Воронежский институт МВД России

СИСТЕМЫ ОХРАННОГО МОНИТОРИНГА

Курс лекций

Воронеж
2021

ББК 30.82
УДК 351.74
С34

Коллектив авторов: С. А. Винокуров, С. А. Гречаный, М. В. Таравков, О. В. Толстых.

Рецензенты: Е. В. Спиридонов, начальник ФГКУ «УВО ВНГ России по Воронежской области», полковник полиции;
Ю. В. Харченко, начальник УВО по г. Воронежу – филиала ФГКУ «УВО ВНГ России по Воронежской области», полковник полиции.

С34 **Системы** охранного мониторинга : курс лекций / С. А. Винокуров [и др.]. – Воронеж : Воронежский институт МВД России, 2021. – 161 с.

ISBN 978-5-88591-898-5

Содержание курса лекций отражает наиболее важные положения основных разделов и тем рабочей программы дисциплины «Системы охранного мониторинга».

В издании проанализированы состав, функциональные возможности применения и эксплуатации основных технических средств и систем охранного мониторинга: охранно-пожарной сигнализации, внутриобъектовых радиоканальных систем безопасности, интегрированных систем безопасности, систем охранных телевизионных, систем контроля управления доступом, систем сбора и обработки информации, систем антитеррористической защиты объектов.

Курс лекций разработан для курсантов и слушателей радиотехнического, юридического факультета, слушателей факультета заочного обучения, а также будет полезен слушателям факультета переподготовки и повышения квалификации и профессиональной подготовки.

.

С-54-36(I)-21 **ББК 30.82**

ISBN 978-5-88591-898-5

СОДЕРЖАНИЕ

Перечень сокращений

АПК – аппаратно-программный комплекс
АРМ – автоматизированное рабочее место
АС – автоматизированная система
БИ – блок излучателя
БОС – блок обработки сигнала
БП – блок приемника
Г – генератор
ГЛОНАСС – глобальная навигационная спутниковая система
ДЦ – диспетчерский центр
ЕДДС – единая дежурно-диспетчерская служба
ИБП – источник бесперебойного питания
ИО – извещатель охранный
ИСБ – интегрированная система безопасности
ИЭ – исполнительный элемент
К – клавиатура
ОЗУ – оперативное запоминающее устройство
ОО – охранный оповещатель
ОПС – охранно-пожарная сигнализация
ПВИ – пассивный вибрационный извещатель
ПО – программное обеспечение
ППК – прибор приемно-контрольный
ПЦО – пункт централизованной охраны
ПЭВМ – персональная электронная вычислительная машина
РСЧС – единая государственная система предупреждения и ликвидации чрезвычайных ситуаций
СКУД – система контроля и управления доступом
СМПО – система мониторинга подвижных объектов
СОМ – системы охранного мониторинга
СОС – система охранной сигнализации
СОТ – система охранная телевизионная
СПИ – система передачи извещений
ССОИ – система сбора и обработки информации
СТС – система тревожной сигнализации
ТС – транспортное средство
ТСОС – техническое средство охранной сигнализации
УКВ – ультракороткие волны
УКНП – устройство контроля напряжения питания
УОО – устройство оконечное объектовое
УОП – устройств оконечное пультовое
ЦОВ – центр обработки вызовов
ЦУКС – центр управления в кризисных ситуациях

ЧЭ – чувствительный элемент
ШС – шлейф сигнализации
ЭОС – экстренная оперативная служба
AHD – analog high definition
GPS – global positioning system
HD-CVI – high definition composite video interface
HD-TVI – high definition transport video interface
IP – internet protocol
LAN – local area network
NTSC – national television system committee
PAL – phase alternating line
PTZ – pan, tilt, zoom
SMS – short message service
SQL – structured query language

ВВЕДЕНИЕ

Среди приоритетных направлений развития науки, технологий и техники Российской Федерации на первом месте стоит «Безопасность и противодействие терроризму». В связи с высокой уязвимостью к криминальным и террористическим угрозам в настоящее время перед правоохранительными органами Российской Федерации поставлена серьезная задача повышения уровня безопасности объектов особой важности, повышенной опасности, жизнеобеспечения, с массовым пребыванием людей, критически важных и других объектов, подлежащих обязательной государственной охране на территории нашей страны. Последствия криминальных воздействий или террористических актов на данных объектах могут привести к гибели большого количества людей, а также нанести значительный материальный, экономический, экологический ущерб обществу и государству.

Чтобы обеспечить требуемый уровень безопасности объектов указанных категорий, не обойтись без должного уровня инженерно-технической укрепленности и построения системы, включающей в себя человеческие ресурсы, технические средства и системы, а главное – умение анализировать информацию о реальных угрозах и их последствиях. Поэтому обеспечение безопасности таких объектов возложено на профессионально подготовленные и технически оснащенные подразделения правоохранительных органов с использованием современных технических средств и систем охранного мониторинга.

Использование систем охранного мониторинга, и в частности систем охранно-тревожной и пожарной сигнализации, внутриобъектовых радиоканальных систем безопасности, систем охранных телевизионных, систем контроля и управления доступом, систем сбора и обработки информации, систем мониторинга подвижных объектов, интегрированных систем безопасности, технических средств и систем безопасности банковских устройств самообслуживания, технических средств и систем антитеррористической защиты объектов, аппаратно-программных комплексов, несомненно, при повышении антитеррористической устойчивости и противокриминальной защиты важных объектов позволит обеспечить комплексную безопасность объектов любой категории сложности.

ТЕМА 1
ОСНОВЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Учебные и воспитательные цели:

Образовательные: ознакомить обучающихся с основами обеспечения комплексной безопасности объектов.

Развивающие: расширить базовые знания обучающихся в области противокриминальной и антитеррористической защиты объектов; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

1.1. Основные термины и определения.

1.2. Категорирование объектов.

1.3. Классификация угроз безопасности объектов. Модель угроз и модель нарушителя.

1.4. Основы концептуального проектирования систем безопасности.

1.5. Предпроектное обследование объекта.

1.1. Основные термины и определения

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Безопасность антитеррористическая – состояние защищенности физического лица или объекта от террористических угроз.

Безопасность защищаемого объекта – состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей; имуществу физических или юридических лиц; государственному или муниципальному имуществу; техническому состоянию, инфраструктуре жизнеобеспечения; внешнему виду, интерьеру(ам), ландшафтной архитектуре; окружающей природной среде.

Безопасность противокриминальная – состояние защищенности объекта, характеризующееся отсутствием недопустимого риска или угроз различного типа, обеспечиваемое комплексом защитных мер.

Безопасность технической системы – состояние защищенности технической системы, характеризующееся отсутствием недопустимого

риска. Интересы жизненно важные – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Мера защитная – мера, используемая для уменьшения риска или угроз различного типа.

Мера защитная техническая – мера, используемая для уменьшения риска или угроз различного типа путем применения технических средств охраны.

Опасность криминальная – состояние, характеризующееся присутствием угроз различного типа или недопустимого риска возникновения ущерба.

Опасные вещества и материалы – пожаро- и взрывоопасные вещества и материалы, токсичные и высокотоксичные неорганические и органические соединения, материалы, способные к самовозгоранию, образованию взрывоопасных смесей при взаимодействии с водой, кислородом воздуха или друг с другом либо разлагающиеся под действием повышенных температур, токсичные и высокотоксичные вещества естественного и искусственного происхождения в любом агрегатном состоянии, радиоактивные вещества и соединения, все виды ядерных материалов, другие вещества и материалы, попадание которых в окружающую среду в определенных концентрациях либо несанкционированное использование которых способно вызвать гибель либо тяжелые заболевания людей, тяжелые экологические последствия, а также значительный материальный ущерб.

Риск – вероятность причинения вреда жизни, здоровью физических лиц, окружающей среде, в том числе животным или растениям, имуществу физических или юридических лиц, государственному или муниципальному имуществу с учетом тяжести этого вреда.

Риск нанесения ущерба – комплексный показатель, характеризующий вероятность возникновения ущерба за нормированный период времени и его величину.

Риск нанесения ущерба допустимый – риск нанесения ущерба, который в конкретной области деятельности признается допустимым при возникновении определенной опасной ситуации.

Защита имущества противокриминальная – совокупность мер, направленных на предотвращение преступного посягательства и несанкционированного доступа на объект и других криминальных действий.

Защита объекта антитеррористическая – совокупность мер, направленных на предотвращение возникновения преднамеренного противоправного уничтожения или нанесения ущерба объекту.

Защита объекта комплексная – совокупность взаимосвязанных по времени, ресурсам и месту проведения мероприятий для достижения

цели(ей) по обеспечению защиты объекта от нормированных угроз техногенного, антропогенного и природно-климатического характера.

Защита физическая – совокупность охраны объекта, организационных, административных и правовых мер, инженерно-технических средств, вооружения и специальных средств, предназначенных для предотвращения несанкционированных действий в отношении объекта.

Обеспечение безопасности защищаемого объекта комплексное – деятельность по созданию условий и обеспечению ресурсов для предотвращения и/или уменьшения последствий для защищаемого объекта от угроз различной природы возникновения и различного характера проявления.

Охрана противокриминальная – комплекс организационных и технических мероприятий по ограничению доступа и предотвращению криминальных угроз и посягательств, защите территории, помещений, источников информации, средств и предметов производства, продукции и объектов различных форм собственности.

Охрана противокриминальная автономная – обособленная противокриминальная охрана объекта без автоматической передачи информации о его состоянии на пункт централизованной охраны.

Охрана противокриминальная централизованная – противокриминальная охрана территориально рассредоточенных объектов с помощью пунктов централизованной охраны.

Критические элементы объекта – зоны, территории, административно-производственные здания и сооружения, конструктивные и технологические элементы объекта, элементы систем, оборудования или устройств потенциально опасной установки, места использования, хранения и уничтожения ОВМ, несанкционированные действия в отношении которых приводят к прекращению нормального функционирования объекта, его повреждению или аварии или созданию угрозы возникновения чрезвычайной ситуации.

Объект жизнеобеспечения – объект, на котором сконцентрированы жизненно важные материальные, финансовые средства и услуги, сгруппированные по функциональному назначению и используемые для удовлетворения жизненно необходимых потребностей населения (например, в виде продуктов питания, жилья, предметов первой необходимости, а также медицинского, санитарно-эпидемиологического, информационного, транспортного, коммунально-бытового обеспечения).

Объект защищаемый – предприятие, организация, учреждение, заведение, жилое домовладение или жилой комплекс, религиозно-конфессиональное объединение (или их неотъемлемая составная часть, включая занимаемую территорию и прилегающую акваторию в отведенных границах), состояние которых контролируется или подлежит

контролю с конкретной целью (для защиты от угроз и/или для профилактики угроз) и на основе соблюдения действующего законодательства.

Объект критически важный – объект, нарушение или прекращение функционирования которого приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению, разрушению или существенному снижению безопасности жизнедеятельности населения, проживающего на этой территории, на длительный период времени.

Объект особо важный – техногенный, природный, природно-техногенный объект, подверженный риску криминальных угроз нанесения неприемлемого ущерба самому объекту, природе и обществу, а также подверженный угрозам возникновения чрезвычайных обстоятельств.

Объект повышенной опасности – объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво- и пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу жизни и здоровью людей, а также окружающей среде.

Объект противокриминальной охраны – строительная конструкция или ее часть, территория или ее фрагмент, отдельно расположенные предметы или предмет (принадлежность для хранения ценностей или имущества, экспонат, культовый атрибут, развлекательно-игровой реквизит, вещь).

Объект с массовым пребыванием граждан – объект инфраструктуры, на котором возможно одновременное пребывание более 500 человек. Указанные объекты делятся на следующие типы: транспорт (авто- и ж/д вокзалы, аэродромы, речные порты); торговые центры (рынки, торговые центры с общей торговой площадью свыше 10 тыс. кв. м); спортивные (стадионы, спортивные манежи и комплексы, бассейны); культурно-массовые (дома культуры, театры, кинотеатры, цирки, культурно-развлекательные центры и т.п.); образовательные учреждения (школы, детские дома, профтехучилища, институты повышения квалификации, вузы); лечебно-оздоровительные организации (больницы, клиники, госпитали, санатории), а также места организованного отдыха и оздоровления детей (100 и более человек).

Субъекты охраны – персонал охраняемого объекта (владельцы, работники, администрация) и его посетители, сотрудники службы охраны и безопасности (охранники, инженерно-технические специалисты), совместно участвующие в функционировании системы охраны и безопасности объекта.

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.

Ценности охраняемые – изделия и предметы, имеющие какую-либо материальную, культурную, духовную или интеллектуальную ценность, являющиеся объектом охраны.

Модель нарушителя – формализованные сведения о численности, оснащенности, подготовленности и осведомленности нарушителей, их мотивации и преследуемых ими целях, используемые при выработке требований к системе физической защиты и оценке ее эффективности.

Нарушитель – лицо, совершившее или пытающееся совершить несанкционированные действия в отношении объекта промышленности или энергетики, а также лицо, оказывающее содействие в этом.

Нейтрализация нарушителя – реализация действий системы физической защиты по отношению к нарушителю, в результате чего он лишается возможности продолжать несанкционированные действия

Несанкционированные действия – непосредственные действия, совершаемые в отношении объекта тем или иным лицом, нарушающие положения действующего законодательства, нормативных актов и установленных на объекте внутриобъектового и пропускного режимов.

Единая дежурно-диспетчерская служба – орган повседневного управления местной (региональной, муниципальной, городской) системой/подсистемой предупреждения, обнаружения и ликвидации чрезвычайных ситуаций на защищаемых объектах и территориях (акваториях).

Инженерно-технические средства охраны – комплекс технических средств и устройств, предназначенных для предотвращения несанкционированных проникновений нарушителя на объект или выявления несанкционированных действий в отношении объекта.

Пульт централизованного наблюдения (ПЦН) – самостоятельное техническое средство (совокупность технических средств) или составная часть системы передачи извещений, устанавливаемая в пункте централизованной охраны (пункте установки ПЦН) для приема от пультовых оконечных устройств или ретранслятора (ов) извещений о проникновении на охраняемые объекты и/или пожаре на них, служебных и контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки, а также (при наличии обратного канала) для передачи через пультовое оконечное устройство на ретранслятор(ы) и объектовые оконечные устройства команд телеуправления.

Рубеж охранной сигнализации – шлейф сигнализации, совокупность шлейфов или лучей (для сигнализации, использующей передачу извещений по радиоканалу), контролирующих охраняемые зоны, территории, здания или помещения (периметр, объем или площадь

последних, непосредственно ценности или подходы к ним) на пути возможного движения нарушителя к материальным ценностям, при преодолении которых выдается соответствующее извещение о проникновении.

Система безопасности интегрированная (ИСБ) – специализированная сложная техническая система, объединяющая на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных технические средства, предназначенные для защиты объекта от нормированной угрозы или нормированных угроз.

Система безопасности комплексная (КСБ) – система безопасности, одновременно выполняющая несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей.

Система интегрированная – система, объединяющая и совместно использующая информационные ресурсы подсистем и одну общую базу данных и при этом, в отличие от автономных систем, позволяющая работать с каждым ресурсом в отдельности.

Система интегрированная закрытая – система, объединяющая типы подсистем (более одного) так, что они разделяют общие информационные ресурсы системы и общую базу данных, в случае если они установлены вместе (интегрированы) в соответствующей конфигурации, причем выбор конечного пользователя может быть ограничен системами (периферийным оборудованием) только одного производителя.

Система интегрированная открытая – система, предназначенная для совместной работы с другими открытыми системами и обеспечения интеграции с ними с использованием в нормальном состоянии общей базы данных, общего интерфейса и программного обеспечения, общего для этих систем при обмене информацией друг с другом, обеспечивающего как вертикальную, так и горизонтальную интеграцию.

Система комбинированная – совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах и пожара на них, передачи, сбора, обработки и представления в заданном виде информации.

Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Система оповещения – комплекс средств оповещения, выполняющий функцию одновременного доведения до большого числа потребителей речевых сообщений, звуковых и/или световых сигналов.

Система оповещения и управления эвакуацией с охраняемого объекта – совокупность технических средств, предназначенных для оповещения о пожаре и указания путей эвакуации с объекта.

Система охранного телевидения – совокупность совместно действующих технических средств, включающая телевизионные камеры с объективами, видеомониторы и вспомогательное оборудование, требуемое для организации видеоконтроля.

Система охранно-пожарной сигнализации – совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах (и/или пожара на них), передачи, сбора, обработки и представления информации в заданном виде.

Система передачи данных (информации) – совокупность совместно действующих технических средств, предназначенных для передачи и приема по каналам связи информации о состоянии охраняемого объекта, а также для передачи и приема команд дистанционного контроля и управления.

Система передачи извещений о проникновении и пожаре (система передачи извещений) – совокупность совместно действующих технических средств, предназначенных для передачи по каналам связи и для приема в пункте централизованной охраны извещений о проникновении на охраняемые объекты и (или) пожаре на них, служебных и контрольно-диагностических извещений, а также (при наличии обратного канала) для передачи и приема команд телеуправления.

Система пожарной сигнализации охраняемого объекта – совокупность технических средств пожарной сигнализации, установленных на объекте и передающих сигналы на пункт охраны объекта.

Система предотвращения пожара на охраняемом объекте – совокупность организационных мероприятий и технических средств, направленных на исключение предпосылок и условий для возникновения, развития и распространения пожара.

Система противодымной защиты охраняемого объекта – совокупность технических средств, предназначенных для предотвращения воздействия на людей дыма, повышенной температуры и токсичных продуктов горения.

Система техническая сложная для защиты объекта – организационно-техническая система, включающая в себя совокупность технических средств или их комплексов, программное обеспечение, а также документированные процедуры штатных действий персонала, эксплуатационную документацию, материалы, инструменты, приборы, необходимые для использования в комплексной защите объекта.

Система тревожной сигнализации автоматическая – система тревожной сигнализации (система охранной (охранно-пожарной) сигнализации), обеспечивающая автоматический переход из нормального состояния в отключенное и обратно под управлением ответственного лица,

пользователя, владельца или жильца без обращения к другим системам, например к системе электросвязи.

Система тревожной сигнализации ручная – система тревожной сигнализации, обеспечивающая переход из нормального состояния в отключенное и обратно не автоматически.

Системы технические антитеррористической и противокриминальной безопасности – системы, включающие в себя технические средства, обеспечивающие безопасность объекта или субъекта от террористических и криминальных угроз.

Средства физической защиты инженерные – технические средства (преграды, барьеры, инженерные конструкции), препятствующие своими физическими свойствами несанкционированному проникновению на объект и/или в охраняемую зону (на часть территории, в здание, строение, сооружение, помещение).

Шлейф охранной сигнализации – электрическая цепь, соединяющая выходные цепи охранных извещателей, включающая в себя вспомогательные элементы и соединительные провода и предназначенная для передачи на приемно-контрольный прибор извещений о проникновении и неисправности, а в некоторых случаях и для подачи электропитания на охранные извещатели.

