора номера (информаторные);

3) радиоканалы;

4) прочие каналы передачи, в том числе сотовая связь и Интернет.

Время доставки тревожного извещения для системы передачи извещений должно быть менее 60 с. Система передачи извещений должна обеспечивать контроль целостности каналов передачи данных между охраняемым объектом и ПЦН.

Время обнаружения неисправностей каналов связи для СПИ в зависимости от типа используемого канала должно быть не более 120 с. Система передачи извещений, имеющая обратный канал передачи данных, для работы в автоматическом режиме постановки на охрану и снятия с охраны (автоматическая тактика охраны объекта) должна обеспечивать передачу сигналов квитирования (подтверждения) на объектовую часть ТСО, установленную на объекте, при взятии на охрану/снятии с охраны.

Для особо важных объектов система передачи извещений (при необходимости) должна обеспечивать резервирование каналов передачи тревожных извещений.

В СПИ должны быть приняты меры защиты передачи данных в каналах связи от несанкционированного доступа.

Вид и методы проверки защиты должны быть указаны в стандартах или технических условиях на СПИ. При необходимости используются также и средства криптозащиты.

Пульт централизованного наблюдения должен обеспечивать:

– прием тревожных извещений о несанкционированном проникновении на охраняемые объекты;

– прием служебных и контрольно-диагностических извещений;

– обработку, отображение, регистрацию полученной информации и представление ее оператору (пользователю) ОТС в заданном виде для дальнейшей обработки, а также (при наличии обратного канала) для передачи команд телеуправления на объектовое оборудование СПИ, смонтированное на защищаемом объекте;

– управление и контроль процесса взятия на охрану/снятия объектов с охраны для систем передачи извещений с ручной тактикой.

Средства тревожной сигнализации представляют собой подсистему охранной сигнализации (или ИСБ) и входят в ее состав. Данные средства могут составлять отдельную подсистему и монтироваться отдельно, но при этом сигналы тревоги от тревожной сигнализации должны передаваться на единый ПЦН. Сигналы тревожной сигнализации должны отличаться от служебных или тревожных сообщений охранной сигнализации или других подсистем ИСБ.

В качестве устройств тревожной сигнализации используются неавтоматические (с ручным или ножным управлением) охранные извещатели в виде электромеханических кнопок, радиокнопок, радиобрелоков, педалей. Кроме того, в состав средств тревожной сигнализации могут входить (при необходимости) специальные технические средства подачи сигнала тревоги вне зависимости от действия персонала объекта (устройства, оснащенные датчиками падения, пульса, дыхания, а также устройства типа «ловушек»: оптико-электронные барьеры, устройства, выполненные в виде предметов, привлекающих внимание нападающих и оснащенных датчиками сигнализации; другие средства аналогичного назначения).

Средства тревожной сигнализации должны функционировать с тактикой «без права отключения» все время нахождения на объекте посетителей и/или персонала объекта. Для реагирования на извещение о нападении от средств тревожной сигнализации время прибытия наряда физической охраны должно быть минимально возможным.

Кнопки (или аналогичные устройства) тревожной сигнализации должны устанавливаться в следующих помещениях объекта:

– помещениях для хранения оружия и боеприпасов;

– хранилищах, кладовых, сейфовых комнатах;

– на рабочих местах кассиров;

– у центрального входа в здание и запасных выходов из него (при необходимости);

– в кабинетах руководителей (при необходимости);

– помещениях службы охраны;

– на постах и в помещениях охраны, расположенных в здании, строении, сооружении и на охраняемой территории;

– в помещениях КПП и/или бюро пропусков (при необходимости);

– помещениях критических элементов объекта;

– на маршрутах передвижения охраны (при необходимости);

– в других помещениях, в которые возможно проникновение нарушителей во время нахождения там персонала объекта (при необходимости);

– коридорах, у дверей и проемов, через которые производится перемещение ценностей;

– на охраняемой территории у центрального входа (въезда) и запасных выходов (выездов) (при необходимости);

– в других местах по требованию руководителя объекта или по рекомендации службы безопасности или охранной организации.

Руководителей объекта, сотрудников службы безопасности и охраны следует оснащать мобильными беспроводными устройствами тревожной сигнализации (радиокнопками или радиобрелоками). На объектах торговли, кредитно-финансовой системы, кражеопасных объектах и объектах, подверженных разбойным нападениям, следует использовать специальные технические средства тревожной сигнализации.

Требования к системе контроля и управления доступом

Система контроля и управления доступом по своей функциональной принадлежности должна обеспечивать:

– санкционированный доступ субъектов и объектов (людей, транспорта и других объектов) в (из) помещения, здания, зоны и на территории путем идентификации по комбинации различных идентификационных признаков. К таким признакам относятся: вещественный код (ключи, карты, брелоки), запоминаемый код (клавиатуры, кодонаборные панели и другие аналогичные устройства), биометрические признаки (отпечатки пальцев, сетчатка глаз и др.) и пр.;

– предотвращение НСД людей, транспорта и других объектов в (из) помещения, здания, зоны и территории;

– выдачу информации на пульт централизованного наблюдения о попытках НСД на объект или при неправомерном использовании идентификаторов, а также при некорректных проходах.

В состав СКУД входят следующие элементы:

1) устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов (в том числе биометрические идентификаторы субъектов);

2) устройства управления (УУ) в составе аппаратных и/или программно-аппаратных средств;

3) устройства преграждающие управляемые в составе преграждающих конструкций и исполнительных устройств управления преграждающими устройствами;

4) дополнительные технические средства, не являющиеся обязательными элементами системы для обеспечения ее функционирования (контроля функционирования СКУД), в зависимости от специфики задач СКУД.

Система контроля и управления доступом должна выполнять следующие типовые функции:

– открытие УПУ при считывании идентификационных признаков, доступ по которым санкционирован, в конкретные зоны доступа (помещение или территорию) в заданный календарный и временной интервал либо по команде оператора СКУД;

– запрет открывания УПУ при считывании идентификационных признаков, доступ по которым не санкционирован, в конкретные зоны доступа (помещение или территорию) в заданный календарный и временной интервал;

– санкционированное изменение (добавление, удаление) идентификационных признаков в УУ и связей их с зонами доступа (помещениями, территориями) и календарными и временными интервалами доступа;

– защита от НСД к программным средствам УУ для изменения (добавления, удаления) идентификационных признаков, зон доступа и календарных и временных интервалов доступа;

– защита технических и программных средств от НСД и саботажа элементов управления СКУД, установка режимов доступа к информации в виде системы идентификаторов, паролей и идентификация пользователей;

– сохранение настроек и базы данных идентификационных признаков при отключениях электропитания СКУД;

– ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при чрезвычайных ситуациях, пожаре и неисправностях элементов СКУД в соответствии с правилами установленного режима и противопожарной безопасности;

– открытие или разблокировка любых УПУ, оборудованных СКУД, с рабочих мест операторов системы СКУД;

– автоматическое открытие определенных УПУ по пожарной тревоге;

– автоматическое закрытие УПУ при отсутствии факта прохода через запрограммированное время после считывания идентификационного признака, если по нему доступ санкционирован;

– закрытие УПУ на определенное время и выдача сигнала тревоги при попытках подбора идентификационных признаков (например, кода);

– отображение на пульте оператора, регистрация и протоколирование всех текущих и тревожных событий в протоколе АРМ СКУД;

– возможность просмотра и печати с заданной детализацией и реализация поиска протоколов функционирования СКУД (действий операторов, системных событий, всех видов проходов субъектов и объектов, тревог и аварийных ситуаций);

– автономная работа считывателя и контроллера с управляемыми преграждающими устройствами в каждой точке доступа при отказе связи с устройствами управления;

– возможность архивирования базы и просмотра архива в автономном режиме (для контроллеров СКУД);

– возможность анализировать рабочее время сотрудников и вести его статистику, проводить анализ нахождения сотрудника на рабочем месте, времени переработки (недоработки), опозданий и ранних уходов сотрудника (система учета рабочего времени как сервисная второстепенная функция АРМ СКУД по заказу собственника);

– возможность идентификации сотрудников и посетителей объекта на постах физической охраны по фотографиям из баз данных СКУД при проходе через турникеты (проезде через ворота).