Декларация о соответствии системы безопасности защищаемого объекта – документ, удостоверяющий соответствие системы безопасности защищаемого объекта установленным требованиям.

Декларирование соответствия системы безопасности защищаемого объекта – форма подтверждения соответствия технических средств системы безопасности защищаемого объекта установленным требованиям по обеспечению безопасности.

Знак соответствия системы безопасности защищаемого объекта – обозначение, служащее для информирования собственников (пользователей) о соответствии системы безопасности защищаемого объекта установленным требованиям.

Значимость защищаемого объекта – оцениваемое по определенному критерию значение (важность) защищаемого объекта с последующей классификацией.

Идентификация системы безопасности защищаемого объекта – установление тождественности характеристик технических подсистем и средств системы безопасности объекта их существенным признакам.

Латентность защищаемого объекта – скрытые, не поддающиеся непосредственному измерению свойства и особенности объекта, определяющие условия его комплексной защиты и потенциально опасные последствия от возникновения угрожающей или чрезвычайной ситуации на объекте.

Латентность фактора угрозы нанесения ущерба (вреда) защищаемому объекту – свойства и особенности фактора угрозы защищаемому объекту, трудно поддающиеся (или не поддающиеся) своевременному, объективному и достоверному прогнозированию и непосредственному измерению последствий при реализации угрозы.

Оценка соответствия системы безопасности защищаемого объекта – прямое или косвенное определение соблюдения требований, предъявляемых к системе безопасности защищаемого объекта и к самому защищаемому объекту.

Подтверждение соответствия системы безопасности защищаемого объекта – комплексная проверка соответствия системы безопасности объекта установленным требованиям по обеспечению безопасности.

Совместимость технических средств электромагнитная – способность технического средства функционировать с заданным качеством в заданной электромагнитной обстановке и не создавать недопустимых электромагнитных помех другим техническим средствам.

Форма подтверждения соответствия системы безопасности защищаемого объекта – установленный порядок документального оформления соответствия системы безопасности защищаемого объекта предъявляемым требованиям.

Видеоконтроль – получение, обработка, передача, регистрация и хранение телевизионных изображений из охраняемой зоны, анализ информации и принятие соответствующего решения оператором.

Объект контроля – человек, имущество (событие, явление), на определение состояния (развития) которого направлен видеоконтроль.

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 – идентификация, основанная на использовании индивидуальных физических признаков человека.

1.2. Категорирование объектов

Решение о присвоении объекту определенной категории принимается комиссией с участием представителей вневедомственной охраны, контрагента и иных заинтересованных организаций.

Для оценки возможных последствий реализации криминальных угроз используют следующие виды ущерба:

– государственно-политический ущерб – ухудшение криминогенной обстановки в стране (регионе), негативный международный и общественный резонанс, негативные публикации в СМИ, подрывающие международный авторитет государства, формирующие негативное отношение к органам внутренних дел;

– финансово-экономический ущерб.

В зависимости от значимости, концентрации материальных, художественных, исторических и культурных ценностей, размещенных на объекте, последствий от возможных криминальных посягательств на них, объекты, охраняемые или подлежащие передаче под централизованную охрану подразделениями вневедомственной охраны, подразделяются на категории:

– А1, А2, и А3 (категория А1 – наивысшая) – это объекты государственной власти, критически важные объекты, особо важные объекты, потенциально опасные объекты и объекты жизнеобеспечения, государственные, а также коммерческие объекты, преступные посягательства на которые могут привести к особо крупному экономическому ущербу государству или собственнику имущества и иметь широкий международный и общественный резонанс;

– Б1 и Б2 – это объекты организаций различных форм собственности, преступные посягательства на которые могут привести к крупному и значительному материальному ущербу предприятию или собственнику. Объекты, не вошедшие в перечни, классифицируются по ближайшему аналогу с учетом возможного риска и ущерба вследствие преступного посягательства на них.

Объекты категории А1 (наивысшая).

Специальные помещения, расположенные на территории (в зданиях, сооружениях) объектов критически важных, особо важных и потенциально опасных объектов инфраструктуры Российской Федерации, объектов подлежащих обязательной охране полицией, определенных перечнями, утвержденными Правительством Российской Федерации.

К объектам категории А1 относятся:

– хранилища и кладовые (сейфовые комнаты) денежных и валютных средств, ценных бумаг;

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

– помещения с оборотом сведений, составляющих государственную тайну;

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

– хранилища наркотических и психотропных веществ и препаратов;

– хранилища федеральных государственных музеев, государственных архивов и федеральных библиотек.

Объекты категории А2.

Государственные и коммерческие объекты с оборотом денежных средств, драгметаллов, драгоценных камней, ювелирных изделий и иных материальных и культурных ценностей, преступные посягательства на

которые могут привести к особо крупному экономическому ущербу государству или собственнику имущества (не вошедшие в категорию А1):

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

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

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

– объекты (комнаты) хранения оружия и боеприпасов, наркотических, сильнодействующих и психотропных веществ и препаратов, драгоценных металлов, камней и изделий из них;

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

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

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

– помещения с хранением документов строгой отчетности или спецпродукции;

– объекты отправления религиозного культа, представляющие историческую ценность.

Объекты категории А3.

Критически важные и потенциально опасные объекты, объекты, подлежащие обязательной охране полицией, в соответствии с соответствующими 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 категории Б1.

Объекты организаций различных форм собственности с сосредоточением материальных ценностей, преступные посягательства на которые могут привести к крупному или значительному ущербу собственнику имущества:

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

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

– объекты мелкооптовой и розничной торговли;

– иные объекты потребительского рынка;

– объекты ЖКХ (ТСЖ, управляющие компании).

Объекты категории Б2.

Государственные или коммерческие объекты, собственниками которых принято решение об установке системы тревожной сигнализации:

– служебные помещения охраны ГСК, автостоянок, помещения консьержей в подъездах жилых домов;

– объекты капитального строительства (строительные площадки);

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

Категорирование квартир.

В зависимости от наличия и сосредоточения на момент проведения обследования материальных ценностей и возможного материального ущерба от кражи квартиры подразделяются на категории.

Квартиры категории В1 (наивысшая).

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

Квартиры категории В2.

Квартиры, преступные посягательства на которые могут привести к особо крупному ущербу собственнику.

Квартиры категории В3.

Квартиры, преступные посягательства на которые могут привести к крупному или значительному ущербу собственнику.

Категорирование мест проживания и хранения имущества граждан.

МХИГ категории Г1.

Частные дома, коттеджи, преступные посягательства на которые могут привести к особо крупному ущербу собственнику.

МХИГ категории Г2.

Частные дома, коттеджи, преступные посягательства на которые могут привести к крупному или значительному ущербу собственнику.

МХИГ категории Г3.

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

1.3. Классификация угроз безопасности объектов. Модель угроз и модель нарушителя

Угроза – это событие, которое в случае его проявления способно нанести ущерб охраняемому объекту. Угроза носит вероятностный характер. В настоящее время объекты защиты подвержены проявлению криминальных и террористических угроз.

На основе изучения статистических данных о деятельности практических подразделений МВД России можно констатировать, что для режимных объектов охраны возможно проявление следующих основных видов угроз:

– несанкционированное проникновение на территорию охраняемого объекта;

– проход на основе маскировки (под сотрудника объекта охраны или посетителя);

– установка на объекте охраны средств негласного слухового, визуального, электромагнитного и др. наблюдения;

– нападение на охраняемый объект с целью хищения материальных ценностей, а также с целью завладения оружием, боеприпасами и спецсредствами;

– угрозы жизни и здоровью, травмы и гибель персонала;

– нарушение линий жизнеобеспечения объекта охраны;

– физическая ликвидация потенциала (ресурсов) объекта охраны (взрыв, разрушение);

– нарушение штатного режима функционирования объекта;

– хищение оперативно-служебных документов;

– несанкционированный съем оперативно-служебной информации (перехват физических полей, контроль радио и телефонных переговоров, визуальное и слуховое наблюдение);

– подкуп, шантаж и вербовка персонала, предпринимаемые с различными целями;

– вывод из строя технических средств охраны (например, их некомпетентное использование, неправильная настройка, деблокирование или отключение технических средств охраны злоумышленниками, подкупленным личным составом);

– химическое заражение;

– общественные беспорядки.

В зависимости от возможных последствий и степени опасности угрозы безопасности охраняемым объектам можно разделить на три вида:

– малоопасные (не причиняющие серьезного урона безопасности объекта);

– опасные (оказывающие значительное влияние);

– особо опасные (приводящие к неэффективности охранных мероприятий и нарушению целостности объекта, вызывающие серьезные последствия).

Если в качестве классификационных признаков рассматривать причины (факторы, обуславливающие возможность возникновения) угроз, то можно выделить естественные и искусственные угрозы:

– искусственные – угрозы, происхождение которых связано с деятельностью человека (антропогенные);

– естественные – угрозы, происхождение которых не связано с деятельностью человека, а полностью определяется природными явлениями.

Если же в качестве классификационного признака рассмотреть источник происхождения и характер воздействия (способ реализации) угрозы на охраняемый объект, то можно выделить внешние и внутренние угрозы:

– внутренние – угрозы, источник реализации которых находится внутри охраняемой зоны;

– внешние – угрозы, источник реализации которых находится за пределами охраняемой зоны.

Модель угроз – это детальная проработка всей совокупности путей и способов реализации угроз охраняемому объекту.

Модель угроз разрабатывается с целью:

– определения угроз безопасности охраняемого объекта;

– планирования мер по отражению угроз;

– обоснования выбора средств зашиты охраняемого объекта.

Пути реализации угроз:

1. Реализация угроз без проникновения на охраняемую территорию (характерен для внутренних и внешних угроз естественного происхождения).

2. Реализация угроз посредством проникновения на охраняемую территорию (характерен для внешних угроз искусственного происхождения).

Способы реализации угроз определяются видами воздействия на охраняемый объект с целью причинения ему ущерба. Наиболее характерные из них:

1. Нанесение ущерба с помощью воздействия поражающих факторов взрыва.

2. Нанесение ущерба с помощью воздействия пожара.

3. Нанесение ущерба с помощью кражи материальных ценностей и (или) информации.

4. Нанесение ущерба с помощью вывода из строя технических систем инженерной инфраструктуры и т.д.

В самом общем виде модель угроз изображена на рис. 1.1.

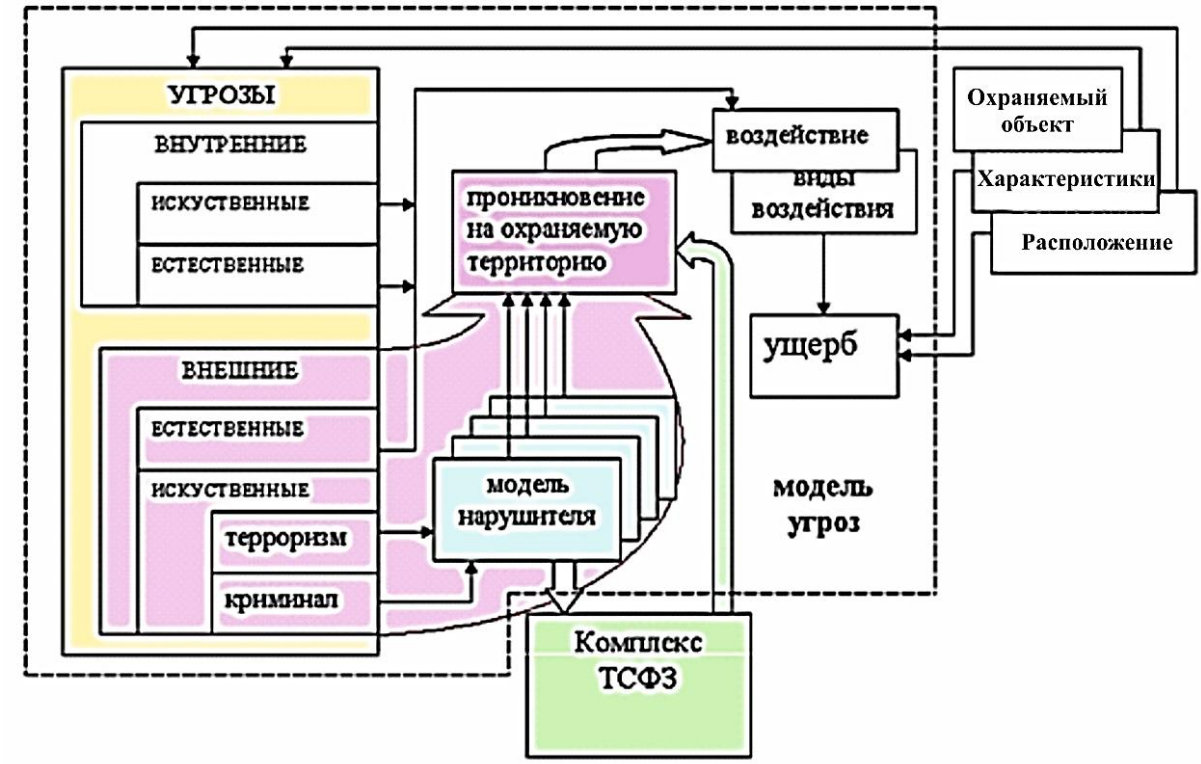


Рис. 1.1. Модель угроз безопасности объекта

Модель угроз безопасности объекта включает в себя:

– полный перечень угроз охраняемому объекту;

– модель нарушителя;

– полный перечень возможных действий (целей и способов их достижения) нарушителя после проникновения его на охраняемую территорию с целью реализации угроз.

Перечень угроз охраняемому объекту во многом определяется его характеристиками и расположением.

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

Таким образом, нарушитель является средством реализации внешних искусственных угроз охраняемому объекту.

Из приведенной модели угроз видно, что основным предназначением комплекса технических средств физической защиты (КТСФЗ) является исключение проникновения нарушителя на охраняемую территорию и, как следствие, предотвращение его воздействия на охраняемый объект с целью нанесения ущерба.

Следовательно, для определения требуемого уровня защищенности объекта (способности его противостоять действиям нарушителя) необходимо формирование модели нарушителя, на способности и возможности которого должен ориентироваться создаваемый КТСФЗ.

Модель нарушителей – совокупность сведений о численности, оснащенности, подготовленности, осведомленности и тактике действий нарушителей, их мотивации и преследуемых ими целях, которые используются при выработке требований к системе физической защиты и оценке ее эффективности.

В самом общем виде модель нарушителя представлена на рис. 1.2.

Рис. 1.2. Модель нарушителя

Способы проникновения нарушителя на объект обладают

информационными признаками, которые должны использоваться для определения каналов проникновения.

На основании статистики нарушений режима, установленного на объекте, и анализа окружающей его криминогенной обстановки, а также оценки возможностей круга заинтересованных в НСД к охраняемому имуществу лиц (организаций) составляется образ (модель) наиболее вероятного нарушителя. Такая модель наделяется максимальными для выбранного типа способностями и возможностями по преодолению СЗП. Созданная модель нарушителя принимается как базовая и относительно нее проходит разработка СЗП. Определение целей вторжения на территорию объекта, модели наиболее вероятного нарушителя и наиболее вероятных сценариев его действий дает возможность сформировать требования к КТСФЗ (например, к системе защиты периметра (СЗП)), при реализации которых возможно ее эффективное противостояние существующим угрозам.

Созданная модель нарушителя принимается как базовая и относительно нее проходит разработка СЗП.

Таким образом:

1. Модель угроз определяет всю совокупность путей и способов реализации угроз охраняемому объекту.

2. Нарушитель является средством реализации внешних искусственных угроз охраняемому объекту.

3. Модель нарушителя определяет всю совокупность характеристик нарушителя, а также способов его проникновения на охраняемый объект.

Модель нарушителя дает возможность определить каналы проникновения и сформировать требования к инженерно-техническим средствам системы охраны, при реализации которых возможно эффективное противостояние существующим угрозам.

Возможная классификация нарушителей представлена на рис. 1.3.

Каждой категории объектов защиты характерны соответствующие виды угроз, например, для объектов топливно-энергетического комплекса характерен следующий перечень потенциальных угроз совершения актов незаконного вмешательства:

1. Угроза захвата.

2. Угроза взрыва.

3. Угроза размещения или попытки размещения на объекте взрывных устройств (взрывчатых веществ).

4. Угроза поражения опасными веществами.

5. Угроза блокирования.

6. Угроза хищения.

7. Угроза технического воздействия.

Рис. 1.3. Классификация нарушителей

1.4. Основы концептуального проектирования систем безопасности

Безопасность любого объекта определяется степенью защищенности его жизненно важных интересов, ресурсов и структур от внешних и внутренних угроз. Комплексная безопасность объекта характеризует защищенность объекта от спектра угроз различного характера. Основные задачи безопасности решаются созданием системы безопасности объекта, которая представляет совокупность организационных, технических и инженерных структур, объединенных определенным алгоритмом функционирования.

Система безопасности может выполняться в виде отдельных целевых систем:

– система физической безопасности (защиты) (СФЗ);
– система защиты объекта при чрезвычайных ситуациях;
– система информационной безопасности (СИБ);
– система экономической безопасности (СЭБ);
– система контроля и управления доступом (СКУД);
– система пожарной сигнализации (СПС);
– система охранная телевизионная (СОТ);
– система охранной сигнализации (СОС);

– или созданием интегрированных систем, в которых объединяются некоторые целевые системы безопасности (СБ).

Формула создания СФЗ достаточно проста – надо сделать так, чтобы в нужное время и в нужном месте на пути нарушителей находились в достаточном количестве средства обнаружения, средства защиты и силы охраны, действующие с требуемой эффективностью. В техническом плане создание СФЗ разделяется на этапы, в которых общая задача конкретизируется по направлениям.

Сложный длительный процесс создания СФЗ состоит из нескольких крупных последовательных этапов, которые в свою очередь делятся на серию разделов и операций, выполняемых как последовательно, так и параллельно и образующих сетевую структуру процесса создания СФЗ. Порядок создания СФЗ крупных объектов представлен на рис. 1.4.

Прежде чем излагать конкретные методы проектирования СФЗ, определим некоторые общие понятия, относящиеся к проектированию любых систем независимо от их физической природы и назначения.

Проект – совокупность документов (расчетов, чертежей и др.) для создания какого-либо сооружения или изделия.

Проектирование – процесс создания прообраза предполагаемого объекта в форме технической документации.

Основные процедуры проектирования. Проектирование включает решение задач расчета, анализа, оптимизации и синтеза. Эти задачи называются проектными процедурами и имеют следующее содержание.

Расчет – определение выходных параметров и характеристик системы при неизменных значениях внутренних параметров и постоянной структуре.

Анализ – определение изменения выходных параметров и характеристик системы при изменении внутренних и входных параметров.

Оптимизация – определение наилучших в том или ином смысле выходных параметров и характеристик путем целенаправленного изменения внутренних параметров системы (параметрическая оптимизация) или структуры системы (структурная оптимизация).