Система контроля и управления доступом в сетевой версии программного обеспечения АРМ СКУД имеет возможности организации учета клиентов СКУД по типу пропусков:

1) постоянные пропуска (действуют длительное время для постоянных сотрудников);

2) временные пропуска (действуют определенный срок: от нескольких дней до полугода – для командированных лиц, практикантов, заменяющих лиц – или до получения постоянных пропусков, удаляются из системы автоматически по окончании этого срока);

3) гостевые (разовые) пропуска (дают право прохода на одно посещение).

Считыватели для СКУД должны обеспечивать:

– считывание идентификационного признака с идентификаторов;

– сравнение введенного идентификационного признака с хранящимся в памяти контроллера СКУД или базе данных УУ;

– формирование сигнала на открытие УПУ при идентификации пользователя, если доступ санкционирован;

– обмен информацией с контроллером и УУ.

Считыватели должны быть защищены от манипулирования путем перебора или подбора идентификационных признаков и других типовых методов саботажа СКУД. Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.

Устройства управления (контроллер или персональный компьютер с ПО СКУД) должны обеспечивать:

– прием информации от УВИП, ее анализ, отображение и формирование сигналов управления УПУ;

– ведение баз данных клиентов СКУД с возможностью формирования характеристик их доступа (кода, календарного и временного интервалов доступа, уровней доступа и пр.);

– ведение электронных журналов (протоколов) регистрации проходов субъектов и объектов через точки доступа СКУД;

– приоритетный вывод информации о тревожных ситуациях и некорректных проходах пользователей в точках доступа СКУД;

– контроль исправности состояний УПУ, УВИП и линий связи СКУД.

Система контроля и управления доступом должна обеспечивать организацию и выполнение требований контрольно-пропускного и объектового режимов, установленных на предприятии, а также предусматривать разделение объекта на различные типы зон доступа.

Существует три основные зоны доступа для СКУД:

1) первая зона определяет здания, территории (локальные зоны), помещения, доступ в которые персоналу и посетителям не ограничен (зона свободного доступа);

2) вторая зона определяет помещения (локальные зоны), доступ в которые разрешен ограниченному перечню сотрудников и посетителей объекта по разовым или временным пропускам или в сопровождении персонала объекта;

3) третья зона определяет специальные помещения объекта, доступ в которые имеют строго определенные сотрудники и руководители объекта.

Конструктивно СКУД должны строиться по модульному принципу и обеспечивать:

– взаимозаменяемость сменных однотипных технических средств;

– удобство эксплуатационно-технического обслуживания, эксплуатации;

– исключение возможности НСД к элементам управления СКУД;

– санкционированный доступ ко всем элементам, узлам и блокам СКУД, требующим настройки, ремонта или эксплуатационно-технического обслуживания в процессе эксплуатации.

Помещения, которые рекомендуется оборудовать СКУД для обеспечения контрольно-пропускного и объектового режимов, следующие:

– проходы и проезды на территорию объекта, в том числе КПП (шлагбаумы, ворота, противотаранные устройства и т. д.);

– УПУ входов в здание;

– кабинеты руководства;

– двери выходов из лифтовых холлов (при необходимости);

– служебные входы, запасные выходы;

– помещения охраны;

– помещения, в которых непосредственно сосредоточены материальные ценности;

– режимные помещения и зоны ограниченного доступа (серверные, АТС, кроссовые, аппаратные, диспетчерские пункты, помещения жизнеобеспечения здания и т. п.);

– помещения, согласованные с руководителем объекта дополнительно в ходе проектирования СКУД.

Система контроля и управления доступом может содержать следующие автоматизированные рабочие места:

– АРМ администратора;

– АРМ дежурного оператора охраны;

– АРМ оператора на проходной;

– АРМ бюро пропусков и АРМ отдела кадров.

Функции отдельных АРМ СКУД могут объединяться на одном рабочем месте.

Требования к охранной телевизионной системе

Система охранного телевидения должна обеспечивать передачу видеоинформации о состоянии защищаемых помещений, зон, периметра территории объекта на мониторы постов охраны либо на ПЦО по специализированным каналам связи. Применение охранного телевидения позволяет контролировать оперативную обстановку на территории и в помещениях объекта, определять характер ситуации, выявлять правонарушения и преступления, место и обстоятельства происшествия, направление движения нарушителя и принимать оптимальные меры противодействия. Кроме того, иногда СОТ позволяет идентифицировать нарушителя и выявлять необходимые признаки идентификации.

Система охранная телевизионная, предназначенная для работы в автоматизированном режиме, применяется в составе ИСБ или в дополнение к системе ОТС. Видеоизображение в СОТ может выводиться на видеомонитор (устройство отображения видеоизображений) оператора поста охраны на постоянной основе или только в случае возникновения тревоги (по сигналу тревоги, получаемому от извещателя охранной сигнализации, связанного с камерами видеонаблюдения). Задача СОТ в данном случае – предоставить оператору (дежурному ПЦН) дополнительную информацию о НСД к охраняемой зоне, например, с целью исключения ложных тревог или включения видеозаписи для последующего анализа ситуации или контроля действий службы охраны.

Система охранная телевизионная, предназначенная для работы в неавтоматизированном режиме, применяется для текущего контроля

оперативной обстановки на защищаемом объекте, территории, в помещении, зоне. В этом случае для работы СОТ требуется организация отдельного поста видеонаблюдения с дежурным оператором видеонаблюдения. Система охранная телевизионная должна обеспечивать возможность выполнения следующих функций:

– визуальный контроль объектов охраны и прилегающих к ним территорий;

– оперативный контроль действий персонала службы безопасности (подразделения охраны) и предоставление необходимой информации для координации этих действий;

– архивирование видеоинформации для последующего анализа событий;

– программирование режимов работы;

– функционирование под управлением систем контроля и управления доступом и охранной сигнализации.

Современные СОТ в основном используют цифровую обработку сигналов и превосходят аналоговые системы охранного телевидения по своим базовым показателям. Для цифровых СОТ используются специализированные платы видеозахвата, вставляемые в типовые персональные компьютеры, или специализированные видеосистемы на базе видеосерверов, или видеорегистраторы как отдельные цифровые устройства. Такие устройства позволяют организовать более эффективную систему защиты объектов. Системы охранные телевизионные, использующие цифровую обработку видеоинформации, способны обеспечивать выполнение комплекса специфических функций:

– разграничивать полномочия всех типов пользователей СОТ (оператора, администраторов, инсталляторов) для предотвращения неквалифицированного и/или несанкционированного управления СОТ;

– совмещать видеоизображение на мониторе оператора с графическими планами объекта разных уровней детализации, использовать компьютерную графику и средства визуализации, что в целом позволяет повысить наглядность, удобство восприятия и управления системой СОТ;

– решать задачи цифрового увеличения изображения, разрешения, распознавания и идентификации номеров автотранспорта, лиц людей, отдельных предметов и т. п.;

– использовать дуплексные и триплексные режимы работы видеорегистраторов, многорежимные возможности сервисных функций видеорегистраторов и видеосерверов;

– настраивать и менять контролируемые зоны камер СОТ, качество представления изображения, настраивать датчики обнаружения движения в различных частях кадров изображений и контролируемых зон видеокамер;

– осуществлять циклическую запись видеоинформации на цифровые носители с заданным качеством и временем хранения;

– поддерживать для каждой телевизионной камеры индивидуальные настройки качества изображения и частоты кадров записи в режимах «норма» и «тревога», тип вывода изображения на экран монитора; кроме того, все режимы работы камер могут изменяться по календарным и временным расписаниям;

– осуществлять цифровое мультиплексирование видеозаписи от всех камер;

– поддерживать программное обеспечение приоритетов качества записей изображений с камер тех охраняемых зон, откуда поступают тревожные сообщения (повышенные частота кадров и разрешение изображений);

– предоставлять возможность обеспечения программирования режимов записи в условиях управления от внешних устройств подачи тревожных сообщений (датчики тревоги), программирования времени записи тревоги (если запись не ведется постоянно);

– осуществлять поиск видеоинформации в архиве видеозаписей по заданному времени, дате, номеру камеры и т. д.;

– предоставлять возможность просмотра видеоархива по локальной сети, записи видеоизображения на внешние носители информации и распечатки любого кадра изображения на внешнем принтере и др.