Наиболее сложными являются задачи параметрического и структурного синтеза. В проектировании синтезом называют генерацию исходного варианта системы, включая ее структуру (структурный синтез) и значения внутренних параметров (параметрический синтез).

Цель проектирования – в нашем случае, разработка структуры СФЗ с обоснованием выбора технических, инженерных и организационных средств защиты и создание проектно-сметной документации, необходимой для монтажа и эксплуатации СФЗ.

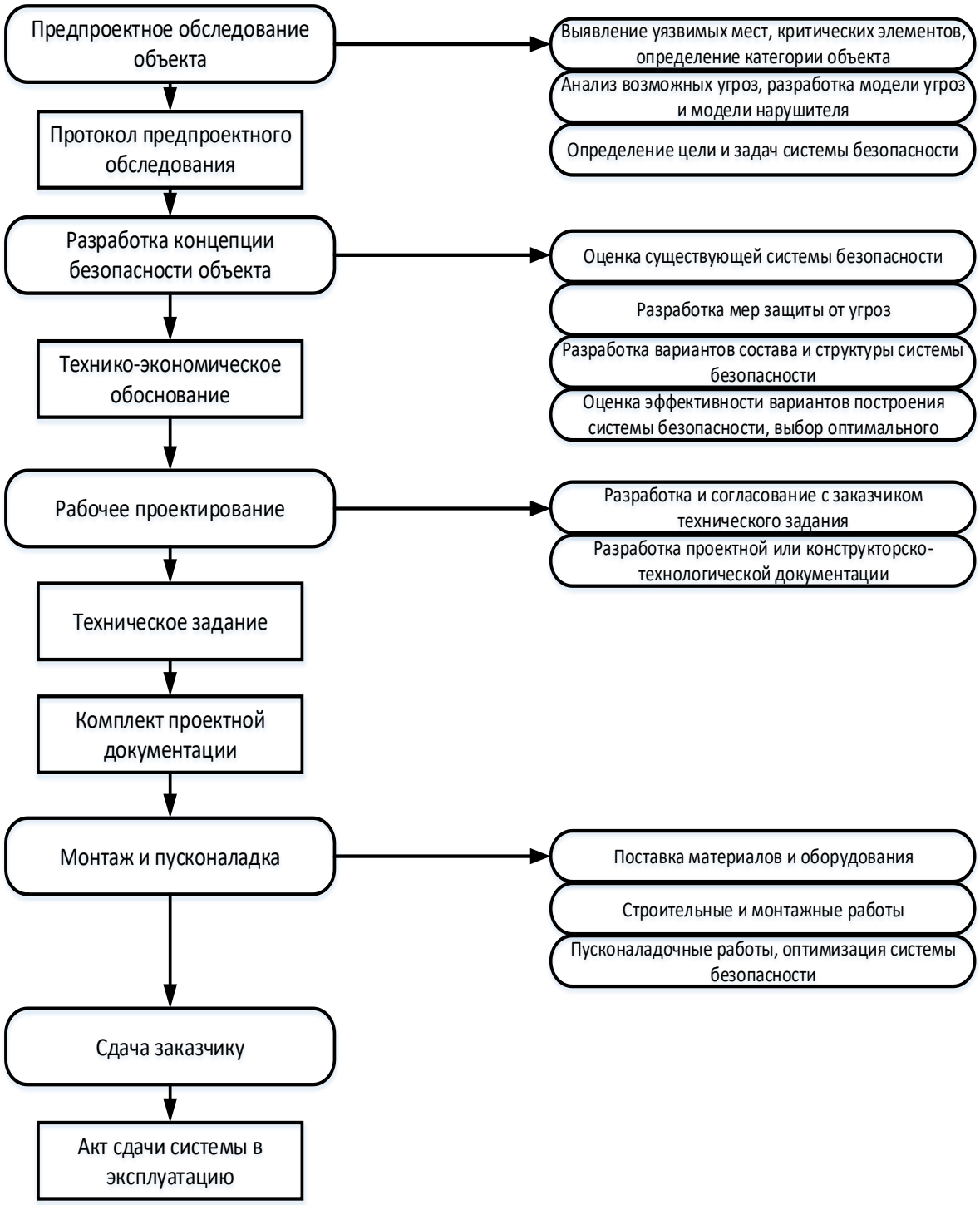


Рис. 1.4. Порядок создания СФЗ крупных объектов

Для достижения цели в процессе проектирования решается комплекс задач:

– анализ вероятных угроз, разработка моделей нарушителей и выбор тактики охраны;

– синтез оптимальной структуры СФЗ;

– определение (расчет) основных параметров СФЗ;

– обоснование выбора технических и инженерных средств охраны;

– разработка организационных структур охраны;
– технико-экономическое обоснование проекта;
– разработка технической документации и рабочих чертежей.

Основная часть перечисленных задач может быть решена только с помощью анализа и синтеза структур СФЗ, параметрической или структурной оптимизацией, проведением процедур расчета. Осуществление перечисленных процедур возможно только путем использования различных моделей СФЗ, особенно на стадии концептуального проектирования.

Непосредственно, проектирование СФЗ состоит из двух стадий:
– концептуального проектирования;
– рабочего проектирования.

Концептуальное проектирование включает этап предпроектного обследования и этап разработки концепции защиты. Рабочее проектирование заканчивается созданием комплекта проектно-сметной документации и рабочих чертежей.

Необходимость стадии концептуального проектирования при создании СФЗ крупных объектов объясняется сложностью и значимостью возлагаемых на СБ задач и возможной невосполнимостью потерь при осуществлении преступных акций. Именно на этапе концептуального проектирования формируется стратегия и тактика защиты объекта, закладывается уровень эффективности защиты. В то же время процедуры концептуального проектирования предполагают использование достаточно сложных методик, насыщенных математическим аппаратом.

1.5. Предпроектное обследование объекта

СФЗ конкретного объекта всегда создается в единственном числе. В силу неповторимости географического положения объекта, индивидуальности взаимного расположения предметов защиты и ЛО невозможно даже для однотипных объектов разработать некий стандартный вариант и тиражировать его в необходимых количествах, обеспечивая одинаковое качество защиты. Индивидуальность объекта предопределяет необходимость проведения изыскательских работ на объектах – предпроектное обследование объекта.

Первый блок вопросов, исследуемых в процессе предпроектного обследования объекта относится к проблемам безопасности:

– определяются и категорируются объекты в целом и ЛО (что защищать);
– анализируются угрозы и разрабатываются модели нарушителей (от кого защищать);
– оцениваются все виды ресурсов (чем защищать);
– формулируются цели и задачи создания СФЗ (сколь эффективно защищать);
– выбираются возможные рубежи защиты (где защищать).

Второй блок вопросов, решаемых во время предпроектного обследования объекта, относится к техническим:

– определяются существующие на объекте виды инженерных средств охраны, их характеристики и состояние;

– оценивается техническое состояние существующего КТСО и характеристики ТСО;

– составляются планы и схемы расположения ЛО, предметов защиты, существующих ИСО и ТСО, места ввода на объекты инженерных коммуникаций;

– выявляются зоны повышенного риска, делается их описание;

– анализируется существующая структура построения сил охраны на объекте и тактические характеристики сил охраны;

– комплектуется необходимая для проектирования документация.

Первый блок вопросов позволяет в дальнейшем сформулировать стратегию и тактику защиты, а также требуемые выходные характеристики СФЗ, а второй блок – определить внутренние и входные параметры СФЗ, а также направления разработки и технической модернизации ИСО и КТСО.

Результаты работы на данном этапе оформляются совместно с заказчиком специальным типовым протоколам обследования.

Основанием для проведения таких работ является договор с заказчиком, в котором формируются общие проблемы обеспечения безопасности на объекте.

Изложенный материал отражает общий укрупненный подход к предпроектному обследованию объектов. При проектировании СБО для наиболее характерных объектов, охраняемых подразделениями вневедомственной охраны, где самой распространенной является угроза кражи, как правило, ориентируются на типовой набор видов охранных систем, которые отработаны многолетним опытом их разработки. В этом случае разрабатывается не концепция защиты объекта, а предложения по организации охраны. Главным управлением вневедомственной охраны разработаны подробные рекомендации по проведению предпроектного обследования. Ниже предлагается типовой порядок обследования, в котором использованы некоторые положения. Этот порядок может быть использован при обследовании объектов любого вида.

Порядок предпроектного обследования объектов.

Предпроектное обследование объекта предусматривает изучение на месте характеристик объекта, определяющих его устойчивость на момент обследования к преступным посягательствам.

Целью предпроектного обследования является:

– определение категории объекта и наиболее характерных угроз;

– выявление уязвимых мест на объекте;

– оценка эффективности существующей системы охраны объекта;

– разработка согласованных с «собственником» предложений по организации охраны объекта, обеспечивающих необходимый уровень безопасности.

Основанием для проведения обследования объекта является обращение «собственника» в проектную организацию с просьбой о разработке СФЗ. Обследование проводится межведомственной комиссией в составе представителей проектной организации, Государственной пожарной службы (ГПС) МЧС России, заказчика и, если необходимо, представителей органов местного самоуправления и правоохранительных органов или вневедомственной охраны.

Проведение обследования рекомендуется проводить в последовательности, изложенной ниже.

Определение категории объекта и характерных угроз:

– наименование объекта;

– ведомственная принадлежность;

– производственное или другое назначение;

– местоположение объекта и оценка местности, непосредственно прилегающей к нему;

– наиболее вероятные пути проникновения на объект;

– оценка степени тяжести возможного ущерба (включая угрозу здоровью и жизни людей) от несанкционированного проникновения на объект;

– изучение криминогенной обстановки в районе;

– описание возможных угроз;

– присвоение объекту категории, включая категории, присвоенные отдельным его зонам.

Ознакомление с план-схемой и строительными чертежами объекта:

– расположение на местности;

– занимаемая площадь;

– конфигурация периметра: общая протяженность и протяженность линейных участков (участков прямой видимости);

– количество строений: административных зданий, отдельно стоящих складских помещений, вспомогательных и других строений и т.п., их этажность, наличие чердачных и подвальных помещений, размеры по периметру;

– режимы работы объекта, наличие ограничения доступа в отдельные здания или помещения.

Проверка инженерных сооружений периметра объекта:

– вид и состояние внешнего ограждения;

– выявление уязвимых мест;

– наличие и состояние полосы отчуждения;

– работоспособность технических средств, установленных по периметру;

– наличие обеспечивающих и вспомогательных средств освещения, линий связи, электроснабжения и т.д.

Проверка территории:

– количество, размеры, состояние и расположение открытых площадок для хранения ценностей: автостоянок, мест складирования товаров (в том числе – под навесами) и т.п;

– расположение зданий, сооружений, инженерных коммуникаций.

Проверка состояния охраны:

– структура имеющейся на объекте охраны: милицейская, военизированная, сторожевая и т.п.;

– укомплектованность штата охраны;

– соответствие дислокации постов местам хранения ценностей;

– состояние и количество контрольно-проходных и контрольно-проездных пунктов (КПП);

– техническая оснащенность КПП: наличие автоматизированных устройств контроля прохода, систем и средств управления доступом, средств связи и т.п.;

– количество и состояние запасных автотранспортных и железнодорожных ворот.

Проверка зданий и помещений:

– техническое состояние крыш и техническая укрепленность всех коммуникаций, выходящих на крыши;

– деление помещений на группы в соответствии с их назначением, стоимостью и количеством предметов преступных посягательств (денежных средств и ценностей, оружия и боеприпасов, ядовитых, наркотических и радиоактивных веществ и т.п.);

– количество отапливаемых и неотапливаемых помещений, их геометрические размеры (длина и ширина, высота потолка);

– количество и характеристики (размеры, материал и т.п.) элементов строительных конструкций (окон, дверей, люков, некапитальных стен, перекрытий и т.п.), их техническая укрепленность (наличие металлических решеток, запорных и замковых устройств и т.п.);

– характеристики размещения предметов преступных посягательств;

– количество уязвимых мест и вероятные способы проникновения через них (открывание, взлом или пролом, другие способы);

– количество телефонных линий, категория энергоснабжения.

Для типовых объектов, где основным видом угроз являются кражи ценных предметов и имущества (офисы, склады, объекты административного и производственного назначения), по результатам обследования разрабатываются предварительные предложения по организации (усилению) охраны, которые содержат:

– объем и характер режимных мероприятий: порядок вывоза и выноса имущества, ограничения в передвижении по охраняемой территории, установление запретных зон на подступах к охраняемому объекту;

– рекомендуемые виды охраны: централизованная, военизированная, сторожевая, с использованием служебных собак – и ее структура: по периметру, по отдельным частям объекта, смешанная;

– состав служебной документации, которая должна находиться в караульном помещении, комнате полиции или на посту охраны объекта;

– необходимое количество постов и маршрутов, их дислокация, требуемое количество личного состава охраны по должностям;

– рекомендации по оборудованию объекта комплексом технических средств охраны и устройству заграждений, наружного освещения объекта и подступов к нему, организации телефонной и иной связи.

Предложения должны разрабатываться на основе сформированных типовых решений, обеспечивающих достаточную безопасность объекта по доступной цене. При этом отражаются следующие вопросы:

– необходимость проведения монтажных работ на объекте;

– предлагаемый комиссией принцип организации охраны объекта: по периметру, по отдельным частям объекта, с применением средств видеоконтроля и управления доступом;

– порядок защиты окон, дверей, люков, воздуховодов техническими средствами;

– блокировка технических конструкций: наименование материалов, из которых они изготовлены, размеры, количество;

– структура комплекса охранной сигнализации: количество рубежей защиты, автономная или централизованная, резервирование электропитания;

– необходимость применения средств усиления охраны: систем видеоконтроля и управления доступом;

– состав, количество и размещение оборудования;

– протяженность, тип прокладки проводов и кабелей, их защита;

– ориентировочная стоимость оборудования объекта;

– надежность охраны.

Для крупных важных и особо важных объектов по результатам обследования объекта разрабатывается концепция защиты объекта с обоснованием выбранной структуры СФЗ, стратегии и тактики защиты.

Вопросы для самостоятельной работы

1. Назначение категорирования объектов.
2. Категорирование объектов.
3. Категорирование квартир.
4. Категорирование МХИГ.
5. Основания для классификации угроз охраняемому объекту.
6. Понятие системы охранной безопасности.
7. Понятие угрозы безопасности.
8. Модель угроз безопасности объекта.
9. Модель нарушителя.
10. Основные виды угроз.
11. В чем заключается сущность концепции обеспечения комплексной безопасности объектов?
12. Перечислите и охарактеризуйте основные процедуры проектирования.
13. Перечислите и охарактеризуйте основные этапы предпроектного обследования объектов.

ТЕМА 2
СИСТЕМЫ ОХРАННО-ТРЕВОЖНОЙ И ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Учебные и воспитательные цели:

Образовательные: изучить основные требования к системам охранной, тревожной и пожарной сигнализации.

Развивающие: расширить базовые знания обучающихся в области особенностей построения систем охранной, тревожной и пожарной сигнализации; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

2.1. Назначение и особенности построения систем охранной, тревожной и пожарной сигнализации.

2.2. Основные требования к системам охранной, тревожной и пожарной сигнализации.

2.3. Особенности монтажа и электрических соединений технических средств систем охранной, тревожной и пожарной сигнализации.

2.4. Классификация банковских устройств самообслуживания.

2.5. Проектирование системы видеонаблюдения для охраны банковских устройств самообслуживания.

2.6. Особенности применения специализированных средств охраны банковских устройств самообслуживания.

2.1. Назначение и особенности построения систем охранной, тревожной и пожарной сигнализации

Изучение принципов построения и функционирования систем охранной, пожарной и тревожной сигнализации начнем с определений компонентов, входящих в их состав.

Система охранной сигнализации (СОС) – совокупность совместно действующих технических средств охраны (безопасности), предназначенных для обнаружения криминальных угроз, сбора, обработки, передачи и представления в заданном виде информации о состоянии охраняемого объекта или имущества.

Система тревожной сигнализации (СТС) – электрическая установка, предназначенная для обнаружения опасности и сигнализации о ее наличии.

Охранный извещатель (ИО) – техническое средство охранной сигнализации, предназначенное для формирования тревожного извещения автоматическим или ручным способом при обнаружении проникновения (попытки проникновения) на охраняемый объект или других противоправных воздействий.

Адресный извещатель – извещатель, формирующий адресные извещения в виде электронного цифрового кода, содержащие информацию о состоянии извещателя и позволяющие однозначно идентифицировать его в составе системы охранной (охранно-пожарной, тревожной) сигнализации.

Средства электропитания – технические средства, обеспечивающие бесперебойное электропитание технических средств охраны и модулей, входящих в систему централизованного наблюдения.

Оповещатель – техническое средство охранной, пожарной или охранно-пожарной сигнализации, предназначенное для оповещения людей на удалении от охраняемого объекта о проникновении или попытке проникновения и/или пожаре.

Устройство оконечное объектовое (УОО) – составная часть системы передачи извещений, устанавливаемая на охраняемом объекте для приема извещений от извещателей, приборов приемно-контрольных (ППК) и других ТСОС, установленных на охраняемом объекте, преобразования и передачи извещений по каналам связи на систему передачи извещений, ретранслятор или пульт централизованного наблюдения, а также (при наличии обратного канала связи) для приема от ретранслятора или пульта централизованного наблюдения команд телеуправления.

Шифроустройство (ШУ) – составная часть системы охранной или охранно-пожарной сигнализации, обеспечивающая управление состоянием извещателя или прибора приемно-контрольного ответственными лицами, обладающими кодом управления, для их входа на охраняемый объект и выхода с объекта без выдачи извещения о тревоге.

Автоматизированное рабочее место (АРМ) – персональное рабочее место, обеспечивающее автоматизацию взаимодействия сотрудника пункта централизованной охраны (мониторингового центра) с СЦН.

Обобщенная структурная схема системы ОПС приведена на рис. 2.1.

На схеме обозначены:

ИО – извещатель охранный (тревожный);

ИП – извещатель пожарный;

ИУ – исполнительное устройство (световой, звуковой оповещатель и т.д.);

БП – блок питания (резервированный источник бесперебойного питания постоянного тока или сеть переменного тока);

ПКП – приемно-контрольный прибор;

ШУ – шифроустройство (или считыватель ключей/карт для постановки/снятия шлейфов на охрану / с охраны);

УОО СПИ – устройство оконечное объектовое системы передачи извещений, стоящей на вооружении конкретного подразделения охраны;

АРМ СПИ – автоматизированное рабочее место (ПЭВМ с установленным программным обеспечением, поддерживающим СПИ).

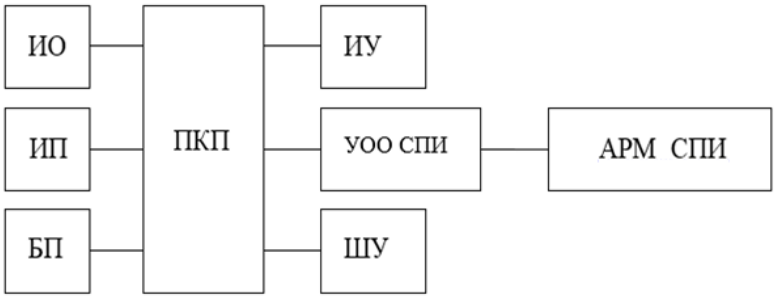


Рис. 2.1. Структурная схема системы ОПС

Классификация извещателей.

Для обнаружения нарушителя или пожара на объекте используются извещатели (средства обнаружения).

Магнитоконтактный извещатель предназначен для блокировки окон, дверей, люков и т.п. на открывание. Серия извещателей ИО 102.

Пьезоэлектрический вибрационный извещатель предназначен для обнаружения разрушения строительных конструкций, а также сейфов, металлических шкафов и банкоматов. Извещатели «Шорох».

Акустический извещатель предназначен для обнаружения разбития стекол различных марок. Извещатели «Астра-С», «Стекло», «Арфа».

Пассивный инфракрасный извещатель предназначен для обнаружения движения нарушителя (как источника теплового/инфракрасного излучения) в объеме помещения. Извещатели «Фотон», «Пирон», «Икар», «Астра».

Радиоволновый извещатель предназначен для обнаружения движения нарушителя в объеме помещения при регистрации изменения частоты излучаемых *радиоволн*, отраженных от движущегося объекта (эффект Доплера). Извещатели «Аргус», «Волна».

Ультразвуковой извещатель предназначен для обнаружения движения нарушителя в объеме помещения при регистрации изменения частоты излучаемых *ультразвуковых волн*, отраженных от движущегося объекта (эффект Доплера). Извещатели «Эхо», «Витрина».

Активный инфракрасный извещатель предназначен для обнаружения пересечения нарушителем инфракрасного луча между излучателем и приемником. Извещатели «СПЭК».

Периметральный радиоволновый извещатель предназначен для обнаружения пересечения нарушителем электромагнитного поля в виде эллипсоида вращения между излучателем и приемником. Извещатели «Радий», «Линар».

Радиоволновый извещатель для блокировки открытых площадок предназначен для обнаружения движения нарушителя в зоне подходов к объектам и др. Извещатель «Фон».

Средства тревожной сигнализации предназначены для подачи сигнала тревоги реагирующим силам в случае нападения (угрозы кражи, жизни и здоровью людей). Извещатели: тревожные кнопки и тревожные педали.

Извещатель-ловушка – охранный извещатель, скрытно устанавливаемый внутри охраняемого объекта на наиболее вероятном направлении перемещения нарушителя, блокирующий или имитирующий какой-либо предмет, наиболее подверженный криминальной угрозе. Извещатели «Кукла-Л», «Радиокукла», «Миникредит-Л», «Браслет-Л», «Клипса».

Пожарные извещатели дымовые, тепловые, пламени. Предназначены для обнаружения очагов возгорания и пожаров на объектах.

Пожарные извещатели ручные. Предназначены для подачи сигнала о пожаре реагирующим силам. Извещатели: ИР, ИПР.

Классификация приемно-контрольных приборов, оповещателей и источников питания.

В основу выбора способов построения комплекса ОПС на объекте положен принцип разбиения охраняемого объекта на зоны защиты или охраняемые зоны (принцип многорубежности), в соответствии с которым материальные ценности защищаются несколькими по возможности не зависящими друг от друга рубежами охраны.

Зона охраны – часть охраняемого объекта, оборудованная техническими средствами охраны, для которой установлен отдельный режим. Другими словами, это часть охраняемого объекта, контролируемая одним проводным шлейфом сигнализации (радиальным) или одним адресным извещателем.

Носителями опасности для охраняемого объекта являются люди и предметы, реально существующие во времени и пространстве, которые могут перемещаться и производить определенные действия как вне, так и внутри объекта.

Для повышения надежности защиты объекта от угроз его территория разбивается на зоны защиты, границами которых, как правило, служат искусственные или естественные ограждения, а также строительные конструкции.

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

При преодолении элементов инженерно-технической укрепленности (ИТУ) или перемещении по охраняемой зоне выдается соответствующее извещение на выносные оповещатели или службу реагирования. Охраняемые зоны должны быть расположены таким образом, чтобы при подходе к местам размещения ценностей с любой стороны было зафиксировано нарушение не менее чем одним рубежом сигнализации.

В качестве самостоятельного рубежа сигнализации может использоваться система тревожной сигнализации (тревожные кнопки, педали). При наличии на объекте нескольких рубежей охранной сигнализации в каждом рубеже используются технические средства ОС, основанные на различных принципах обнаружения нарушителя. Совокупность двух и более рубежей охранной сигнализации образует многорубежный комплекс охранной сигнализации.

Многорубежный комплекс охранной сигнализации – совокупность двух или более рубежей охранной сигнализации, на которых применяются технические средства охранной сигнализации, основанные на различных физических принципах действия.

В многорубежной системе сигнализации по сравнению с однорубежной системой возрастают:

– живучесть системы;

– вероятность обнаружения нарушителя;

– достоверность получаемого извещения, которое подтверждается несколькими независимыми рубежами сигнализации;

– информативность извещений на ПЦО.

Условное изображение многорубежной системы охраны приведено на рис. 2.2.

Живучестью комплекса ОПС называется способность комплекса выполнять свою основную функцию при выходе (выводе) из строя отдельных технических средств охраны из-за воздействия на них неблагоприятных факторов.

Построение первого рубежа охраны.

Первым рубежом сигнализации называется рубеж, отделяющий охраняемый объект от внешней (неконтролируемой) среды. Особенностью 1-го рубежа охраны является большой удельный вес средств инженерно-технической укрепленности (ИТУ). Инженерно-техническая укрепленность 1-го рубежа охраны должна быть достаточна для обеспечения защиты:

– помещений от проникновения нарушителя на время, необходимое для выявления и пресечения нарушения;

– хранимых материальных ценностей от скоротечных хищений с использованием квалифицированных методов взлома;

– персонала и посетителей объектов от вооруженных нападений.

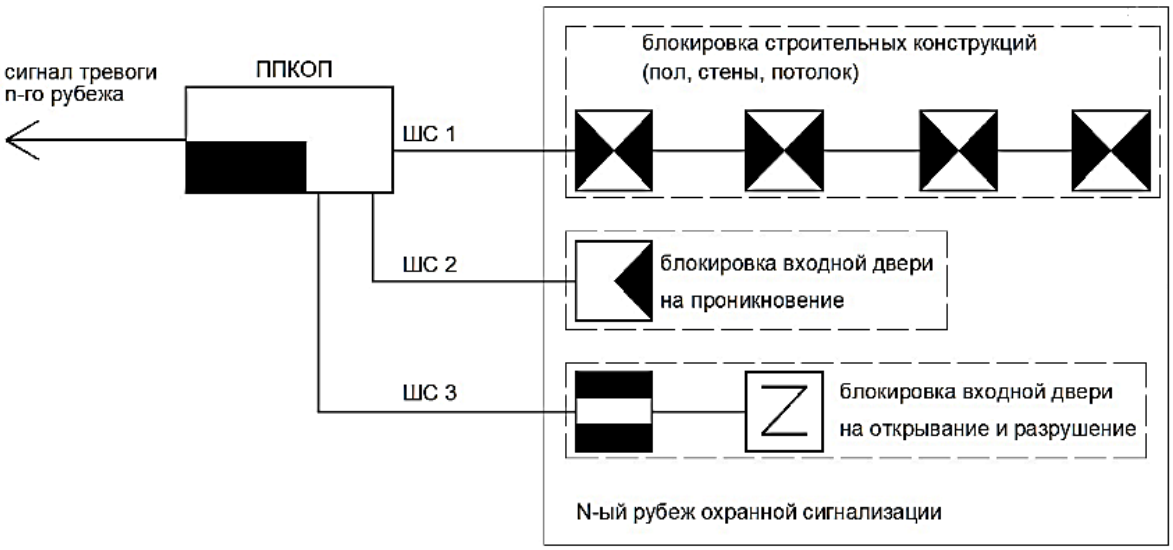


Рис. 2.2. Многорубежный комплекс охранной сигнализации

Наилучшие результаты защиты объектов достигаются при рациональном сочетании инженерно-технической укрепленности строительных конструкций и технических средств ОПС.

В основу построения КТС ОПС объекта положены упреждающие мероприятия по противодействию предполагаемым способам посягательств на ценности, находящиеся на объекте. В многорубежном КТС ОПС обнаружение попытки проникновения нарушителя на объект должно происходить на самой ранней стадии проникновения (на дальних подступах к ценностям). Поэтому первый рубеж охраны, как правило, блокирует удаленные от ценностей области объекта.

Для повышения вероятности пресечения кражи необходимо:

– увеличивать время, которое требуется нарушителю для преодоления защитных конструкций объекта;

– обнаруживать нарушителя на начальной стадии его проникновения на объект;

– уменьшать время прибытия ГЗ на объект.

Оборудование объекта как элементами инженерно-технической укрепленности, так и средствами ОС следует начинать с уязвимых мест объекта.

Уязвимым местом (при охране) называется часть, элемент, фрагмент периметра объекта, здания, помещения, через который наиболее вероятна попытка проникновения. Первый рубеж сигнализации блокирует (за-

щищает) уязвимые места внешних строительных конструкций объекта с целью выявления проникновения в охраняемое помещение извне.

К уязвимым местам, контролируемым первым рубежом, относятся:

– оконные и дверные проемы по периметру зданий или помещений объекта;

– вентиляционные каналы;

– выходы к пожарным лестницам, люки;

– места ввода коммуникаций, близлежащие распределительные устройства электропитания средств ОПС и места подключения средств ОПС к линиям связи;

– некапитальные и капитальные (если необходима их защита) стены;

– крыши зданий и чердачные помещения.

Уязвимые места первого рубежа могут блокироваться извещателями различных типов, способными обнаружить:

– открывание окон, форточек, дверей, люков, выходов к пожарным лестницам, щитов электропитания, телефонных боксов. Открывание строительных конструкций обнаруживается с помощью магнитоконтактных извещателей, пассивных и активных инфракрасных извещателей, концевых выключателей. Приближение к окнам и дверям обнаруживается емкостными извещателями;

– разрушение стен, перегородок, перекрытий, крыш, дверей, остекленных проемов. Разрушение строительных деталей обнаруживается электроконтактными, ударноконтактными, вибрационными и акустическими извещателями.

Построение второго рубежа охраны.

Технические средства ОПС обладают конечной вероятностью обнаружения и могут быть преодолены подготовленным нарушителем. Кроме того, в ряде случаев движение нарушителя к ценностям может начаться внутри объекта, без преодоления внешних барьеров. Обнаружение движения нарушителя внутри защищаемых помещений осуществляется вторым рубежом охраны. Особенностью второго рубежа является меньший удельный вес элементов ИТУ по сравнению с первым рубежом и необходимость контроля значительных объемов помещений. К уязвимым местам, контролируемым вторым рубежом, относятся:

– внутренние объемы помещений;

– подходы к местам сосредоточенного хранения ценностей;

– устройства ОПС внутри помещений, доступные нарушителю для несанкционированного воздействия с целью вывода их из строя;

– проходы между помещениями (устанавливаются ловушки).

Уязвимые места второго рубежа могут блокироваться извещателями различных типов, однако наиболее распространенными являются доплеровские (ультразвуковые и радиоволновые), инфракрасные активные, инфракрасные пассивные и комбинированные.

Построение третьего рубежа охраны.

Третий рубеж охранной сигнализации контролирует места хранения ценностей (стеллажи, полки, металлические шкафы, сейфы) и непосредственно сами ценности (картины и другие культурные ценности). Уязвимыми местами третьего рубежа являются:

– охраняемые предметы при их открытом хранении (оргтехника, музейные экспонаты и т.д.);

– сейфы, металлические шкафы, ящики, в которых хранятся ценности. Уязвимые места третьего рубежа могут блокироваться извещателями различных типов, однако наиболее распространенными являются емкостные, оптико-электронные пассивные, магнитоконтактные (для создания ловушек).

2.2. Основные требования к системам охранной, тревожной и пожарной сигнализации

Подсистемы сигнализации (СОТС, СПС) могут быть централизованными и/или автономными в зависимости от конкретных условий и особенностей процессов деятельности на объекте.

Централизованная подсистема сигнализации должна обеспечивать технический контроль состояния территориально рассредоточенных контрольных зон объекта и передачу полученной информации в ДДП объекта за время, необходимое для решения задач по обеспечению безопасности.

Автономные подсистемы сигнализации должны обеспечивать технический контроль состояния одной или нескольких локально объединенных контрольных зон и светозвуковое отображение полученной информации для восприятия ее персоналом и другими людьми, санкционированно находящимися на объекте.

Функциональное назначение, целевые свойства, режимы работы, состав и техническое построение подсистем сигнализации на объекте определяются видами угроз, информацию о которых они должны регистрировать и передавать (аварийно-технологическая, охранная, пожарная, тревожная, комбинированная).

2.3. Особенности монтажа и электрических соединений технических средств систем охранной, тревожной и пожарной сигнализации

При проведении электромонтажных работ по подключению технических средств охраны необходимо использовать следующие общие рекомендации:

1. Следует руководствоваться правилами техники безопасности при работе с электроустановками и соблюдать все меры предосторожности.

2. Для электропроводок систем безопасности следует применять провода и кабели только с медными жилами.

3. Диаметры медных жил проводов и кабелей должны быть определены из соответствующих расчетов, но не менее 0,5 мм (для многожильных проводов – не менее 0,2 мм).

4. Не допускается прокладка шлейфов и линий связи совместно с линиями напряжением 110 В и выше в одном коробе, трубе, жгуте, замкнутом канале строительной конструкции, или на одном лотке. Совместная прокладка указанных линий допускается в разных отсеках коробов и лотков, имеющих сплошные продольные перегородки с пределом огнестойкости 0,25 ч из негорючего материала.

5. Близко расположенные источники электрических помех могут вызывать сбои в работе системы, поэтому нельзя устанавливать оборудование на расстоянии менее 1 м от электрогенераторов, электродвигателей, реле переменного тока, тиристорных регуляторов света и других источников электрических помех.

6. При прокладке все сигнальные кабели, датчики, исполнительные устройства и кабели низковольтного питания должны быть размещены на расстоянии не менее 0,5 м от силовых кабелей переменного тока, кабелей управления мощными моторами, насосами, приводами и т. д. Пересечение всех сигнальных кабелей с силовыми кабелями допускается только под прямым углом.

7. При пересечении силовых и осветительных сетей кабели и провода сигнализации должны быть защищены резиновыми или полихлорвиниловыми трубками, концы которых должны выступать на 4-5 мм с каждой стороны перехода. При пересечении кабели большей емкости должны прилегать к стене, а меньшей емкости огибать их сверху. Кабели меньшей емкости допускается пропускать под кабелями большей емкости при прокладке их в штробах.

8. Прокладка проводов и кабелей по стенам внутри охраняемых зданий должна производиться 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.

9. Электропроводки, проходящие по наружным стенам на высоте менее 2,5 м или через помещения, которые не подлежали защите, должны быть выполнены скрытым способом или в металлических трубах.

10. В местах поворота под углом 90° (или близких к нему) радиус изгиба прокладываемых кабелей должен быть не менее семи диаметров кабеля.

11. Линии электропитания приборов приемно-контрольных и приборов пожарных управления, а также соединительные линии управления автоматическими установками пожаротушения, дымоудаления или оповещения следует выполнять самостоятельными проводами и кабелями. Не допускается их прокладка транзитом через взрывоопасные и пожароопасные помещения (зоны). В обоснованных случаях допускается

прокладка этих линий через пожароопасные помещения (зоны) в пустотах строительных конструкций класса К0 или пожаростойкими проводами и кабелями.

Шлейф сигнализации (ШС) – электрическая цепь, соединяющая выходные цепи охранных извещателей, включающая в себя вспомогательные (выносные) элементы (диоды, резисторы и другое) и соединительные провода и предназначенная для передачи на прибор приемно-контрольный извещений о проникновении (попытке проникновения) и неисправности, а в некоторых случаях – для подачи электропитания на извещатели. Перед построением ШС необходимо знать, какой ПКП будет использоваться для организации объектового комплекса ОПС, чтобы знать номинальное значение оконечного радиоэлемента (сопротивление, емкость) шлейфа сигнализации, по которому ПКП определяет его состояние. Нормально-замкнутые извещатели подключаются в электрическую цепь ШС последовательно, а нормально-разомкнутые – параллельно. Это следует из основ теории электрических цепей путем отслеживания движения электрического тока по проводнику. Электрический ток, проходящий по шлейфу сигнализации, обязательно должен протекать через оконечное сопротивление с номиналом $R_{ок}$, характерное для конкретного ППКОП, тогда «шлейф в норме» (дежурный режим), если же ток не протекает через оконечное сопротивление, тогда «шлейф в тревоге» (режим тревоги). Тревожное состояние шлейфа сигнализации может быть вызвано срабатыванием датчика извещателя и формированием извещения о тревоге путем размыкания выходных контактов реле (для нормально-замкнутых) или замыкания (для нормально-разомкнутых), либо изменением значения тока в цепи (для извещателей типа «открытый коллектор»), либо умышленным воздействием на шлейф со стороны злоумышленника: обрыв соединительных проводов, установка перемычек – КЗ («обход шлейфа»).

Клеммные колодки нормально-замкнутых извещателей, как правило, выглядят следующим образом (рис. 2.3):

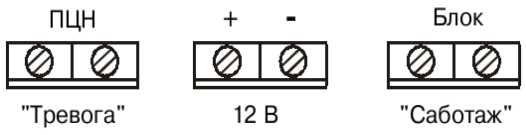


Рис. 2.3. Клеммная колодка нормально-замкнутого извещателя «Фотон-Ш»

Клеммные колодки нормально-разомкнутых извещателей и извещателей типа «открытый коллектор», как правило, выглядят следующим образом (рис. 2.4):

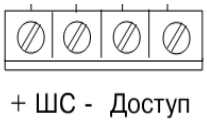
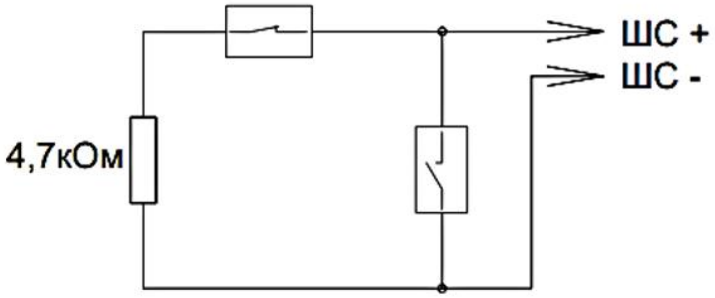


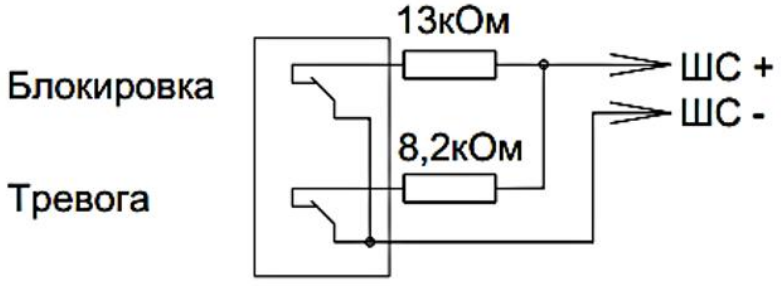
Рис. 2.4. Клеммная колодка нормально-разомкнутого извещателя «Фотон-12-1»

Единственное конструктивное и внешнее отличие заключается в отсутствии у нормально-разомкнутых извещателей клемм электропитания, так как их электропитание осуществляется по шлейфу сигнализации, а не от отдельного источника. Клеммы «Доступ», «Саботаж», «Тампер» предназначены для подключения тамперных контактов извещателей к ПКП для передачи тревожных извещений о вскрытии корпуса извещателей. На практике данные контакты часто не используются по назначению, а используются в качестве дополнительных свободных клемм при осуществлении монтажа электропроводок.