Основные принципы построения СОТ должны применяться в соответствии с требованиями документов [74; 79]. Периферийная часть СОТ состоит из телевизионных камер, которые устанавливаются по охраняемому периметру территорий, внутри зданий, помещений и сооружений. Каналообразующее оборудование СОТ обеспечивает передачу видеосигналов от видеокамер на оборудование приема теле-

визионных сигналов (станционная часть СОТ) и включает в себя следующие элементы:

1) линии связи для передачи телевизионных изображений;

2) передатчики (усилители, преобразователи, разветвители и т. д.) видеосигналов;

3) приемники видеосигналов.

Для передачи видеоизображений в качестве канала связи могут быть использованы:

– коаксиальные кабели;

– локальные вычислительные сети (UTP- или FTP-кабели (витая пара));

– телефонные линии;

– радиоканалы;

– волоконно-оптические линии;

– сотовая связь;

– ИК-канал.

Для цифровых СОТ передача видеосигнала возможна по всем перечисленным типам каналов связи (проводные, оптоволоконные, беспроводные).

Наиболее распространенный способ передачи видеоизображений – передача по коаксиальному кабелю. Такой кабель может обеспечить высокое качество передачи любых типов изображений, и при соблюдении всех правил монтажа, без использования специальных видеоусилителей видеосигналы можно передавать на расстояние до 300 м.

Для передачи сигналов на большие расстояния можно использовать витую пару. Если видеосигналы передаются от аналоговой камеры, то необходимо использовать специальные передатчик и приемник для преобразования сигналов. Для передачи сигналов от IP-камер этого не требуется. При этом дальность передачи сигнала по сети от камеры до коммутатора, маршрутизатора, концентратора, усилителя (network switch, router, hub, repeater) определяется дальностью функционирования сегментов локальной сети в зависимости от ее категории. Например, для витой пары категории 5е дальность составляет не более 90 м.

В настоящее время с развитием технологий 4G и 5G существует техническая возможность передачи сигналов видеоизображений по

каналам сотовой связи. Но передача таких изображений ограничена пропускной способностью и скоростью передачи данных. Кроме того, это самый дорогой способ передачи данных.

Передача видеоизображений по каналам проводных телефонных линий ограничивается низким качеством таких линий, а также пропускной способностью и скоростью передачи данных. Максимальная пропускная способность составляет около 9600 бод.

Наиболее эффективная передача видеосигнала обеспечивается по волоконно-оптическим линиям. При этом требуются специальные приемники и передатчики для преобразования сигналов. Передача видеоинформации по оптоволокну имеет следующие преимущества перед другими каналами связи:

– обеспечивается высокая защищенность от электромагнитных помех и полная электрическая изоляция;

– возможна передача данных на большие расстояния без промежуточного усиления (ослабление сигналов в оптоволокне может составлять менее 0,25 дБ/км);

– при использовании многомодового оптоволокна можно обеспечить одновременную передачу большого числа независимых сигналов по одному каналу;

– оптоволокно по сравнению с кабелями более защищено от возможности утечки информации, что повышает конфиденциальность передаваемой информации.

В станционную (пультовую) часть цифровой СОТ входят: пульты видеоконтроля, клавиатуры, мониторы, видеосерверы, цифровые видеорегистраторы, коммутаторы видеосигнала, источники бесперебойного питания и пр.

Видеосерверы выполняют функции по сбору, обработке, записи, хранению и передаче видеоинформации, полученной от подключенных видеокамер, в виде видеоархивов. Пультовое оборудование СОТ устанавливается в помещении ПЦО или специально выделенном помещении объекта (например, серверная). Для резервирования видеоархивов может использоваться сервер резервного копирования, который выполняет функцию программируемой автоматической записи видеоизображений с видеосерверов (видеорегистраторов) с целью их долговременного хранения. Кроме того, сервер резервного копирования обеспечивает конвертирование видеоизображений, сохраненных

на видеосерверах, в нужный формат видеоданных для их записи и резервного копирования.

Пульты видеоконтроля могут быть в виде отдельных аппаратных средств или виртуальными в ПО видеосервера. Они предназначены для управления вариантами отображения информации на мониторах операторов постов наблюдения, а также для управления режимами работы видеокамер. Пульты видеонаблюдения должны обеспечивать:

– предоставление служебной информации о СОТ, возможность конфигурирования и изменения настроек СОТ для санкционированных пользователей после их идентификации;

– совместную работу СВН с ОТС, СКУД и другими подсистемами ИСБ;

– возможность вывода видеоинформации на мониторах операторов постов наблюдения в любых режимах: как в полноэкранном, так и в мультиэкранном.

На защищаемых СОТ объектах видеокамеры следует устанавливать в следующих местах:

– по периметру охраняемой территории – уличные камеры;

– на КПП и проходных, по ограждению периметра территории, на КПП автомобильного и железнодорожного транспорта;

– постах физической охраны или подступах к постам;

– в досмотровых комнатах для людей и зонах досмотра автотранспорта, на стоянках транспорта;

– у центральных и запасных входов/выходов в здание;

– в уязвимых местах возможного проникновения по периметру защищаемого объекта;

– коридорах и/или отдельных помещениях, по которым перемещаются денежные средства и любые виды ценностей;

– помещениях, в которых хранятся и обрабатываются защищаемые ценности, за исключением банковских хранилищ ценностей для физических лиц;

– на погрузочно-разгрузочных постах и в терминалах;

– складах, в фондах и хранилищах ценностей и товарной продукции;

– в местах хранения и обработки вредных, опасных, взрывчатых веществ;

– пунктах управления технологическими производственными процессами;

– других помещениях и/или на подходах к ним по усмотрению собственника объекта или по рекомендациям службы безопасности, вневедомственной охраны или охранной организации.

Уличные видеокамеры для защиты территории объекта должны обеспечивать работоспособность при температуре окружающего воздуха от –40 до +50 °С (от –55 … –50 °С для холодных климатических зон) и размещаться в герметичных термокожухах с солнцезащитным козырьком.

Видеокамеры устанавливают под углом к линии горизонта таким образом, чтобы солнечные лучи не попадали в объектив. Кроме того, во избежание засветок камеры фарами от транспортных средств их не следует направлять на места, где это возможно. Размещение камер должно препятствовать их саботажу, умышленному повреждению или краже. Желательно, чтобы все камеры находились под охраной, т. е. каждая камера была бы в зоне обзора другой камеры. При необходимости возможны установка дополнительной защиты камер, блокировка средствами ОТС, а также применение автоматических устройств контроля наличия видеосигнала от камер.

Если освещенность контролируемой зоны ниже чувствительности видеокамеры, должно быть охранное (дежурное) освещение или должны использоваться инфракрасные средства подсветки. При этом область дежурного освещения должна быть больше зоны контроля видеокамеры или совпадать с ней.

Для решения задач распознавания и идентификации на больших объектах рекомендуется пользоваться видеокамерами с поворотными устройствами и трансфокаторами. Для наблюдения с помощью одной телекамеры больших территорий объекта должны применяться вариообъективы с переменным фокусным расстоянием и поворотные устройства с дистанционным управлением. Для получения высокого качества изображений рекомендуется использование купольных роботизированных поворотных камер.

В помещениях объекта необходимо использовать камеры с электронным затвором и объективы с ручной регулировкой диафрагмы. При установке напротив мощного источника света применяют камеры со встроенной автоматической компенсацией засветки.

Системы охранные телевизионные, оснащенные видеодетекцией движения, позволяют привлечь внимание оператора к перемещениям субъектов или объектов в контролируемой зоне. При обнаружении движения в охраняемой зоне СОТ обычно выдает звуковое и графическое оповещение на мониторе и выводит полноэкранное изображение для оператора из зоны срабатывания.

Вся видеоинформация должна храниться в видеоархиве на регистраторе и резервироваться на внешний носитель. Хранить видеоархив рекомендуется не менее месяца, но собственником объекта может быть установлен другой срок. Для сокращения объема видеоархива допускается осуществлять видеозапись только по сигналам видеодетектора или извещателей, зона обнаружения которых связана с полем зрения видеокамеры.