Общие правила подключения охранных и тревожных извещателей в шлейф сигнализации отображены на рис. 2.5, 2.6 на примере подключения к прибору приемно-контрольному охранно-пожарному «Сигнал-20».

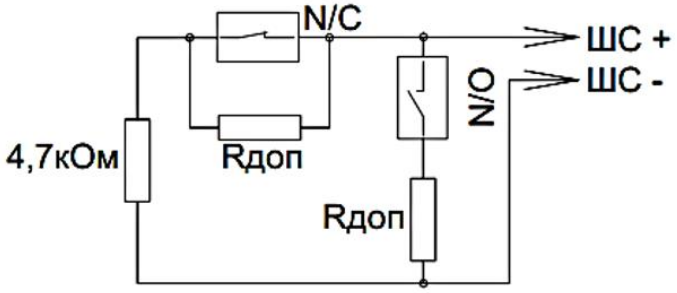


Включение нормально-замкнутых и нормально-разомкнутых охранных извещателей в ШС типа 4 ("Охранный"), 7 ("Охранный входной") и 11 ("Тревожный")



Включение охранных извещателей с блокировочными контактами в ШС типа 5 ("Охранный с контролем блокировки")

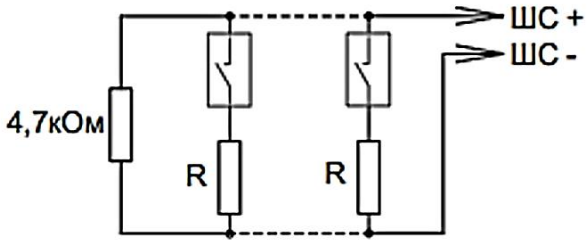
Рис. 2.5. Правила подключения охранных и тревожных извещателей в шлейф сигнализации



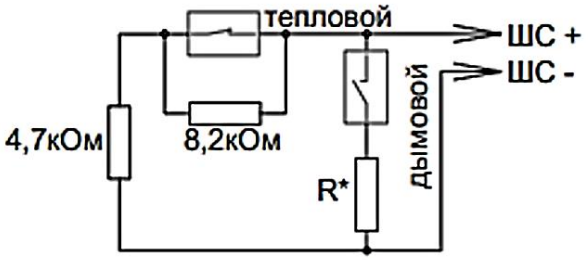
Включение нормально-разомкнутых и нормально-замкнутых датчиков в ШС типа 12 ("Пожарный программируемый")
Rдоп - дополнительный резистор.

Рис. 2.6. Правила подключения охранных и тревожных извещателей в шлейф сигнализации

Общие правила подключения пожарных извещателей в шлейф сигнализации отображены на рис. 2.7, 2.8 на примере подключения к ППКОП «Сигнал-20», ППКОП «Сигнал-10».



Включение нормально-разомкнутых ("дымовых") пожарных извещателей в ШС типа 1 ("Пожарный дымовой с распознаванием двойной сработки").
R = 1,5 кОм±5% для ДИП-3СУ, ДИП-У (напряжение на сработавшем извещателе от 7,5 до 8,5 В)
R = 2,2 кОм±5% для 2100, 2151Е (напряжения на сработавшем извещателе от 4 до 5 В)
R = 2,4 кОм±5% для ИП-101А (напряжения на сработавшем извещателе от 3,5 до 4 В)
R = 3 кОм±5% для извещателей с выходной цепью типа "сухой контакт"



Включение нормально-разомкнутых ("дымовых") и нормально-замкнутых ("тепловых") пожарных извещателей в ШС типа 2 ("Пожарный комбинированный")
R* = 0 для ДИП-3М, ДИП-3СУ, ДИП-У, 2100, 2151Е (напряжение на сработавшем извещателе > 4 В)
R* = 510 Ом для ИП-101А, ИПР513-3 и извещателей с выходной цепью типа "сухой контакт" (напряжение на сработавшем извещателе < 4 В)

Рис. 2.7. Правила подключения пожарных извещателей в ШС

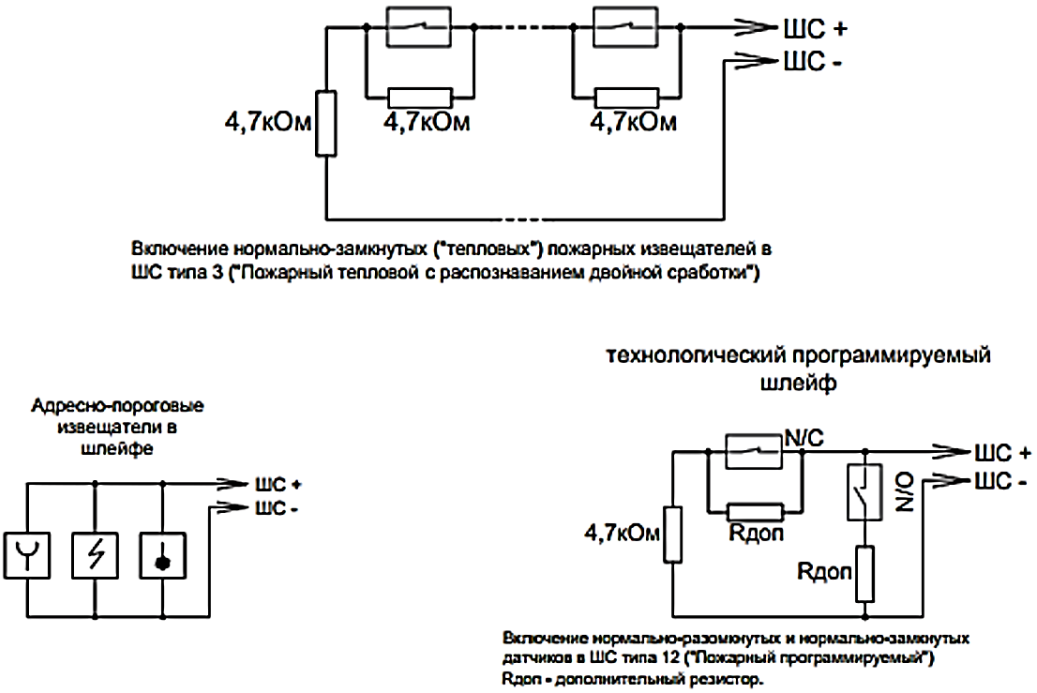


Рис. 2.8. Правила подключения пожарных извещателей в ШС

Приведем примеры схем подключения в шлейф охранных извещателей (рис. 2.9).

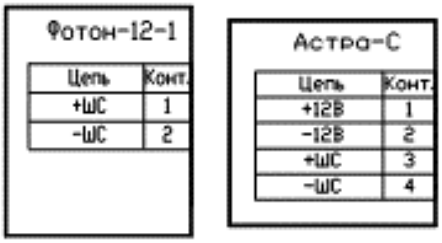


Рис. 2.9. Извещатели охранные нормально-разомкнутые и нормально-замкнутые

Что касается пожарных извещателей, то существуют также и нормально-замкнутые (тепловые) и нормально-разомкнутые (дымовые). Как правило, большинство пожарных извещателей являются токопотребляющими по шлейфу сигнализации. Приведем примеры схем подключения в шлейф дымовых пожарных извещателей (рис. 2.10, 2.11).

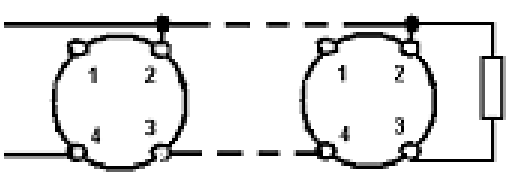


Рис. 2.10. Извещатели пожарные типа ИП 212-46 и их аналоги

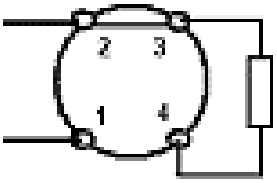


Рис. 2.11. Извещатели пожарные типа «Пульсар»

При подключении в один ШС токопотребляющих извещателей охранных или пожарных их количество ограничено и рассчитывается исходя из суммарного тока потребления, который не должен превышать выходной ток или ток нагрузки в шлейфе ППКОП – $I_{вых}$ (мА).

Оконечный элемент, как правило, резистор, подключается к шлейфу сигнализации таким способом, чтобы к нему был затруднен доступ посторонних лиц, для исключения «обхода» сигнализации, например, оконечный элемент-резистор устанавливается в корпусе одного из извещателей (зачастую в последнем извещателе шлейфа).

2.4. Классификация банковских устройств самообслуживания

Проблема обеспечения безопасности учреждений кредитно-финансовой системы является одной из самых актуальных. Экономические преобразования в России привели к необходимости по-новому подойти к данной проблеме. Это связано с существенным увеличением количества кредитных организаций (коммерческих банков), различных по размерам активов, степени развития сети филиалов и других структурных подразделений, сети банковских устройств самообслуживания (банкоматов, платежных терминалов).

Соответственно, на фоне общей криминальной ситуации в России. возрос интерес преступных элементов к банкам и банковской деятельности, что потребовало принятия новых эффективных мер по обеспечению защиты денежных средств в учреждениях кредитно-финансовой системы, защиты коммерческой тайны и свободы коммерческой деятельности.

В соответствии с этим одним из важнейших направлений деятельности подразделений вневедомственной охраны является охрана объектов кредитно- финансовой системы.

Учитывая актуальность проблемы, ГУВО Росгвардии определен комплекс организационно-практических мероприятий, направленных на предупреждение и пресечение противоправных посягательств на объекты и имущество учреждений кредитно-финансовой системы, надежную защиту клиентов, персонала, охрану денежных средств и других ценностей. Эффективность указанных мероприятий во многом определяется уровнем научно-технического оснащения службы вневедомственной охраны.

На территории Российской Федерации кредитными организациями и платежными агентами в основном используются банкоматы и платежные (информационно-транзакционные) терминалы, которые отличаются конструктивными и дизайнерскими решениями, способами установки и крепления к строительным или специальным конструкциям, областью применения (размещения), максимальным объемом загружаемых и принимаемых наличных денежных средств, функциональными возможностями и уровнем механической защиты нижнего кабинета (сейфа).

Организация противокриминальной защиты банкоматов, платежных терминалов и иных устройств самообслуживания – это комплексная задача, включающая в себя защиту с помощью средств инженерно-технической укрепленности, охранной сигнализации, СКУД, систем охранных телевизионных и других средств защиты.

Независимо от типа банкомата у устройства самообслуживания выделяют две зоны:

– зону самообслуживания (специально выделенное помещение для доступа клиентов к устройству самообслуживания либо территория непосредственно перед банкоматом);

– сервисную зону (помещение, где осуществляется загрузка / выгрузка кассет с денежной наличностью кассовыми работниками / инкассаторами, а также, техническое обслуживание данных устройств). Сервисной зоной банкомата является как специально выделенное внутреннее помещение, так и используемое для этих целей существующее служебное помещение.

Банковские устройства самообслуживания (БУС) классифицируются по 4 признакам.

1. Классификация БУС по конструкции, области применения и способу установки.

В зависимости от конструкции и области применения БУС подразделяются на две основные категории:

– предназначенные для отдельной (обособленной – «О») установки внутри или снаружи помещений;

– предназначенные для монтажа в специальном проеме капитальной строительной конструкции (стене – «С») помещения.

При этом в зависимости от способа установки, особенностей эксплуатации и обслуживания, в каждой категории можно выделить по три группы БУС.

2. Классификация БУС по материальной ценности.

В зависимости от максимального объема загружаемых в банкомат наличных денег или максимальной наполняемости устройства для хранения денежных купюр в платежном терминале, БУС подразделяют на следующие категории материальной ценности:

– категория ценности М1 – максимальная сумма загружаемых (хранящихся) в БУС наличных денег составляет более 1 миллиона

рублей (хищение такой суммы квалифицируется как кража в особо крупном размере);

– категория ценности М2 – максимальная сумма загружаемых (хранящихся) в БУС наличных денег составляет от 250 тысяч до 1 миллиона рублей (хищение такой суммы квалифицируется как кража в крупном размере);

– категория ценности М3 – максимальная сумма загружаемых (хранящихся) в БУС наличных денег составляет менее 250 тысяч рублей.

Если в одном помещении (зоне) установлено несколько БУС, то категорию ценности БУС рекомендуется определять, исходя из суммарной стоимости наличных денег, хранящихся (загружаемых) в БУС, расположенных в данном охраняемом помещении (охраняемой зоне).

Максимальный объем наличных денег, S, загружаемых в банкомат, определяют по специальной формуле.

3. Классификация БУС по функциональным возможностям.

Банкоматы по своим функциональным возможностям и назначению можно разделить на следующие виды:

а) банкоматы с функцией выдачи наличных денег;

б) банкоматы с функциями выдачи и приема наличных денег;

в) банкоматы с функциями полного (замкнутого) оборота наличных, выполняющие функции выдачи и приема наличных денег, использующие получаемые от клиентов купюры для выдачи другим клиентам без процедуры инкассации;

г) многофункциональные банкоматы, выполняющие кроме функций выдачи и приема наличных платежных операций (оплата услуг, налогов, штрафов, приобретение билетов на общественный транспорт, погашение кредитов, пополнение счетов, «электронных кошельков» и т.п), приема (сканирования), обработки, печати и выдачи банковских документов и т.п.

4. Классификация БУС по устойчивости к взлому.

По устойчивости к взлому БУС подразделяют на классы в соответствии с типами их сейфов, которые в зависимости от величины сопротивления к разрушающим воздействиям различными инструментами подразделяются на 8 классов по устойчивости к взлому.

Классификация банкоматов и других устройств самообслуживания по месту установки:

– «офисный» – свободная установка внутри помещения без выделения выгораживаемой сервисной зоны и зоны самообслуживания. Существуют модели банкоматов, в которых загрузка и техническое обслуживание может производиться спереди и сзади;

– «вестибюльно-офисный» – установка через стену внутри помещения. Доступ клиентов к устройству самообслуживания возможен только из внутренних помещений организации. При этом загрузка денежных средств и техническое обслуживание банкомата может производиться только сзади;

– «вестибюльно-уличный» – установка через наружную стену фронтальной частью в вестибюль (тамбур), имеющий выход на улицу. Доступ клиентов к БУС осуществляется без непосредственного входа в организацию;

– «уличный» – установка через наружную стену фронтальной частью на улицу без выделения выгораживаемой зоны самообслуживания. При этом загрузка денежных средств и техническое обслуживание банкомата может производиться только сзади.

Организация комплексной централизованной охраны банковских устройств самообслуживания.

Эффективность мер, принимаемых для обеспечения защиты БУС от преступных посягательств зависит от:

– выбора зон размещения БУС (зон самообслуживания, сервисных зон);

– соблюдения требований к инженерно-технической укрепленности БУС и мест их размещения;

– правильности выбора и применения технических средств охраны.

Для охраны БУС применяют:

1. Средства обнаружения проникновения.
2. Средства тревожной сигнализации.
3. Средства охранные телевизионные.
4. Охранно-поисковые средства.
5. Средства активной защиты и оповещения.
6. Средства защиты кассет с деньгами.
7. Средства защиты от скимминга.
8. Средства контроля и передачи извещений.
9. Средства контроля и управления доступом.
10. Шлюзовые кабины безопасности.

Средства обнаружения проникновения. В качестве средств обнаружения незаконного проникновения на охраняемый объект или в охраняемую зону в составе комплекса ТСО, как правило, используются охранные извещатели различного назначения и принципа действия, применяемые для защиты как самих БУС от преступных посягательств (взлома, повреждения, вандализма, несанкционированного перемещения), так и помещений, в которых они установлены (зоны самообслуживания, сервисной зоны), от незаконного проникновения в охраняемое помещение (зону).

Общие организационно-технические вопросы, отражающие особенности выбора, установки и эксплуатации средств обнаружения проникновения и угроз различных видов (охранных извещателей) в зависимости от степени важности и опасности объектов приведены в Р 069-2017.

2.5. Проектирование системы видеонаблюдения для охраны банковских устройств самообслуживания

Для видеонаблюдения в интересах обеспечения безопасности, контроля БУС и зон их размещения (зоны самообслуживания, сервисной зоны) должны применяться средства и системы охранные телевизионные, соответствующие требованиям ГОСТ Р 51558-2014.

Особенности условий работы видеокамер СОТ, применяемых для контроля БУС. Особенности условий работы видеокамер, устанавливаемых внутри БУС.

В большинстве БУС с функцией выдачи наличных денег устанавливают две внутренние видеокамеры: портретную и презентерную. Кроме того, в современных БУС с функцией приема наличных денег или многофункциональных БУС дополнительно устанавливают валидаторную видеокамеру. Эти три вида видеокамер, устанавливаемых внутри БУС, имеют различные задачи и различные условия работы, что определяет различные требования, предъявляемые к ним.

Целевой задачей портретной видеокамеры является получение четкого изображения лица клиента. Это накладывает дополнительные требования по разрешению видеокамеры, а также связано с размерами сцены по передней границе зоны самообслуживания БУС.

Целевые задачи презентерной и валидаторной видеокамер не связаны с получением изображения лица человека. Основное назначение этих камер – контроль действий клиента в процессе сеанса самообслуживания с помощью БУС при проведении операций с наличными денежными средствами. При этом желательно иметь возможность по изображению определить номинал купюр. Сцены этих камер, как правило, чрезвычайно малы, поскольку наблюдаемые объекты (презентеры и валидаторы БУС) находятся в нескольких сантиметрах или десятках сантиметров от самих видеокамер в силу конструктивных особенностей БУС.

В некоторых случаях, в зависимости от конструкции БУС, места размещения презентора (валидатора) и, соответственно, презентерной (валидаторной) видеокамеры, есть вероятность попадания в поля их зрения клавиатуры для ввода ПИН-кода этого (или другого) БУС либо номера ИЭК клиента во время начала (окончания) сеанса самообслуживания. В связи с этим необходимо соблюдать рекомендации по установке и настройке таких видеокамер.

2.6. Особенности применения специализированных средств охраны банковских устройств самообслуживания

Классификация охранно-поисковых средств.

Технические средства, предназначенные для позиционирования и поиска БУС, относящихся к группам ОП, ОВ и ОУ (в случае их хищения),

можно классифицировать по типу используемых данных и ресурсов следующим образом:

– технические средства позиционирования и поиска БУС, использующие данные и ресурсы действующих спутниковых навигационных систем GPS (США), ГЛОНАСС (Россия), GALILEO (Европейский союз) и BEIDOU (Китай);

– технические средства позиционирования и поиска БУС, использующие данные и ресурсы наземной сети операторов сотовой связи, предоставляющих соответствующую услугу (LBS) (LBS (Location-based service) – услуга, предоставляемая операторами сотовой связи для определения местоположения объекта (абонента) по базовым станциям этих операторов);

– комбинированные технические средства позиционирования и поиска БУС, использующие данные и ресурсы как спутниковых навигационных систем, так и наземных сетей операторов сотовой связи;

– технические средства позиционирования и поиска БУС, использующие данные и ресурсы специально созданных (развернутых) на территории отдельного поселения (в отдельном регионе) радиоканальных систем определения координат контролируемых объектов.

Средства активной защиты и оповещения.

Основные аспекты применения средств активной защиты и оповещения. Согласно теории анализа уязвимости и категорирования охраняемых объектов, основным критерием эффективности функционирования систем охранной сигнализации и противокриминальной защиты является вероятность пресеченияпротивоправных действий нарушителя, которая зависит от:

– вероятности обнаружения нарушителя техническими средствами охраны (охранными извещателями, детекторами движения видеокамер СОТ);

– вероятности удержания нарушителя (создания препятствий на пути проникновения в охраняемую зону) средствами ИТУ и СКУД (при ее наличии);

– вероятности нейтрализации нарушителя (вероятности того, что нарушитель по психофизическим причинам не сможет реализовать свой преступный замысел и будет вынужден покинуть охраняемую зону).

Вероятность быстрой нейтрализации нарушителя при установлении критериев и показателей эффективности систем охраны объектов, особенно объектов высоких категорий значимости, к которым относятся значительная часть БУС (банкоматы категории М1, М2), имеет такое же существенное значение, что и показатели удержания (средствами ИТУ) и обнаружения (при помощи ТСОС и СОТ) нарушителя.

Необходимо учитывать, что срабатывание охранно-дымовых систем может привести к срабатыванию технических средств пожарной сигнализации (если они установлены). Это обстоятельство может

потребовать принятия специальных технических решений, обычно на аппаратно-программном уровне конфигурирования охранно-пожарной или интегрированной системы безопасности объекта, при использовании охранно-дымовых систем в помещениях, оснащенных пожарными извещателями по ГОСТ Р 53325-2012 и (или) автоматическими установками пожаротушения.

Средства защиты кассет с деньгами.

В некоторых случаях, например при большой удаленности охраняемого банкомата от СПВО, могут быть использованы специальные устройства активной защиты кассет с наличными деньгами от несанкционированного доступа (спецкассеты), основанные на технологии окрашивания купюр при срабатывании ТСОС, например извещателей, защищающих банкомат от взлома и криминального открывания сейфа, а также от несанкционированного перемещения банкомата с целью взлома его сейфа в удаленном скрытом месте.

Для обеспечения такой защиты в каждую кассету банкомата могут быть вмонтированы элементы, позволяющие установить систему по защите наличных денег, хранящихся в кассетах, с применением технологии окрашивания купюр.

В состав комплекта защиты, как правило, входят:

– модули активной защиты со специальными несмываемыми чернилами,

– элементы управления для активации защиты.

Для каждого типа кассет существует свой комплект средств защиты, который может работать либо автономно, осуществляя контроль статуса кассет при их работе в банкомате, либо быть интегрированным в комплекс мер по защите денежных средств вне кассового центра при инкассации и хранении.

Основным условием применения технических средств защиты кассет с наличными деньгами, использующих технологию окрашивания купюр при попытке вскрытия или кражи кассет, является обеспечение этими техническими средствами закрашивания всех машиночитаемых признаков (соответствующих зон) на банкнотах, используемых банкоматами с функцией приема наличных денег и платежными терминалами для идентификации подлинности денежных купюр.

Средства защиты от скимминга.

В соответствии с рекомендациями Банка России все БУС должны быть оснащены антискиммингговым оборудованием, обеспечивающим защиту банкоматов и платежных терминалов, а также клиентов кредитных (платежных) организаций от мошенничества, связанного с незаконным считыванием конфиденциальной информации с целью дальнейшей подделки и незаконного снятия средств со счетов граждан. На рынке представлен широкий спектр устройств, предназначенных для защиты

БУС от скимминга.

Технические средства защиты от скимминга можно разделить на две основные группы:

– антискимминговые средства пассивной защиты;

– средства активного противодействия скимммингу.

Принцип действия средств активного противодействия скимммингу основан на создании электромагнитного поля в зоне картридера БУС, блокирующего скимминговые устройства.

Средства активного противодействия скимммингу должны предусматривать:

– возможность интеграции в централизованную систему мониторинга функционирования БУС;

– отсутствие возможности у злоумышленника обнаружить устройство визуально;

– наличие датчика проверки наличия «защитного поля», позволяющего обнаружить выведение из строя трансмиттера или атаку на него (например, путем излучения в противофазе);

– блокирование функционирования или отключение БУС при неисправности антискимминговой защиты, блокировка картридера;

– чувствительность к установке скимминговой оборудования, при обнаружении которого должно формироваться тревожное извещение;

– выдача уведомления о потенциальной угрозе по линии связи БУС с кредитной (платежной организацией);

– выход для формирования тревожного сообщения на ППКОП (УОО СПИ) для последующей передачи информации на ПЦО;

– хранение информации о тревогах в энергонезависимой памяти;

– световая индикация состояния.

В качестве технического средства активного противодействия скимммингу может быть использован, например, комплект оборудования «Cerber» (ООО «АНСЕР ПРО»).

Недостатком технических средств активного противодействия скимммингу является то, что на части устройств БУС близкое расположение считывающего устройства к входу картридера может привести к невозможности установки подобных систем без создания помех работе БУС.

Средства контроля и передачи извещений.

Для контроля состояния технических средств охраны используется объектовое оборудование систем передачи извещений (СПИ), включенных в список ТСО, рекомендованных к применению в подразделениях вневедомственной охраны Росгвардии.

Кроме того, необходимо иметь в виду, что обычные РСПИ, использующие общедоступный радиоканал или GSM-канал связи, могут быть выведены из строя квалифицированными нарушителями при помощи средств подавления радиосигналов. При этом антенны РСПИ (в случае их размещения снаружи БУС) могут быть умышленно выведены из строя.

В связи с этим для организации охраны БУС, в особенности групп ОП, ОВ и ОУ высокой категории материальной значимости (категории М1, М2), размещенных в местах средней, повышенной и высокой степени риска, целесообразно применение РСПИ повышенной надежности и устойчивости к саботажу, которые должны обеспечивать:

– устойчивую связь на необходимых для оперативного реагирования ГЗ СПВО расстояниях;

– регулярный автоматический контроль канала связи;

– устойчивость к подавлению радиосигналов;

– защиту от подмены;

– возможность скрытой установки объектового оборудования и антенны внутри БУС (в т.ч. в сейфе банкомата).

Средства контроля и управления доступом.

Средства контроля и управления доступом (СКУД) в отдельно выделенную зону круглосуточного банковского самообслуживания («зону 24») предназначены для:

– организации санкционированного доступа клиентов и персонала кредитных (платежных, сервисных) организаций, обслуживающих БУС, в помещение «зоны 24»;

– ограничения проникновения в «зону 24» случайных лиц, в том числе имеющих криминальные цели;

– предотвращения умышленного повреждения БУС и осуществления других незаконных действий;

– повышения безопасности клиентов при совершении ими банковских (платежных) операций;

– повышения безопасности инкассаторов и технических специалистов кредитных (платежных, сервисных) организаций при загрузке или выгрузке наличных денег и техническом обслуживании БУС.

Извещение о превышении времени нахождения человека возле БУС, санкционированно вошедшего в помещение «зоны 24», может передаваться в мониторинговый центр кредитной организации, а также служить управляющим сигналом для оператора СОТ, контролирующего данную «зону 24».

Вопросы для самостоятельной работы

1. Понятие объектового комплекса ОПС.
2. Понятие уязвимого места. Уязвимые места 1, 2, 3 рубежей охраны.
3. Шлейф сигнализации.
4. Понятие охраняемой зоны и принципа многорубежности объектового комплекса охраны.
5. Рубеж охраны.
6. Рубеж охранной сигнализации.
7. Шлейф сигнализации.

8. Способы формирования извещений о тревоге извещателями, подключенными в шлейф сигнализации.

9. Порядок подключения в шлейф сигнализации нормально-замкнутых извещателей типа «сухой контакт».

10. Порядок подключения в шлейф сигнализации нормально-разомкнутых извещателей типа «сухой контакт».

11. Порядок подключения в шлейф сигнализации нормально-разомкнутых извещателей типа «открытый коллектор».

12. Порядок подключения в шлейф сигнализации пожарных извещателей.

13. Порядок подключения оконечного элемента в ШС.

14. Какими проводами и кабелями следует пользоваться при организации сигнальных линии связи и шлейфов сигнализации?

15. Возможна ли совместная прокладка или пересечение шлейфов и сигнальной линии с линиями напряжением 110 В и более в одном коробе, трубе, жгуте, замкнутом канале строительной конструкции или на одном лотке?

16. Каково должно быть расстояние при параллельной открытой прокладке проводов и кабелей шлейфов и сигнальной линии до силовых и осветительных кабелей?

17. Основные правила техники безопасности при монтаже, техническом обслуживании и ремонте средств ОПС.

18. Порядок действий электромонтеров при измерении сопротивления ШС.

19. Порядок действий электромонтеров при измерении сопротивления утечки (изоляции) ШС.

20. Классификация банковских устройств самообслуживания.

21. Классификация БУС по конструкции, области применения и способу установки.

22. Классификация БУС по материальной ценности.

23. Классификация БУС по функциональным возможностям.

24. Классификация БУС по устойчивости к взлому.

25. Категорирование мест размещения банковских устройств самообслуживания.

26. Какие средства применяют для охраны БУС?

27. Какие охранно-поисковые средства применяют для охраны БУС?

28. Какие средства активной защиты и оповещения применяют для охраны БУС?

29. Какие средства защиты от скимминга применяют для охраны БУС?

ТЕМА 3
ВНУТРИОБЪЕКТОВЫЕ РАДИОКАНАЛЬНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Учебные и воспитательные цели:

Образовательные: изучить назначение и особенности построения внутриобъектовых радиоканальных систем безопасности.

Развивающие: расширить базовые знания обучающихся в области особенностей построения внутриобъектовых радиоканальных систем безопасности; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

3.1. Общие сведения о внутриобъектовых радиоканальных системах безопасности.

3.2. Пример построения беспроводной системы охранно-пожарной сигнализации на базе оборудования «Астра-Zитадель».

3.1. Общие сведения о внутриобъектовых радиоканальных системах безопасности

В настоящее время актуальной представляется проблема обеспечения безопасности коттеджей (коттеджных поселков), так как объем их строительства стремительно растет, а также исторических памятников, музеев, церквей и др. Особенностью таких объектов является сложность прокладки и сохранности проводных линий, а также необходимость сохранения внутреннего интерьера помещения.

Важными параметрами, характеризующими радиосистему, являются ее надежность и емкость.

Надежность радиосистемы определяется такими параметрами, как:

– помехоустойчивость;
– криптозащита;
– время работы радиоизвещателей от источника питания;
– температурный диапазон.

Помехоустойчивость определяется такими показателями, как:

– количество частотных диапазонов, в которых может работать радиосистема;
– количество частотных каналов в каждом диапазоне;
– возможность автовыбора резервных каналов;

– наличие автоматической регулировки мощности излучения.

Криптозащита. Рассматривая вопросы применения охранно-пожарных радиосистем, мы прежде всего говорим об охране стационарных объектов. Следовательно, необходимо принимать во внимание тот факт, что злоумышленник может скрытно на протяжении длительного времени проводить сканирование, запись и анализ всех сигналов радиосистемы. Поэтому при каждой передаче контрольных сигналов и сигналов управления участники обмена должны помимо использования динамически изменяемых ключей обеспечить невозможность саботирования системы с использованием предварительно записанных сигналов системы.

Время работы радиоизвещателей от источника питания. Существует ряд алгоритмов, которые могут ощутимо увеличить время работы периферийных устройств от источников питания: алгоритм регулирования мощности излучения, передача сообщений с квитированием, режим работы «день/ночь».

Температурный диапазон. Для того чтобы радиосистемы действительно стали надежной альтернативой проводным охранно-пожарным системам, необходимо обеспечить их работоспособность в диапазоне температур от –30 до +55 ºС (стандартном для проводных систем). Причем сложнее обеспечить стабильную работу радиосистемы в области отрицательных температур. Однако суть проблемы заключается не столько в характеристиках используемых источников питания (которые стабильно работают и при более низких температурах), сколько в обеспечении автоматической подстройки частоты радиоустройств, находящихся в различных температурных условиях.

Емкость радиосистемы, так же, как и надежность, определяет степень профессиональности той или иной радиосистемы. Очевидно, что для защиты достаточно значимого объекта сложно применять охранно-пожарные радиоканальные системы с числом адресных устройств менее 100.

Емкость радиосистемы (число адресуемых устройств) во многом определяется способностью системы регулировать объем передаваемой информации, а также мощностью излучения всех радиоустройств. Чем больше информации необходимо передать и чем сильнее устройства «экранируют» друг друга, тем меньшее число устройств может работать на одном частотном канале связи. Например, использование механизмов, исключающих передачу одного и того же сигнала «Тревога» несколько раз, существенно снижает объем передаваемой информации, а следовательно, увеличивает максимальное число совместно работающих устройств.

На современном рынке безопасности предлагается достаточно большое количество радиоканальных систем, позволяющих в полной мере

и с минимальными затратами реализовать требования, предъявляемые к системам организации безопасности.

Рассмотрим наиболее распространенные из них.

Радиоканальная система «Астра-РИ-М» предназначена для организации на объекте беспроводной охранно-пожарной и других видов сигнализации (тревожной, аварийной и т.п.) с использованием адресных радиоканальных извещателей и передачи закодированных извещений на ретранслятор периферийный РПУ «Астра РИ-М».

Особенности системы:

– радиус действия радиоканальных извещателей не менее 300 м в прямой видимости;

– радиус действия брелока РПДК не менее 1300 м в прямой видимости;

– радиус действия тревожной кнопки «Астра-3221» не менее 1000 м в прямой видимости;

– радиус действия радиопередающего устройства РПД системы «Астра-РИ» не менее 2500 м в прямой видимости;

– радиус действия ретранслятора (РТР) и радиоканального модуля реле и оповещения (МРО) не менее 500 м на открытой местности;

– контроль одним РПУ без применения ППКОП «Астра-812» до 48 радиоустройств (извещателей и РТР), из них РТР – не более 4 шт.;

– максимальная емкость системы «Астра-РИ-М» с применением «Астра-812» или «Астра-812М» – 196 радиоустройств;

– двусторонний протокол связи РПУ с ретрансляторами и беспроводными модулями реле и оповещения;

– динамическое кодирование сообщений с защитой от «квалифицированного обхода» (подмена извещателя, использование ранее записанных извещений);

– алгоритм контроля связи;

– алгоритм исключения наложений сигналов от нескольких радиоканальных извещателей;

– формирование РПУ кода в формате Touch Memory для управления постановкой на охрану / снятием с охраны по выходе ТМ;

– функция сохранения в ПК и восстановления из ПК резервных копий памяти регистрации радиоустройств в РПУ и в РТР, позволяющая при замене ключевых устройств в системе быстро восстановить ее работу без перерегистрации радиоустройств;

– три частотные литеры;

– новые сервисные функции:

– невозможность постановки системы на охрану (кроме пожарных и охранных круглосуточных), если не изменен заводской пароль инженера;

– невозможность взятия разделов на охрану (в том числе пожарных и охранных круглосуточных), если на эти разделы не назначены идентификаторы для управления;

– фильтр, не позволяющий пожарные извещатели привязать к охранным разделам и наоборот;

– блокирование клавиатуры ППКОП при применении незарегистрированного идентификатора 3 раза подряд.

Состав системы:

– «Астра-РИ-М РПУ» – модернизированное радиоприемное устройство (частотный диапазон 433 МГц, смена частотных литер программная или при помощи перемычек, контроль 48 извещателей, 2 выходных реле, USB разъем).

– «Астра-812» – приемно-контрольный прибор (контроль до 4 РПУ, до 4 ретрансляторов, до 192 радиоканальных извещателей или до 768 ШС, USB разъем).

– «Астра-812М» – приемно-контрольный прибор (программирование функций с помощью ПК и клавиатуры; возможность установки модуля радиоканального приемо-передающего, модуля резервированного источника питания.

– Модуль РПП «Астра-РИ-М» – модуль радиоканальный приемо-передающий (диапазон 433 МГц, для установки в ППКОП «Астра-812М» (базовую); поддержка до 192 извещателей, 4 ретрансляторов, 4 релейных модуля; смена частотных литер).

– «Астра-5121» – радиоканальный ИК пассивный извещатель (диапазон 433МГц, объемный, микропроцессор, 4-площадочный PIR-детектор, устойчивость к животным (до 20 кг), температурная компенсация.

– «Астра-5131» – радиоизвещатель ИК пассивный (433МГц, 2 исполнения: исполнение А – объемный, 10 м, 90 град., исполнение Б – поверхностный, 10 м, 10 град., дальность радиоканала – 300 м).

– «Астра-6131» – радиоизвещатель звуковой (433МГц, дальность – 6 м, дискретная регулировка чувствительности, дальность радиоканала – 300 м).

– «Астра-3321» – извещатель магнитоконтактный радиоканальный (433МГц, контроль вскрытия, дальность радиоканала – 300 м).

– «Астра-421» – радиоканальный пожарный дымовой извещатель (433МГц, дальность радиоканала – 300 м).

– «Астра-4511» – радиоканальный ручной пожарный извещатель (433МГц, дальность радиоканала – 300 м).

– «Астра-РИ-М РПДК» – брелок радиоканальный (433МГц, дальность радиоканала – 1300 м).

– «Астра-3221» – радиоканальная тревожная кнопка (433 МГц, бесшумный ход, возможность стационарного крепления, ношения с помощью зажима или цепочки, дальность радиоканала – 1000 м).