В качестве устройств управления и коммутации видеосигналов, поступающих с видеокамер, используются видеоменеджеры, переключатели, квадраторы, матричные коммутаторы.

Устройства управления и коммутации должны обеспечивать приоритетное автоматическое отображение на экране мониторов поста охраны тех контролируемых зон, откуда поступило тревожное сообщение. Конструктивно СОТ должны строиться по модульному принципу для обеспечения:

– взаимозаменяемости и унификации однотипных технических средств СОТ;

– удобства эксплуатационно-технического обслуживания и ремонта СОТ;

– исключения НСД к элементам управления СОТ;

– санкционированного доступа ко всем элементам, узлам и блокам СОТ, с помощью которых осуществляются регулировка, обслуживание или замена неисправных элементов в процессе эксплуатации.

Требования к подсистеме защиты от краж отдельных предметов

Подсистема защиты предназначается для защиты от несанкционированного выноса из помещения отдельных предметов и выполняет следующие функции:

– дистанционное обнаружение и распознавание предметов с установленными на них метками с идентификаторами при появлении предметов с метками в зоне контроля системы;

– выдача специального сигнала при входе в зону контроля системы или выходе из зоны контроля системы меток с идентификаторами либо при разрушении или неисправности метки (в случае ее саботажа нарушителем) с учетом последнего сигнала обмена информации системы с меткой;

– мониторинг состояния предметов повышенной опасности с метками с идентификаторами.

Подсистема защиты от краж отдельных предметов в типовом состоянии состоит из следующих компонентов:

1) меток с идентификаторами (в том числе электронные пломбы), выполненных с использованием любых технологий и устанавливаемых на защищаемых предметах, подлежащих охране;

2) системы обнаружения меток с идентификаторами, которые обеспечивают обнаружение предмета при его движении или нахождении в зоне действия системы обнаружения, а также выдают специальный сигнал при входе в защищаемую зону либо при выходе метки из защищаемой зоны;

3) системы мониторинга предметов повышенной опасности.

Метки с идентификаторами должны:

– иметь такое конструктивное исполнение, которое позволило бы осуществлять их установку (закрепление) на охраняемый предмет без нарушения целостности этого предмета, за исключением меток с идентификаторами, которые используются для скрытой маркировки предметов повышенной опасности при условии сохранения в целостности их основных частей (например, для огнестрельного оружия и боеприпасов);

– содержать информацию, достаточную для достоверной идентификации конкретного защищаемого предмета;

– обеспечивать для предметов повышенной опасности (оружия, основных частей огнестрельного оружия, боеприпасов) хранение в электронных метках с идентификаторами информации, санкционированное ее изменение и обмен информацией об индивидуальном учете данных предметов.

Электронные метки с идентификаторами, устанавливаемые на упаковку (тару) предметов повышенной опасности, также должны хранить информацию о количестве, виде, типе, моделях помещенных в нее предметов и их индивидуальных номерах.

Требования к электромагнитной совместимости

Технические средства защиты от НСД, в том числе средства ИСБ, в зависимости от устойчивости к воздействию электромагнитных помех должны иметь (по ГОСТ Р 50009-2000) следующие степени жесткости:

– первая или вторая степень жесткости при нормальной устойчивости (жилые и офисные помещения);

– третья степень жесткости при повышенной устойчивости (производственные помещения);

– четвертая степень жесткости при высокой устойчивости (помещения с высоким уровнем электромагнитных помех).

В технических условиях на технические средства ИСБ конкретного типа устанавливаются требования по устойчивости к искусственно создаваемым электромагнитным помехам. Такие требования предъявляются к устройствам и системам, имеющим степень жесткости не ниже второй. Уровень допустимых помех при работе технических средств ИСБ должен соответствовать ГОСТ Р 50009-2000.

Требования к надежности

На технические средства и подсистемы ИСБ конкретного типа устанавливают следующие показатели надежности [15]: средняя наработка на отказ (ч), среднее время восстановления работоспособного состояния (ч), средний срок службы (лет). При установлении показателей надежности указываются критерии отказа.

По желанию заказчика для конкретных средств и систем могут быть установлены дополнительные требования по обеспечению надежности. Средняя наработка на отказ и средний срок службы технических средств и подсистем ИСБ определяются для каждой из подсистем соответствующими техническими условиями и действующими нормативными документами для данных подсистем ИСБ.

Требования к электропитанию ИСБ

Основное электропитание подсистем ИСБ должно осуществляться от сети переменного тока частотой (50±1) Гц и номинальным напряжением 220 В. Подсистемы ИСБ должны обеспечивать работоспособность при допустимых отклонениях напряжения сети от –15 до +10 %. Электропитание отдельных технических средств допускается осуществлять от других источников (например, вторичных источников) с другими параметрами выходных напряжений, но при этом требования к таким средствам должны быть установлены в нормативных документах на конкретные типы технических средств.

Подсистемы ИСБ должны иметь резервное электропитание при пропадании основного напряжения питания. В качестве резервных источников питания могут использоваться резервная сеть переменного тока или вторичные источники питания постоянного тока. Номинальное напряжение резервных (вторичных) источников питания постоянного тока выбирается из значений 12 или 24 В.

Переход на резервное питание должен происходить автоматически без нарушения установленных режимов работы и функционального состояния подсистем ИСБ и без выдачи тревожных извещений. При этом должно обеспечиваться формирование информационных сигналов о пропадании основного питания и переходе на резервное питание и наоборот.

Резервные источники питания (емкость аккумуляторных батарей источников) должны обеспечивать выполнение основных функций подсистем ИСБ при пропадании основного напряжения в питающей сети на время, определяемое действующими нормативными документами для каждой из подсистем.

Допускается не применять резервное электропитание с помощью аккумуляторных батарей для УПУ СКУД, которые требуют значительных мощностей приводных механизмов (приводы ворот, шлюзы и т. п.). При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания и иметь системные средства индикации аварии электропитания.

При использовании в качестве источника резервного питания аккумуляторных батарей для подсистем ИСБ должен выполняться их автоматический заряд, при этом рекомендуется иметь индикацию разряда батареи ниже допустимого предела.

В ИСБ желательно применять резервные источники питания, позволяющие осуществлять удаленный контроль (на ПЦН) их состояний и основных параметров электропитания, в том числе контроль глубокого разряда батарей. Химические источники питания, встроенные в идентификаторы СКУД, беспроводные извещатели подсистем (систем) охранной и тревожной сигнализации должны обеспечивать работоспособность в течение времени, оговоренного в тактико-технических характеристиках оборудования, но не менее трех лет. Иные требования (кроме вышеперечисленных) к ИСБ (приводятся в действующей нормативной документации на конкретные технические средства и должны быть отражены в технических условиях и эксплуатационной документации конкретных технических средств ИСБ):

– требования к тактико-техническим данным и характеристикам конкретных технических средств ИСБ;

– требования к устойчивости и имитостойкости технических средств ИСБ;

– требования по устойчивости к внешним дестабилизирующим факторам;

– требования к конструкции.

Выбор ИСБ для оборудования объектов

При оснащении конкретных объектов ИСБ важно заранее иметь представление об организации тактики охраны отдельных зон и помещений защищаемого объекта [29]. При этом основное значение для эффективности функционирования ИСБ будут иметь состав и уровни интеграции подсистем ИСБ. В целом эффективность применения ИСБ определяется следующими показателями:

– соответствие используемых технических средств охраны и безопасности уровням реальных угроз для защищаемого объекта;

– обеспечение соблюдения принятых на объекте правил контрольно-пропускного и объектового режимов, в том числе обеспечение режима доступа;

– уровень противодействия технических средств ИСБ НСД для различных типов нарушителей;

– уровень обеспечения достоверности информации о попытках НСД или несанкционированных действиях;

– обеспечение должной защиты каналов связи для передачи извещений подсистем ИСБ;

– возможность обеспечения качественного контроля за состоянием ИСБ в целом и изменениями в защищаемых помещениях;

– степень защиты охраняемых помещений или зон от НСД, несанкционированных, в том числе криминальных, действий;

– общая организация физической охраны объекта, в том числе и централизованной охраны, деятельность службы безопасности объекта;

– возможности по пресечению НСД, нарушений и несанкционированных действий, проведение профилактических мероприятий по недопущению нарушений;

– оперативность реагирования физической охраны объекта, в том числе и централизованной охраны, на попытки НСД и/или совершения несанкционированных действий.

Для упрощения построения ИСБ, снижения затрат на монтаж подсистем ИСБ, пусконаладку, обслуживание, эксплуатацию подсистем ИСБ необходимо руководствоваться рядом принципов.

Принцип адекватности по отношению к НСД, несанкционированным действиям и возникающим угрозам защищаемым ценностям предусматривает принятие на объекте организационных мер и таких технических механизмов реализации защиты территорий и помещений объектов, которые бы в полной мере соответствовали возникающим угрозам для защищаемых ценностей.

Зональный принцип заключается в том, что ИСБ объекта носит распределенную структуру и может состоять в АРМ ИСБ из отдельно программируемых адресных извещателей, зон, разделов с различными уровнями организации доступа и защиты охраняемых ценностей. При формировании границ отдельных охраняемых зон внутри объекта обеспечивается усиление защищенности от границы периметра объекта к его центру (зоны безопасности, как правило, имеют вложенную структуру). Интегрированная система безопасности должна иметь открытую структуру построения для возможности масштабирования, наращивания и резервирования выходящих из строя элементов оборудования.

Принцип равнопрочности заключается в том, что необходимый уровень эффективности функционирования ИСБ должен обеспечи-

ваться для всех типов угроз защищаемым ценностям, в том числе с учетом критерия эффективность – стоимость подсистем ИСБ.

Принцип адаптивности заключается в том, что эксплуатация ИСБ не должна создавать препятствий для деятельности объекта, а также должна быть адаптирована к производственным факторам его работы, в том числе и при обеспечении защиты объекта от НСД в условиях чрезвычайных ситуаций.

Выбор технических средств по оснащению объекта ИСБ начинают с анализа предъявляемых к ИСБ технологических требований, обследования объекта, а также определения возможностей и методов реализации выбранных технических решений.

По результатам обследования определяют тактико-технические характеристики и состав подсистем ИСБ, составляют техническое задание по оснащению объекта ИСБ. В техническом задании [1] указываются:

– предназначение ИСБ, технико-экономическое обоснование выбора проектного решения, общее описание ИСБ;

– место расположения составных частей (подсистем) ИСБ;

– условия эксплуатации составных частей (подсистем) ИСБ;

– основные технические характеристики составных частей (подсистем) ИСБ;

– требования к маскировке и защите элементов подсистем ИСБ, в том числе от саботажа и вандализма;

– структура обеспечения физической охраны объекта и способы реагирования охраны на оповещение о тревожных и аварийных ситуациях, последовательность действий нарядов при пресечении или предупреждении инцидентов на объекте;

– возможности функционирования ИСБ, обеспечения целостности и сохранения данных ИСБ при отказе АРМ ИСБ;

– алгоритмы функционирования подсистем ИСБ в режиме чрезвычайной и/или аварийной ситуации;

– структура, состав, обоснование выбора программного обеспечения АРМ ИСБ;

– набор требований по безопасности составных частей (подсистем) ИСБ;

– набор требований по электропитанию составных частей (подсистем) ИСБ;

– набор требований по эксплуатационно-техническому обслуживанию и ремонту, а также резервированию элементов подсистем ИСБ.

При интеграции составных частей (подсистем) ИСБ учитываются: совокупность параметров, значительно влияющих на удобство эксплуатации ИСБ при выполнении основных функций системы; совместимость и надежность совместной работы составных частей (подсистем) ИСБ; удобство, время и трудоемкость работ по эксплуатационно-техническому обслуживанию и ремонту.

Кроме того, при обосновании выбора ИСБ следует учитывать:

– необходимость синхронизации функционирования всех составных частей (подсистем) ИСБ и их элементов;

– комплексирование составных частей (подсистем) ИСБ на программном, аппаратном и (при необходимости) релейном уровнях;

– организацию каналов связи составных частей (подсистем) ИСБ посредством использования стандартных интерфейсов;

– техническую реализацию составных частей (подсистем) ИСБ в едином состоянии сигнальных выходов подсистем ИСБ во всех используемых режимах.

При требуемом состоянии охраны объекта необходимо обеспечить техническую, программную, информационную и эксплуатационную совместимость всех структурных элементов и составных частей (подсистем) ИСБ.

Проектирование ИСБ состоит из следующих этапов работ:

– анализ уязвимостей объекта, оценка эффективности составных частей (подсистем) ИСБ для действующих объектов;

– проведение комплексных обследований объекта и составление актов обследований;

– формирование и утверждение технического задания на разработку проектной документации по каждой из составных частей (подсистем) ИСБ объекта;

– разработка проектной документации по каждой из составных частей (подсистем) ИСБ объекта.

Проектная документация ИСБ должна соответствовать требованиям документов [1; 12; 13; 14].

Оценка эффективности действующей системы безопасности и состояния инженерно-технического укрепления объекта осуществля-

ется в ходе обследования комиссией, формируемой заказчиком [5]. При необходимости по результатам обследования составляется задание по усилению инженерно-технического укрепления элементов строительных конструкций объекта в виде приложения к акту.

Техническое задание на проектирование по каждой из составных частей (подсистем) ИСБ объекта разрабатывается заказчиком или организацией, уполномоченной на проведение данного вида работ в соответствии с договором, и согласовывается с охранной организацией. Проектная документация содержит следующий типовой комплект документов [1; 12; 13; 14]:

1) техническое задание на разработку проектной документации по каждой из составных частей (подсистем) ИСБ объекта;

2) пояснительную записку к проекту (в ней отражаются требования технического задания по выбранному техническому решению);

3) рабочие чертежи проекта по каждой из составных частей (подсистем) ИСБ объекта, включающие в себя поэтажные планы помещений объекта, генплан, структурные схемы, планы расположения оборудования, трассы прокладки кабелей, схемы подключений технических средств;

4) требования к монтажу, кабельный журнал, схемы монтажа извещателей и приборов;

5) спецификации оборудования и материалов по каждой из составных частей (подсистем) ИСБ объекта;

6) сметную документацию по каждой из составных частей (подсистем) ИСБ объекта;

7) эксплуатационную документацию по каждой из составных частей (подсистем) ИСБ объекта (при необходимости).

Проектная документация согласовывается с заказчиком. Обоснованные отступления (изменения, исправления) от проектной документации в процессе монтажа допускаются только по согласованию заказчика и организаций, участвующих в утверждении и согласовании проектной документации.

Разработка документации, содержащей сведения конфиденциального характера, а также ее хранение и доступ к ней осуществляются в соответствии с действующим законодательством с учетом специфики объекта.

Контрольные вопросы

1. Назовите принципы создания и интегрирования аппаратно-программных комплексов интегрированных систем (ИСБ) охраны и безопасности.
2. Укажите состав подсистем охраны и безопасности типовых ИСБ.
3. Назовите технические меры по обеспечению информационной безопасности при функционировании ИСБ.
4. Назовите организационные меры по обеспечению информационной безопасности при функционировании ИСБ.
5. Назовите требования к системе ОТС в составе ИСБ.
6. Назовите требования к СКУД в составе ИСБ.
7. Назовите требования к СОТ в составе ИСБ.
8. Назовите требования к подсистеме защиты от краж отдельных предметов в составе ИСБ.
9. Назовите требования по обеспечению электромагнитной совместимости и надежности функционирования ИСБ.
10. Назовите требования к программному обеспечению АРМ в составе ИСБ.
11. Как организуется взаимодействие между подсистемами ИСБ?
12. Назовите требования к используемым каналам связи при передаче информации от подсистем ИСБ.
13. Назовите требования к электропитанию подсистем охраны и безопасности в составе ИСБ.
14. Назовите критерии выбора оборудования подсистем охраны и безопасности в составе ИСБ.
15. Укажите состав проектной документации при проектировании ИСБ.