– «Астра-361» – извещатель утечки воды аварийного типа радиоканальный (433 МГц, дальность радиоканала – 300 м, комплектуется

из проводного извещателя «Астра-361» и извещателя «Астра-3321» в качестве радиопередатчика).

Система «Астра-Zитадель» предназначена для организации на объекте беспроводной охранно-пожарной и других видов сигнализации (тревожной, аварийной и т.п.) с использованием адресных радиоканальных извещателей системы «Астра-Zитадель».

Особенности системы:

– двусторонний радиообмен в соответствии со стандартом для беспроводных сетей IEEE 802.15.4 и спецификацией ZigBee Pro для использования в нелицензируемом диапазоне частот 2,4 ÷ 2,48 ГГц с нелицензируемыми уровнями мощности до 100 мВт;

– высокая надежность и устойчивость канала связи за счет:

– автоматического сканирования и выбора наименее занятого канала из 16 в процессе инсталляции (в перспективе будет организована автоматическая перестройка радиосети на менее занятые каналы в процессе работы системы);

– расширения спектра радиоканала до 2 МГц методом прямой последовательности и применением O-QPSK манипуляции (Offset-Quadrature Phase Shift Keying);

– обеспечения резервных вариантов путей доставки сообщения (система контролирует не менее 2 путей от каждого узла);

– динамическая маршрутизация информационных потоков – радиоустройства «сами отыскивают» пути доставки сообщений, а по индикации и показаниям ППКОП можно оценить параметры качества связи и наличие резервных путей;

– высокая пропускная способность в двустороннем канале радиосвязи, что позволяет организовать большую информативность при малом времени реакции системы (в том числе передачу аналоговых и дополнительных параметров извещателей);

– динамическая криптозащита со 128-битными ключами (для других радиосистем используются ключи 16-, 24-, 32-битные), что соответствует уровню высоко защищенных проводных интерфейсов;

– максимальная емкость системы – 250 радиоустройств разных типов;

– количество уровней ретрансляции – до 16;

– количество универсальных системных выходов – до 32;

– количество логических разделов в системе – до 96;

– количество пользователей системы – до 256;

– каждому пользователю системы можно назначить до 4 идентификаторов различного физического типа (брелоки, ТМ-коды, PIN-коды);

– каждому идентификатору могут быть присвоены различные полномочия на взятие / снятие отдельных разделов и групп разделов.

Состав системы:

– «Астра-Z-812М» – ППКОП с установленным приемо-передающим модулем РПП (диапазон 2,4÷2,48 ГГц, поддержка до 250 радиоустройств различных типов);

– «Астра-942» – лазерный пульт для проверки работоспособности радиоустройств системы (оптимизация радиосвязи между радиоустройствами, запуска регистрации в радиосети; входит в комплект поставки «Астра-Z-812М»);

– «Астра-Z-8845» исп. А – ретранслятор-маршрутизатор (электропитание от источника напряжения 10 – 27 В; возможность установки АКБ на 24 ч работы; 1 ШС с токовым контролем, 1 системный выход);

– «Астра-Z-8845» исп. Б – ретранслятор-маршрутизатор (электропитание от внешнего резервированного источника питания напряжением 10–27 В; 1 ШС с токовым контролем, 2 системных выхода);

– «Астра-Z-8745» исп. А – ретранслятор-маршрутизатор, включаемый в сетевую розетку АС 220 V (проходная розетка, возможность установки АКБ на 24 ч работы);

– «Астра-Z-8745» исп. Б – ретранслятор-маршрутизатор, включаемый в сетевую розетку АС 220 V (проходная розетка, управление подключенными устройствами дистанционно или кнопкой на корпусе);

– «Астра-Z-5145» исп. Б – радиоканальный извещатель ИК пассивный, (2,4 ГГц, поверхностный, 10 м, 10 град., дальность радиоканала – до 300 м);

– «Астра-Z-6145» – радиоканальный звуковой поверхностный извещатель (2,4 ГГц, дальность – 6 м, дальность радиоканала – до 300 м);

– «Астра-Z-4245» – радиоканальный пожарный дымовой извещатель (2,4 ГГц, оптико-электронный, дальность радиоканала – до 300 м);

– «Астра-Z-3245» – брелок радиоканальный 4-кнопочный (тревога, постановка, снятие, сервис, 2,4 ГГц, дальность радиоканала – до 200 м);

– «Астра-Z-2945» – оповещатель речевой (2,4 ГГц; 95 дБ, 8 речевых сообщений, возможность подключения линий ГО и ЧС, питание от двух элементов – основного и резервного);

– «Астра-884» – сеть GSM (речевые сообщения на 8 любых телефонов разрядностью до 15, SMS на мобильные телефоны, цифровой поток в стандарте ADEMCO CONTACT ID на ПЦН).

Внутриобъектовая радиосистема охранно-пожарной и адресно-аналоговой пожарной сигнализации «Стрелец».

Система предназначена для организации охранно-пожарной и адресно-аналоговой пожарной сигнализации на объектах не только частного, но и общественного пользования, где по различным причинам (сохранение целостности интерьера, непрерывная эксплуатация помещений и т.д.) применение проводных систем невозможно или ограничено.

Особенности системы:

– двухсторонний протокол обмена между всеми радиоустройствами «Аргус-Диалог»;

– 10 радиочастотных каналов передачи (с автоматическим и ручным выбором);

– автоматический выбор резервного канала передачи (свободного от помех);

– разнесенный радиоприем;

– до 400 радиоустройств, находящихся в зоне взаимной радиовидимости на одном радиочастотном канале передачи;

– возможность построения полноценной адресной пожарной радиосистемы;

– программируемый период передачи контрольных радиосигналов от 12 с до 2 мин;

– криптографическая защита сигналов с механизмом динамической аутентификации;

– микросотовая топология системы.

Емкость системы «Стрелец»:

– до 16 радиорасширителей;

– до 512 радиоизвещателей (до 32 извещателей на каждый радиорасширитель);

– до 256 радиоканальных исполнительных устройств, сирен, брелоков и пультов управления (до 16 устройств на каждый радиорасширитель).

Построение системы «Стрелец» представлено на рис. 3.1.

Состав системы:

Радиорасширители:

– радиорасширитель охранно-пожарный РРОП (ППКОП);

– радиорасширители пожарные АСБ-РС и РРП-240.

Радиоизвещатели:

– пожарный дымовой адресно-аналоговый «Аврора-ДР» (ИП 21210-3); пожарный тепловой адресно-аналоговый «Аврора-ТР» (ИП 10110-1-А1);

– пожарный комбинированный адресно-аналоговый «Аврора-ДТР» (ИП 21210/10110-1-А1);

– пожарный ручной электроконтактный «ИПР-Р» (ИПР 51310-1);

– охранный поверхностный звуковой «Арфа-Р» (ИО 32910-2);

– охранный поверхностный звуковой «Арфа-2Р» (ИО 32910-3, с входом для подключения охранного ШС);

– охранный объемный оптико-электронный «Икар-Р» (ИО 40910-3);

– охранный объемный оптико-электронный, устойчивый к движению животных (весом до 40 кг) «Икар-5Р»;

– охранный магнитоконтактный универсальный РИГ (ИО 10210-4, с входом для подключения охранного, пожарного или тревожного ШС).

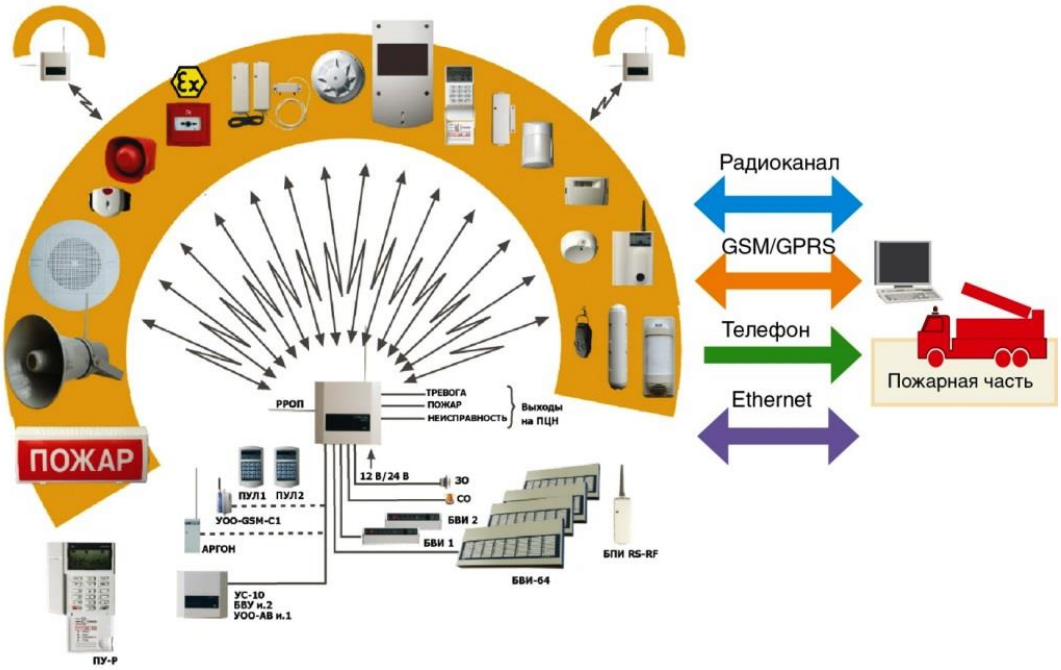


Рис. 3.1. Построение системы «Стрелец»

Исполнительные блоки:

- исполнительный блок релейный ИБ-Р;
- исполнительный блок релейный ИБ-Р2;
- оповещатель звуковой радиоканальный «Сирена-Р»;
- радиоканальная система речевого оповещения «Орфей-Р».

Устройства управления и индикации:

– радиобрелок управления РБУ;

– клавиатура управления с проводным интерфейсом ПУЛ;

– клавиатура управления с беспроводным интерфейсом ПУЛ-Р;

– клавиатура программирования и управления с беспроводным интерфейсом ПУ-Р;

– блоки выносной индикации БВИ и БВИ-64.

Система «Стрелец-Интеграл».

В системе возможна организация 500 тысяч адресов и объединения до 255 зданий.

Новое поколение системы «Стрелец» – ИСБ «Стрелец-Интеграл» – позволяет объединить по протоколу промышленной автоматики LonWorks десятки радиосистем в единую систему емкостью до 500 000 адресов с централизованным управлением.

Такая система может быть необходима при оборудовании больничного комплекса: например, в корпусах установлена радиоканальная система, а между корпусами – витая пара, локальная сеть или интернет до единого пульта наблюдения. Или когда на этаже высотного здания устанавливаются беспроводные устройства, а между этажами прокладывается единая объединяющая «шина». Таким образом, в

рамках одного объекта можно совмещать преимущества проводного и радиоканального решений. Построение системы показано на рис. 3.2.

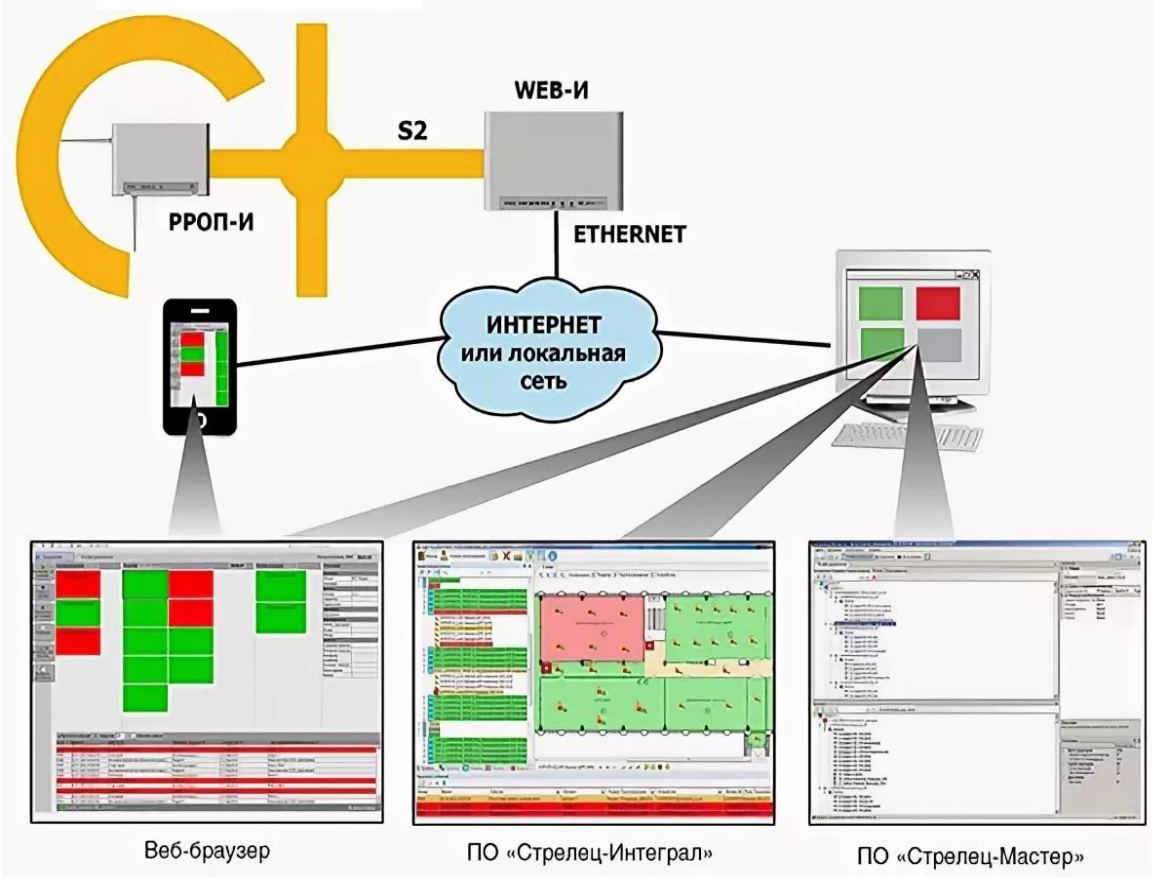


Рис. 3.2. Построение системы «Стрелец-Интеграл»

Интегрированная система безопасности «Стрелец-Интеграл» – это:

– беспроводная и проводная охранная сигнализация;

– беспроводная и проводная пожарная сигнализация;

– беспроводная и проводная система управления оповещением и эвакуацией (Э);

– беспроводная и проводная система автоматического управления пожаротушением;

– система контроля и управлением доступом;

– система видеорегистрации;

– автоматический мониторинг по всем каналам связи.

Особенности системы:

– гибридность системы: «радио» + «провод»;

– интеграция с промышленной автоматикой (LonWorks®);

– автоматический мониторинг по всем каналам (радио, IP-сеть, GSM, Contact ID).

Гибридность системы: ИСБ «Стрелец-Интеграл» обладает уникальными возможностями интегрирования беспроводных устройств предыдущего поколения системы «Стрелец» (извещатели, исполнительные

устройства, пульты управления и т.д.) и проводных устройств системы нового поколения.

ИСБ «Стрелец-Интеграл» состоит из сегментов. Один сегмент — это отдельное здание или группа этажей в здании.

Емкость системы:

– 255 сегментов в системе;

– 127 приборов в сегменте (например, РРОП-И или БШС8-И);

– 2048 адресов в сегменте (например, извещателей или шлейфов).

Интеграция с промышленной автоматикой: оборудование ИСБ «Стрелец-Интеграл» интегрируется с подсистемами автоматизации зданий (вентиляция, кондиционирование, освещение и т.д.), использующими для обмена протокол промышленного стандарта LonWorks ANSI/EIA 709.1 / EN 14908.

Для системы «Стрелец-Интеграл» разработан набор специализированных объектовых устройств (модемов), подключаемых к объектовой системе по протоколу LonWorks, обеспечивающих автоматический мониторинг по GSM/GPRS, Contact ID, IP-сетям, радиоканалу (150 МГц, 25мВт; 146-174 МГц, 5 Вт; 403-470 МГц, 5 Вт).

Преимущества использования сетевой платформы LONWORKS:

– высокая помехозащищённость линий связи, благодаря:

– дифференциальному способу передачи данных;

– гальванической изоляции устройств от линии связи;

– алгоритмам помехоустойчивого кодирования;

– квитированию и многократному повторению каждого пакета данных;

– отсутствие необходимости использования кабелей с экранированной витой парой;

– отсутствие необходимости соблюдения полярности подключения проводников;

– возможность использования единой среды для передачи сигналов различных систем;

– возможность использования произвольных сетевых топологий (шина, звезда, кольцо, смешанная);

– высокая скорость передачи информации (от 78 кбит/с);

– поддержка различных физических сред передачи данных (витые пары, Ethernet/Internet);

– высокая имитостойкость обмена данными, предотвращающая несанкционированное вмешательство в работу системы.

Каждое устройство ИСБ имеет уникальный физический адрес NID (аналог MAC-адреса, использующегося в компьютерных сетях). Адрес NID имеет длину 6 байт, и представляется в виде последовательности из 6 пар шестнадцатеричных цифр, например «00 A1 DF AE DF 1C». Адрес NID используется для передачи команд к устройству при его первоначальном

конфигурировании, а также в случае необходимости удалённого изменения его конфигурационных свойств.

Адрес NID нанесён на ярлыке на поверхности модуля сетевого интерфейса. Адрес передаётся устройством в линию связи при нажатии на кнопку “Service”, встроенную в каждое устройство ИСБ.

Использование двунаправленной связи со случайным множественным доступом и адаптивной динамической маршрутизации значительно повышает надежность (помехоустойчивость, живучесть) системы и позволяет использовать её не только для мониторинга коммерческих объектов, но и для пожарного мониторинга социальных и особо значимых объектов, оперативного управления пожаротушением и оповещением при пожарах и других чрезвычайных ситуациях.

3.2. Пример построения беспроводной системы охранно-пожарной сигнализации на базе оборудования «Астра-Zитадель»

На примере магазина промтоваров демонстрируется применение объектовой системы беспроводной охранно-пожарной сигнализации «Астра-Zитадель».

Особенности системы «Астра-Zитадель»:

– особенность беспроводной части системы «Астра-Zитадель» – информационный обмен в радиосетях в соответствии со стандартом IEEE 802.15.4 в радиочастотном диапазоне 2,4 – 2,4835 ГГц;

– особенность проводной части – информационный обмен в сетях произвольной топологии стандарта TIA/EIA-485-A (RS-485 с улучшенными показателями драйверов, позволяющими подключение в сеть до 64 устройств без применения специальных мер согласования и развязки);

– поддержка радиоканальных устройств системы «Астра-РИ-М» через радиорасширитель (РР) «Астра-РИ-М»;

– поддержка адресных извещателей системы «Астра-А» через адресный проводной расширитель «Астра-А РПА»;

– «сквозная» настройка всей системы и каждого ее устройства с помощью программного комплекса мониторинга (ПКМ) «Астра Pro» при подключении к компьютеру только центрального ППКОП серии Pro («Астра-8945 Pro» или «Астра-812 Pro»);

– упрощенная настройка системы с помощью программы Pconf-Pro без необходимости установки SQL. В программе отсутствуют функции локального мониторинга и настройки радиоканального речевого оповещения.