ЗАКЛЮЧЕНИЕ

В пособии дана подробная классификация технических средств инженерно-технического укрепления элементов строительных конструкций, а также составных частей средств охранно-тревожной сигнализации, СКУД и СВН. Рассмотрены требования нормативно-распорядительных и методических документов по проведению обследований объектов, размещению технических средств охраны и безопасности по территории и помещениям защищаемого объекта.

Стремительное развитие технических средств охраны и безопасности предъявляет новые, повышенные требования к техническим специалистам в области систем безопасности. В современных средствах защиты от НСД используются микропроцессоры, вычислительная техника, самые последние достижения в области радиотехники по обработке сигналов.

Приведенная в пособии информация – дополнительная к курсу «Техническая защита информации», носит справочный и нормативно-методический характер, предполагает наличие знаний по смежным разделам радиотехники, электротехники, теории информации, микроэлектроники и других дисциплин.

Большое внимание уделено особенностям технологического обеспечения проектирования и монтажа средств ОТС, СКУД и СВН на типовом объекте информатизации.

Даны рекомендации по выбору оборудования и приведены типовые требования к установке технических средств охраны и безопасности при оснащении объектов ОТС, СКУД и СВН.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. РД 25.952-90. Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Порядок разработки задания на проектирование. – М. : М-во электротехн. пром-сти и приборостроения СССР, 1997. – 19 с.

2. Пособие к руководящему документу РД 78.145-93. Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ. – М., 1993. – 25 с.

3. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации. – М., 2018. – 89 с.

4. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» (рекомендован решениями заседаний Технического совета ГУВО Росгвардии (протокол № 2 от 15 – 16 мая 2019 г., протокол № 3 от 22 июля 2019 г.)). – М., 2018. – 75 с.

5. Р 063-2017. Методические рекомендации. Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации. – М., 2017. – 50 с.

6. Р 078-2019. Методические рекомендации. Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации. – М., 2019. – 58 с.

7. Р 78.36.033-2013. Методические рекомендации. Мониторинг применения и сравнительный анализ испытаний различных видов оконных блоков, жалюзи, защитных решеток и остекления. Классификация, способы установки и усиления конструкции. – М., 2013. – 87 с.

8. Р 78.36.034-2013. Методические рекомендации. Мониторинг применения и сравнительный анализ испытаний различных видов периметрового ограждения (основного ограждения, дополнительного ограждения, предупредительного внешнего и внутреннего ограждения). Классификация. – М., 2013. – 56 с.

9. РМ 78.36.003-2013. Обзор и сравнительный анализ видов защитных ограждений и противотаранных заграждений. – М., 2013. – 26 с.

10. Р 78.36.043-2014. Методические рекомендации. Выбор и применение дверных блоков. Классификация, способы установки и усиления конструкции. – М., 2014. – 45 с.

11. РМ 78.36.004-2014. Обзор и сравнительный анализ дверных блоков. – М., 2014. – 56 с.

12. ГОСТ 2.114-2016. Единая система конструкторской документации. Технические условия. – М. : Стандартинформ, 2016. – 15 с.

13. ГОСТ 2.601-2013. Единая система конструкторской документации. Эксплуатационные документы. – М. : Стандартинформ, 2014. – 36 с.

14. ГОСТ 2.610-2006. Единая система конструкторской документации. Правила выполнения эксплуатационных документов. – М. : Стандартинформ, 2007. – 39 с.

15. ГОСТ 27.003-2016. Надежность в технике. Состав и общие правила задания требований по надежности. – М. : Стандартинформ, 2017. – 23 с.

16. ГОСТ 111-2014. Стекло листовое бесцветное. Технические условия. – М. : Стандартинформ, 2015. – 11 с.

17. ГОСТ 5533-2013. Стекло узорчатое. Технические условия. – М. : Стандартинформ, 2014. – 42 с.

18. ГОСТ 9272-81. Блоки стеклянные пустотелые. Технические условия. – М., 1981. – 15 с.

19. ГОСТ 14254-2015. Степени защиты, обеспечиваемые оболочками (код IP). – М. : Стандартинформ, 2016. – 39 с.

20. ГОСТ 15150-69. Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды. – М. : Стандартинформ, 2010. – 59 с.

21. ГОСТ 24866-2014. Стеклопакеты клееные. Технические условия. – М. : Стандартинформ, 2015. – 28 с.

22. ГОСТ 26342-84. Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры. – М., 2005. – 18 с.

23. ГОСТ 30826-2014. Стекло многослойное. Технические условия. – М. : Стандартинформ, 2015. – 28 с.

24. ГОСТ 32997-2014. Стекло листовое, окрашенное в массе. Общие технические условия. – М. : Стандартинформ, 2015. – 11 с.

25. ГОСТ Р 50862-2017. Сейфы, сейфовые комнаты и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому. – М. : Стандартинформ, 2018. – 40 с.

26. Р 068-2017. Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок. – М., 2017. – 110 с.

27. Р 069-2017. Рекомендации по выбору и применению средств обнаружения проникновения в зависимости от степени важности и опасности охраняемых объектов. – М., 2017. – 160 с.

28. Р 071-2017. Рекомендации. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения. – М., 2017. – 20 с.

29. Р 78.36.018-2011. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности. – М., 2011. – 73 с.

30. ГОСТ Р 56102.1-2014. Системы централизованного наблюдения. Часть 1. Общие положения. – М. : Стандартинформ, 2015. – 10 с.

31. ГОСТ Р 56102.2-2015. Системы централизованного наблюдения. Часть 2. Подсистема объектовая. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2016. – 15 с.

32. Р 78.36.022-2012. Методическое пособие. Применение радиоволновых и комбинированных извещателей с целью повышения обнаруживающей способности и помехозащищенности. – М., 2012. – 120 с.

33. Р 78.36.036-2013. Методическое пособие по выбору и применению пассивных оптико-электронных инфракрасных извещателей. – М., 2013. – 195 с.

34. Р 78.36.044-2014. Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений. – М., 2014. – 92 с.

35. Р 78.36.050-2015. Методические рекомендации. Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам. – М., 2015. – 92 с.

36. Р 78.36.051-2015. Методические рекомендации. Типовые проектные решения оснащения техническими средствами охраны объектов различных категорий, охраняемых подразделениями вневедомственной охраны полиции. – М., 2015. – 109 с.

37. Р 78.36.053-2015. Методические рекомендации. Применение оборудования с использованием защищенных каналов передачи данных, представляемых операторами сотовой связи. – М., 2015. – 26 с.

38. Р 074-2018. Методические рекомендации. Типовые проектные решения по оборудованию техническими средствами охраны частных домов, коттеджей и иных мест хранения имущества граждан. – М., 2019. – 133 с.

39. Р 78.36.035-2013. Рекомендации по организации комплексной централизованной охраны банковских устройств самообслуживания. – М., 2013. – 160 с.

40. ТП 78.36.001-2014. Типовой рабочий проект. Система охранно-тревожной сигнализации. Комната хранения оружия. – М., 2014. – 47 с.

41. ТП 78.36.002-2014. Типовой рабочий проект. Система охранно-тревожной сигнализации. Административное здание. – М., 2014. – 34 с.

42. Р 065-2017. Рекомендации по выбору и применению объектового оборудования проводных систем передачи извещений, устойчивых к несанкционированному обходу. – М., 2019. – 68 с.

43. ГОСТ 30601-97. Совместимость технических средств электромагнитная. Устройства охранные сигнально-противоугонные автотранспортных средств. Требования и методы испытаний. – М. : Изд-во стандартов, 2004. – 7 с.

44. ГОСТ 32321-2013. Извещатели охранные поверхностные ударно-контактные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2014. – 19 с.

45. ГОСТ 34025-2016. Извещатели охранные поверхностные звуковые для блокировки остекленных конструкций помещений. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2017. – 28 с.

46. ГОСТ Р 50009-2000. Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний. – М. : Стандартинформ, 2001. – 12 с.

47. ГОСТ Р 50658-94. Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений. – М. : Госстандарт России, 2005. – 13 с.

48. ГОСТ Р 50659-2012. Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2014. – 23 с.

49. ГОСТ Р 50777-2014. Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2014. – 39 с.

50. ГОСТ Р 52434-2005. Извещатели охранные оптико-электронные активные. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2006. – 24 с.

51. ГОСТ Р 52435-2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2016. – 28 с.

52. ГОСТ Р 52436-2005. Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2006. – 16 с.

53. ГОСТ Р 52551-2016. Системы охраны и безопасности. Термины и определения. – М. : Стандартинформ, 2016. – 28 с.

54. ГОСТ Р 52650-2006. Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2007. – 19 с.

55. ГОСТ Р 52651-2006. Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2007. – 19 с.

56. ГОСТ Р 52933-2008. Извещатели охранные поверхностные емкостные для помещений. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2009. – 15 с.

57. ГОСТ Р 53560-2009. Системы тревожной сигнализации. Источники электропитания. Классификация. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2010. – 11 с.

58. ГОСТ Р 53702-2009. Извещатели охранные поверхностные вибрационные для блокировки строительных конструкций закрытых помещений и сейфов. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2011. – 24 с.

59. ГОСТ Р 54455-2011. Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам. – М. : Стандартинформ, 2012. – 20 с.

60. ГОСТ Р 54832-2011. Извещатели охранные точечные магнитоконтактные. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2012. – 23 с.

61. ГОСТ Р 55017-2012. Пульты централизованного наблюдения для использования в системах противокриминальной защиты. Требования к информации. – М. : Стандартинформ, 2014. – 14 с.

62. ГОСТ Р 55150-2012. Извещатели охранные комбинированные ультразвуковые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний. – М. : Стандартинформ, 2014. – 19 с.

63. Аналитический обзор. Изучение возможности применения носимых средств позиционирования, обеспечивающих передачу информации по каналам сотовой связи, в качестве средств индивидуальной тревожной сигнализации. – М., 2015. – 27 с.

64. Аналитический обзор. Исследование современных методов персональной идентификации в целях применения в системах централизованного наблюдения. – М., 2015. – 88 с.

65. Аналитический обзор. Модернизация серийно выпускаемых радиоканальных систем передачи извещений (РСПИ), а также подсистем с использованием каналов сотовой связи. – М., 2015. – 27 с.

66. Р 78.36.058-2016. Методические рекомендации. Оценка трудозатрат работ по проектированию, монтажу и пусконаладке технических средств и систем противокриминальной защиты. – М., 2016. – 51 с.

67. Р 78.36.048-2015. Рекомендации. Применение оборудования радиоканальных систем передачи извещений (РСПИ). – М., 2015. – 182 с.

68. Р 78.36.045-2014. Методические рекомендации. Защита локальных вычислительных сетей пунктов централизованной охраны при использовании глобальной сети Интернет для передачи данных между объектовым и пультовым оборудованием СПИ. – М., 2014. – 200 с.

69. Р 076-2018. Методические рекомендации. Ложные срабатывания технических средств охранной сигнализации и методы борьбы с ними. – М., 2018. – 41 с.

70. Р 064-2017. Методические рекомендации. Выбор и применение технических средств и систем контроля и управления доступом. – М., 2017. – 92 с.

71. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2009. – 31 с.

72. ГОСТ Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2012. – 19 с.

73. ТП 78.36.005-2014. Типовой рабочий проект. Система контроля и управления доступом. Административное здание. – М., 2019. – 37 с.

74. Р 78.36.002-2010. Рекомендации. Выбор и применение систем охранных телевизионных. – М., 2010. – 183 с.

75. Р 78.36.027-2012. Рекомендации по применению тепловизионного оборудования в системах охранного телевидения. – М., 2012. – 304 с.

76. Р 78.36.042-2014. Рекомендации по использованию комплекта оборудования для фиксации и передачи видеоинформации с охраняемого объекта на ПЦО. – М., 2014. – 97 с.

77. ТП 78.36.004-2014. Типовой рабочий проект. Система охранного телевидения. – М., 2014. – 34 с.

78. Р 78.36.049-2015. Рекомендации. Применение оборудования охранных телевизионных систем в условиях ограниченной видимости или других дестабилизирующих факторов. – М., 2015. – 111 с.

79. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2014. – 27 с.

ПРИЛОЖЕНИЯ

Приложение 1

Приложение №_____
к договору №_____
от «____»_____20__г.

АКТ ПЕРВИЧНОГО ОБСЛЕДОВАНИЯ №_____

_____ «____»_____20__г.
(наименование населенного пункта)

Комиссия в составе:
представителя собственника объекта (далее Заказчик)

_____
(должность представителя Заказчика и наименование организации)
представителя охранной организации

_____
(должность представителя и наименование организации)
представителя заинтересованных организаций

_____
(должность представителя и наименование организации)

_____
(должность представителя и наименование организации)
произвела обследование объекта Заказчика:

_____
(наименование объекта с указанием организации)
расположенного по адресу:

_____
(почтовый адрес объекта, контактный телефон)
режим работы объекта:

_____

ОБСЛЕДОВАНИЕМ УСТАНОВЛЕНО:

Краткая характеристика объекта:

_____
(указывается инженерно-техническая укрепленность объекта на местности,

ориентиры, ограждение территории, подъезды, наличие физической охраны,

главный и запасные входы, этажность, количество и экспликация обособленных

помещений, материалы стен здания, наличие подвала и чердака, наличие

смежных помещений сторонних организаций, тип крыши)

Инженерно-техническая укрепленность:

(указывается инженерно-техническая укрепленность строительных конструкций

стен, перекрытий, дверей, оконных проемов (витрин), люков, наличие

некапитальных стен, решеток, сейфов, платежных терминалов, входов

инженерных коммуникаций, определяется строительная готовность объекта

для приема под охрану)

Оснащенность объекта средствами охраны и связи:

(указываются установленные средства сигнализации, места блокировки,

количество и тип извещателей, места установки, тип оконечного устройства

СПИ и места установки оповещателей, наличие и тип резервного источника

питания, места расположения и защищенность распределительных

(коммутационных) узлов проводной абонентской телефонной связи и точки

подключения Интернета, прохождение УКВ-радиосигнала и приоритетный оператор GSM

_____

(при соответствующих подключениях на ПЦО), при необходимости определяется помеховая обстановка на объекте (наличие помех

_____

_____

и шумов), степень пожароопасности и взрывоопасности помещений объекта)

ВЫВОД КОМИССИИ:

Отнести объект к классу_____

Инженерно-техническая укрепленность объекта _____

_____

(соответствует/не соответствует установленной категории)

Уязвимые места и вероятные способы проникновения через них (нападение, открытие, пролом и т. д.)

_____

_____

Смонтированные технические средства охраны (состав и наличие) _____, по выполненному монтажу_____

(соответствует/не соответствует) (соответствует/не соответствует)

Техническая возможность подключения ТСО объекта на ПЦО

_____

(указать ПЦО, имеется/не имеется)

Предложения охранной организации:

В соответствии с заявкой объект подлежит оборудованию средствами _____ с последующим заключением договора на

(указать тип сигнализации)

централизованную охрану с _____

(указать наименование охранной организации)

после выполнения Заказчиком в установленные сроки **мероприятий по инженерно-технической укрепленности:**

_____

(указываются конкретные мероприятия по инженерно-техническому укреплению)

_____

_____

_____

_____

мероприятий по оснащению объекта средствами сигнализации и подключению каналов связи:

_____

(указываются конкретные мероприятия по оснащению объекта средствами

_____

сигнализации и подключению каналов связи на ПЦО)

_____

общих мероприятий по усилению охраны объекта:

_____

(указываются конкретные мероприятия по усилению надежности охраны объекта)

_____

_____

Назначить предварительный срок контрольной проверки выполнения мероприятий на «____»_____20__г.

Приложения к акту _____ на _____листах.

(исходные данные, описания, схемы блокировки и т. д.)

Примечание. Настоящий акт является неотъемлемой частью договора о централизованной охране объекта и составлен в ____экземплярах.

Приложение 2

Резолюция руководителя

_____

_____

(дата, подпись)

А К Т (ОБРАЗЕЦ)
обследования технического состояния объекта

« » 20 г. г._____

Мы, нижеподписавшиеся, представитель «Исполнителя» *(наименование охранной организации, ФИО, должность специалиста, проводящего обследование)* _____

с одной стороны, и представитель «Заказчика» *(ФИО, должность уполномоченного представителя собственника объекта)*_____

с другой стороны, произвели обследование технического состояния охраняемого объекта: *(наименование объекта),* расположенного по адресу:_____

_____

ХАРАКТЕРИСТИКА ОБЪЕКТА

Объект расположен на первом этаже пятиэтажного здания торгового комплекса.

1. ОБСЛЕДОВАНИЕМ УСТАНОВЛЕНО:

1.1. Состояние технической укрепленности (ограждений, освещения, дверей, окон, запоров, решеток, контрольно-пропускных пунктов, проездных ворот и т. д.).

Объект представляет собой частную торговую организацию, расположенную в пятиэтажном кирпичном строении с плоской крышей. Объект занимает часть помещений 1-го этажа и подвала, имеет один центральный вход и один запасной выход. Общая защищаемая площадь_____кв. м, объект принадлежит подгруппе_____ согласно _____.

1. Центральные входные двери двойные, металлопластиковые, со стеклянными вставками. Металлическими решетками не защищены. Наружные центральные входные двери (общего пользования) не оборудованы средствами охранной сигнализации. Внутренние центральные входные

двери (непосредственно магазина) оборудованы извещателями на открывание и разрушение стекла.

2. Между наружными и внутренними дверями расположен тамбур общего пользования с выходом на лестничную клетку и в лифтовый холл. Все центральные входные двери запираются на врезные запорные устройства – по одному на дверь.

3. Оконные проемы (стеклопакеты) металлическими решетками не защищены. Оборудованы ТСО на разрушение стекла и открывание (на открывающихся рамах).

4. На объекте имеется кассовая комната. Входная дверь в кассу деревянная, филенчатая, с окном приема денег.

5. Подвал имеет две входные двери (металлические, каждая оборудована одним запорным устройством). Внутренний объем подвала защищен ТСО – объемными ИК-извещателями.

6. В подвале имеются два оконных проема, один оконный проем защищен металлическим ставнем изнутри помещения, второй оконный проем защищен металлической решеткой изнутри помещения, оборудован ТСО на открывание.

7. В подвале имеется выход из лифтовой шахты. Дверь металлическая, запирается на металлический засов изнутри подвала. Дверь оборудована ТСО на открывание.

8. В подвале имеется коллектор вентиляционных коробов. Все возможные места проникновения из вентиляционных коробов оборудованы ТСО – объемными ИК-извещателями.

9. На объекте имеются помещения с отдельным входом сторонних организаций. Внутренние стены между охраняемыми и неохраняемыми помещениями не капитальные в 0,5 кирпича.

1.2. Оснащенность техническими средствами охраны (ТСО)

_____*(достаточная, недостаточная)*___

1.2.1. Необходимость дополнительной установки технических средств охраны

_____*(имеется или отсутствует)*_____

1.2.2. Проведение капитального ремонта средств ТСО

_____*(требуется или не требуется*)_____

1.2.3. Сигнализация смонтирована __ _____

В целях обеспечения надежной охраны объекта(ов) «Заказчику» необходимо выполнить следующие мероприятия.

1. На входные и тыловые двери, а также двери, ведущие в подвал, установить дополнительно по одному врезному запорному устройству на расстоянии не менее 300 мм друг от друга.
2. Все оконные проемы и центральные двери объекта защитить распашной или раздвижной металлической решеткой с внутренней стороны охраняемого помещения или защитным остеклением класса защиты Р3А, Р4А по ГОСТ Р 30826-2014. Решетка должна быть изготовлена из металлического прутка диаметром не менее 16 мм, шаг ячейки не более 150×150 мм, в местах пересечения металлические прутки должны быть сварены между собой. Решетка обрамляется металлическим уголком размерами 35×35×4 мм. Данные решетки прикрепляются к стенам и перекрытиям металлическими анкерами диаметром не менее 8 мм на глубину не менее 120 мм, шаг установки анкеров – не более 500 мм.
3. Деревянную филенчатую дверь в кассу заменить на металлическую толщиной не менее 2 мм или усилить обивкой с двух сторон листовой сталью толщиной не менее 0,6 мм, с загибом листа на внутреннюю поверхность двери или на торец полотна внахлест, с креплением по периметру и диагоналям полотна гвоздями диаметром 3 мм и шагом не более 50 мм.
4. На входе коллектора вентиляционных коробов в подвале установить металлическую решетку из прутка диаметром не менее 16 мм, шаг ячейки не более 150×150 мм, в местах пересечения металлические прутки должны быть сварены между собой.
5. Некапитальные внутренние стены, граничащие с неохраняемыми помещениями других организаций, усилить стальными, сваренными в соединениях решетками из прутка толщиной не менее 10 мм, с ячейкой размерами не более 150×150 мм. Данные решетки закрепляются металлическими анкерами диаметром не менее 8 мм на глубину не менее 120 мм, шаг установки анкеров – не более 500 мм. Установленную решетку закрыть стеновыми (облицовочными) панелями или штукатуркой.
6. Сейф в кассе весом менее 1000 кг закрепить металлическими анкерами или приварить к полу и стене.

Мероприятия по пунктам_____ предлагаются с____*(дата)*_____;
по пунктам_____ предлагаются с____*(дата)*_____.
Указанные мероприятия должны быть выполнены «Собственником» в следующие сроки:

_____

«Заказчик» обязуется:
– информировать «Исполнителя» о предполагаемых перепланировках и перепрофилировании объекта(ов) с целью своевременного внесения изменений в систему охраны;
– не загораживать посторонними предметами зону действия приборов ТСО;
– выполнить предлагаемые мероприятия в установленные сроки.
Настоящий акт является неотъемлемой частью договора на охрану объекта(ов), составлен в двух экземплярах и хранится у «Исполнителя» и «Заказчика».

Представитель «Исполнителя»	Представитель «Заказчика»
_____	_____
_____	_____
_____	_____
(подпись)	*(подпись)*
М.П.	М.П.

Список используемых сокращений

АКБ – аккумуляторная батарея
АКЛ – армированная колючая лента
ВОЛС – волоконно-оптические линии связи
ГЗ СП ВО – группа задержания специального подразделения вневедомственной охраны войск национальной гвардии Российской Федерации
ГУВО Росгвардии – Главное управление вневедомственной охраны Федеральной службы войск национальной гвардии Российской Федерации
ЗП – задание на проектирование (реконструкцию) системы охранной сигнализации
ИТС – инженерно-технический состав подразделений вневедомственной охраны
ИТУ – инженерно-техническая укрепленность
ИЭПВР – источник электропитания вторичный с резервом
КПП – контрольно-пропускной пункт
МВД России – Министерство внутренних дел Российской Федерации
МПХИГ – места проживания и хранения имущества граждан
МХИГ – места хранения имущества граждан
НСД – несанкционированный доступ
ОС – охранная сигнализация
ПУЭ – правила устройства электроустановок
ПЦН – пульт централизованного наблюдения
ПЦО – пункт централизованной охраны подразделений вневедомственной охраны войск национальной гвардии Российской Федерации
СКУД – система контроля управления доступом
СОС – система охранной сигнализации
СОТ – система охранная телевизионная
СПИ – система передачи извещений
ТСО – техническое средство охраны
УКВ – ультракороткие волны
УОО – устройство оконечное объектовое
УС – устройство самообслуживания
ФСБ России – Федеральная служба безопасности Российской Федерации
ШС – шлейф сигнализации

Учебное издание

Комплексная защита объектов информатизации. Книга 29

ТЕЛЬНЫЙ Андрей Викторович

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Проектирование технических средств защиты территорий и объектов
от несанкционированного доступа

Учебное пособие

Редактор Т. В. Евстюничева
Технический редактор Е. А. Лебедева
Корректор Н. В. Пустовойтова
Компьютерная верстка Е. А. Кузьминой
Выпускающий редактор А. А. Амирсейидова

Подписано в печать 21.12.20.
Формат 60×84/16. Усл. печ. л. 14,65. Тираж 50 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.