– интуитивно понятный интерфейс программы Pconf-Pro и модуля настройки из комплекта ПКМ «Астра Pro»;

– простота монтажа беспроводной части;

– полная свобода при размещении и монтаже радиоустройств системы на объекте;

– автоматическое построение основных и резервных путей передачи информации.

План расположения оборудования и структурная схема разработанной системы приведены на рис. 3.3 и рис. 3.4 соответственно.

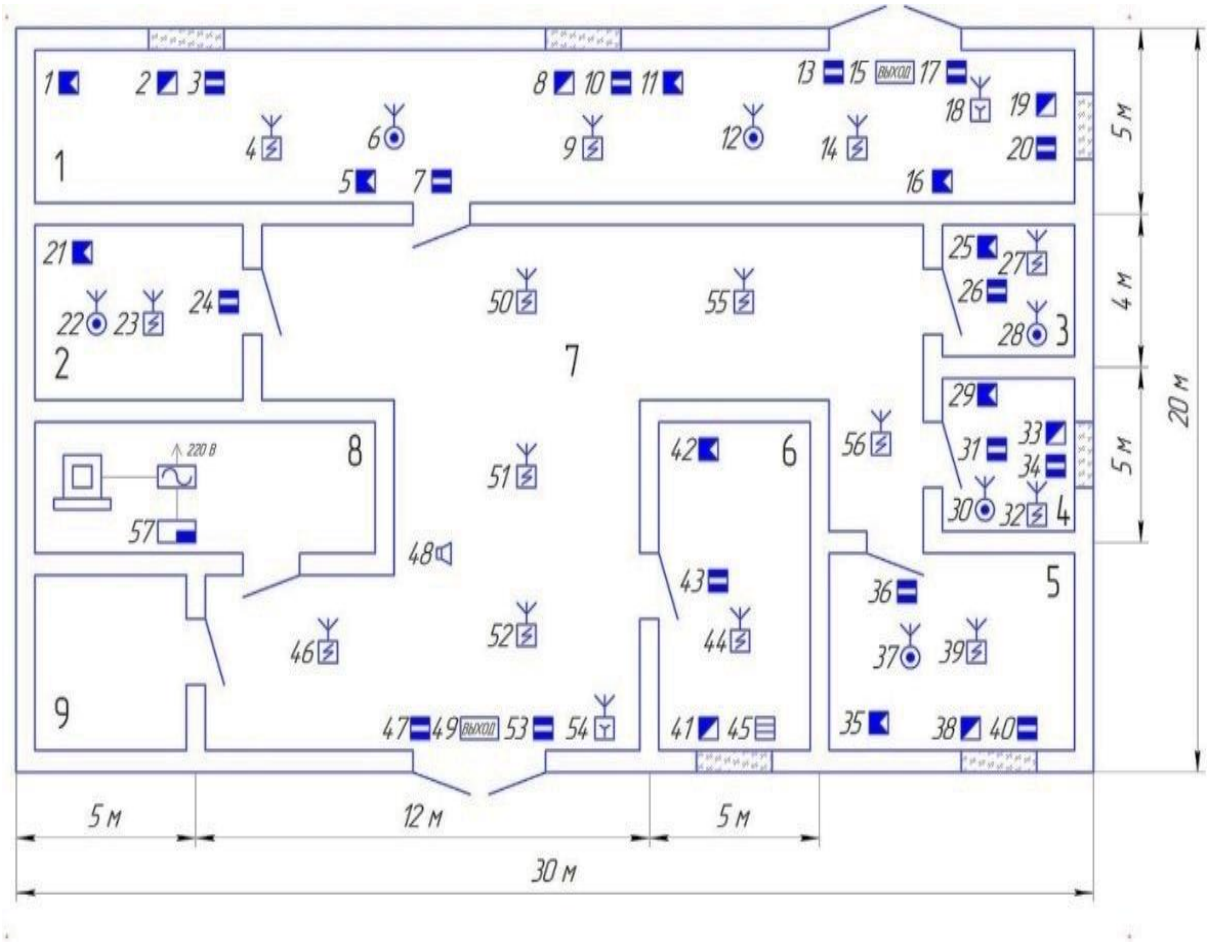


Рис. 3.3. План расположения оборудования системы охранно-пожарной сигнализации объекта торговли

Выбор системы продиктован тем, что информационный обмен осуществляется в радиосетях в соответствии со стандартом IEEE 802.15.4 ZigBee Pro в радиочастотном диапазоне 2,4 – 2,4835 ГГц. По сравнению с диапазонами 433 и 868 МГц используемый канал для передачи данных образовался относительно недавно, что говорит о меньшей его загруженности. Кроме того, используемый протокол ZigBee Pro обладает самоорганизующейся и самовосстанавливающейся ячеистой топологией с ретрансляцией и маршрутизацией сообщений внутри сети.

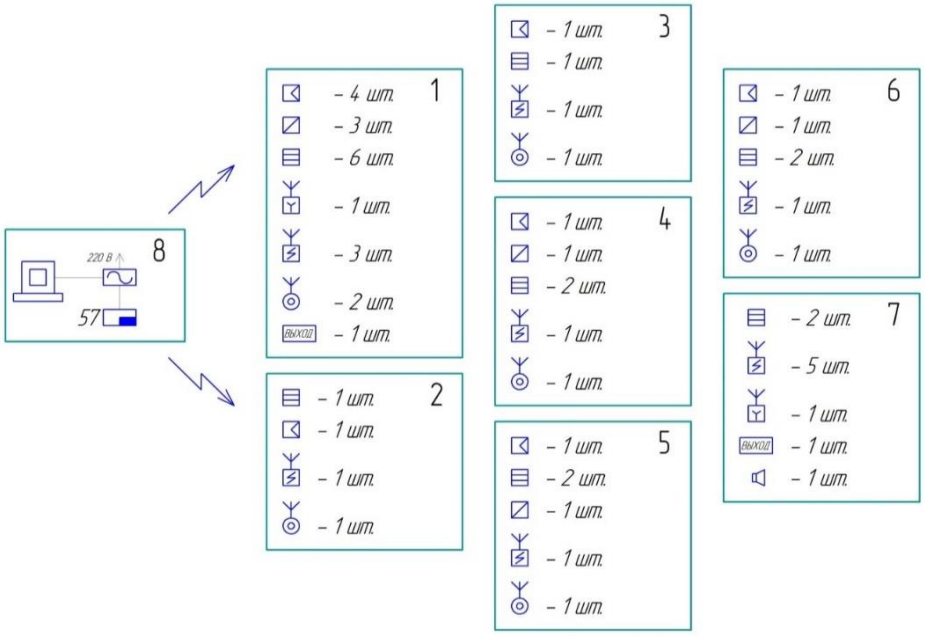


Рис. 3.4. Структурная схема системы охранно-пожарной сигнализации объекта торговли

В составе системы 57 технических средств охраны (табл. 3.1), при этом каждый извещатель представляет собой самостоятельный радиопередатчик, обменивающийся информацией о своем состоянии с прибором приемно-контрольным охранно-пожарным «Астра-8945 Pro». Мониторинг состояния системы осуществляется с помощью автоматизированного рабочего места в комнате охраны (помещение № 8), где осуществляется также постановка на охрану / снятие с охраны созданных логических разделов. Физическая охрана осуществляет только мониторинг состояния объекта в ночное время, патрулирование не предусмотрено.

Элементы системы разделены на три раздела (табл. 3.2), в каждом из которых выделены подразделы, объединяющие технические средства обнаружения в различных помещениях объекта по общему признаку (охранная, пожарная или тревожная сигнализация). К числу наиболее уязвимых мест объекта относятся: двери, заблокированные магнитоконтактными извещателями «на открывание»; окна, защищенные магнитоконтактными извещателями «на открывание» и звуковыми извещателями «на разбитие». Предусмотрена блокировка внутренних объемов объекта пассивными оптико-электронными извещателями. Контроль стен «на разрушение» нецелесообразен. Кроме того, в помещениях установлены тревожные кнопки, предназначенные для подачи сигнала «Тревога» при возникновении угрозы жизни, здоровью сотрудников и посетителей либо в случае возникновения других чрезвычайных обстоятельств. Пожарная сигнализация организована с использованием дымовых оптико-электронных извещателей и ручных

пожарных извещателей. Во время пожара предусмотрено звуковое (сирена) и световое оповещение (табло «ВЫХОД»). Санитарный узел (помещение № 9) средствами сигнализации не оборудован.

Для расчета стоимости технического обслуживания и трудозатрат технические средства охраны приведены к условным установкам. Суммарные затраты на технические средства охраны системы составляют 171 336 руб. (табл. 3.1). Общее количество условных установок 12,16 единиц.

Таблица 3.1

Используемые технические средства охраны

Номер	Наименование оборудования	Количество	Стоимость единицы	Стоимость общая	Количество условных установок	Общее количество условных установок	Условное графическое обозначение ТСО
1	«Астра-Z-5145» исп. А. Извещатель инфракрасный пассивный объемный, 10м, 90 град. дискр. рег. чувствительности, дальность РК до 300 м, универсальный кронштейн	9	1999	17991	0,3	2,7	
2	«Астра-8945 Pro». Прибор приемно-контрольный охранно-пожарный	1	5891	5891	0,3	0,3	
4	«Астра-Z-3345». Извещатель магнитоконтактный контроль вскрытия, контроль питания, подключение внешних СМК, дальность радиоканала до 300 м	16	1612	25792	0,01	0,16	
5	«Астра-Z-4545». Извещатель пожарный ручной, дальность радиоканала до 300 м	2	2466	4932	0,1	0,2	
6	«Астра-Z-4245». Извещатель пожарный дымовой, оптико-электронный, дальность радиоканала до 300 м	13	1852	24076	0,3	3,9	
7	«Астра-Z-6145». Извещатель звуковой, поверхностный, дальность 6 м, микропроцессор дискр. рег.	6	2466	14796	0,4	2,4	

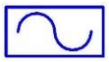
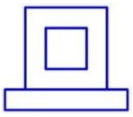
Номер	Наименование оборудования	Количество	Стоимость единицы	Стоимость общая	Количество условных установок	Общее количество условных установок	Условное графическое обозначение ТСО
	чувствительности, контроль вскрытия, дальность радиоканала до 300 м.						
8	«Астра-Z-3245». Брелок радиоканальный 4-х кнопочный (тревога, постановка, снятие, сервис), дальность действия до 200 м	2	1507	3014	0,1	0,2	
9	Источник вторичного электропитания резервированный СКАТ-1200И7	1	4350	4350	0,3	0,3	
10	«Астра-Z-2745». Световой указатель, питание от двух элементов, дальность радиоканала до 300 м	2	2540	5080	0,1	0,2	
12	«Астра-Z-2945». Оповещатель речевой; 95 дБ, 8 речевых сообщений, возможность подключения линий ГО и ЧС, питание от двух элементов, дальность радиоканала 300 м	1	5414	5414	0,1	0,1	
13	АРМ ДПЦО	1	30000	30000	1,7	1,7	

Таблица 3.2

Разделы системы охранно-пожарной сигнализации

Разделы	Зоны
Пожарная сигнализация	
Помещение № 1	4, 9, 14, 18
Помещение № 2	23
Помещение № 3	27
Помещение № 4	32
Помещение № 5	39
Помещение № 6	44
Помещение № 7	46, 49, 50, 51, 52, 54, 55, 56
Охранная сигнализация	
Помещение № 1	1, 2, 3, 5, 7, 8, 10, 11, 13, 15, 16, 17, 19, 20

Разделы	Зоны
Помещение № 2	21, 24
Помещение № 3	25, 26
Помещение № 4	29, 31, 33, 34
Помещение № 5	35, 36, 38, 40
Помещение № 6	41, 42, 43, 45
Помещение № 7	47, 53
Тревожная сигнализация	
Помещение № 1	6, 12
Помещение № 2	22
Помещение № 3	28
Помещение № 4	30
Помещение № 5	37

В заключение необходимо отметить, что использование беспроводных технологий при построении систем безопасности объектов различных форм собственности позволяет существенно сократить время на их внедрение, а также существенно повысить живучесть объектовых систем охранной и пожарной сигнализации. Пример построения беспроводной системы охранно-пожарной сигнализации наглядно иллюстрируется в настоящей работе с использованием оборудования системы «Астра-Zитадель», рекомендованной к использованию подразделениям вневедомственной охраны Росгвардии.

Вопросы для самостоятельной работы

1. Перечислите внутриобъектовые радиоканальные системы безопасности, рекомендованные к использованию в подразделениях вневедомственной охраны.
2. Дайте понятие уязвимого места. Уязвимые места 1-го, 2-го, 3-го рубежей охраны.
3. Дайте понятие охраняемой зоны и принципа многорубежности объектового комплекса охраны.
4. Что понимается под рубежом охранной сигнализации?
5. Какие параметры радиоканальной системы влияют на ее надежность?
6. В каких случаях целесообразно применение внутриобъектовых радиоканальных систем безопасности?
7. Каковы типовые технические характеристики внутриобъектовых радиоканальных систем безопасности?

ТЕМА 4
СИСТЕМЫ ОХРАННЫЕ ТЕЛЕВИЗИОННЫЕ

Учебные и воспитательные цели:

Образовательные: изучить назначение и особенности построения систем охранных телевизионных.

Развивающие: расширить базовые знания обучающихся в области организации системы охраны с использованием систем охранных телевизионных; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

4.1. Назначение и особенности построения систем охранных телевизионных.

4.2. Основные требования к системам охранным телевизионным.

4.3. Телевизионные камеры в системах охранных телевизионных.

4.1. Назначение и особенности построения систем охранных телевизионных

Система охранная телевизионная (СОТ) – телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты.

Основные задачи СОТ:

– осуществление оперативных задач по охране (подтверждение факта несанкционированного проникновения на объект);

– видеоконтроль (прямое видеонаблюдение оператором);

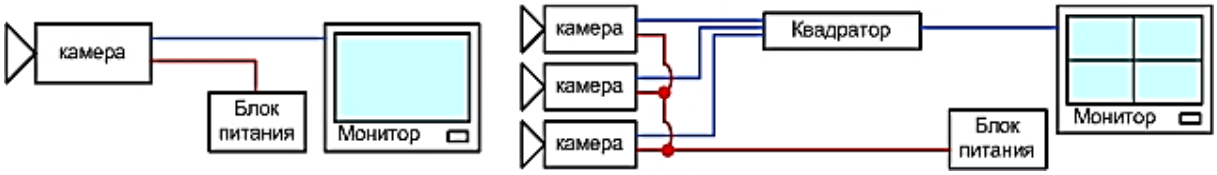
– видеорегистрация (архивирование видеоинформации).

4.2. Основные требования к системам охранным телевизионным

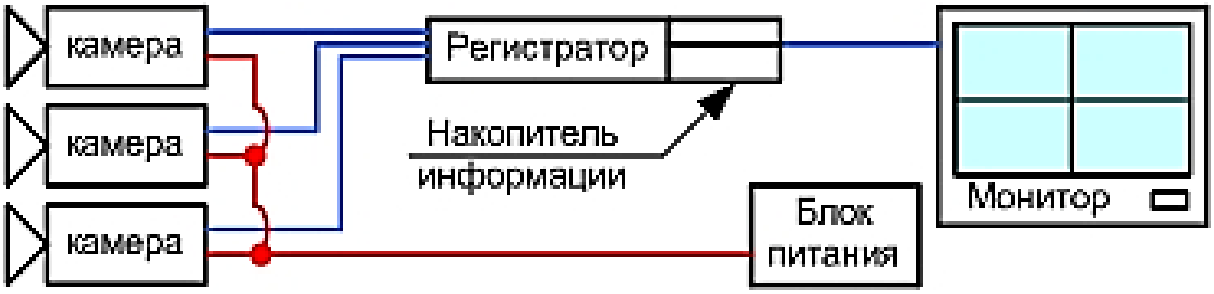
Системы охранные телевизионные по ГОСТ должны с учетом конкретных условий и особенностей процессов деятельности на объекте обеспечивать визуальное наблюдение ситуационной обстановки в заданном формате изображения, обнаружение и идентификацию субъектов наблюдения в зависимости от назначения – людей, транспортных средств,

имущества, элементов объектовой инфраструктуры, а также визуальное документирование и архивирование получаемой видеоинформации.

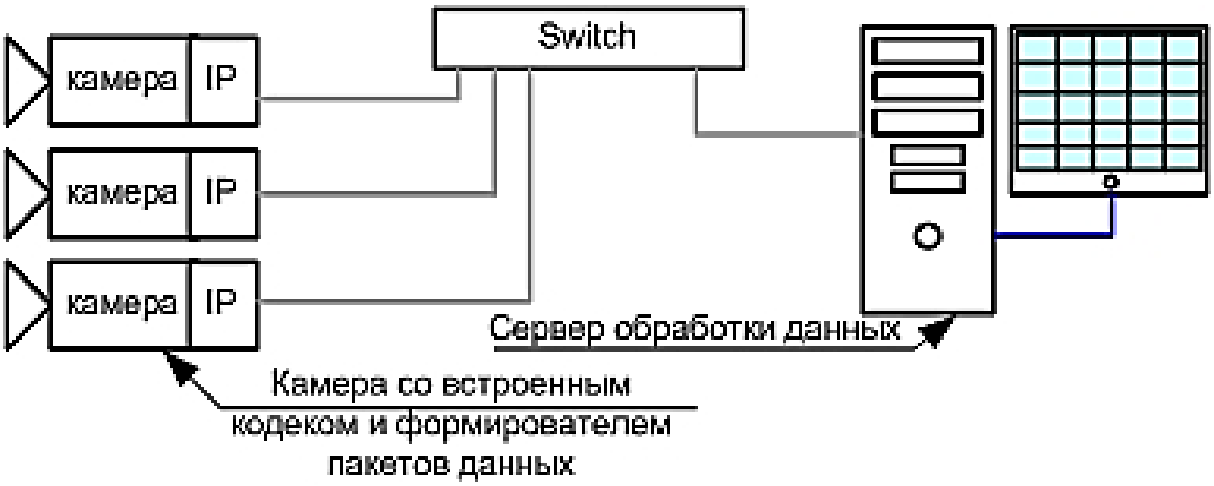
Видеоинформация из контрольных зон объекта должна поступать в локальные и/или в централизованные пункты ДДП для верификации и регистрации. Обобщённые структурные схемы СОТ приведены на рис. 4.1. в соответствии с действующей классификацией.



а) аналоговые СОТ



б) комбинированная СОТ



в) цифровая СОТ

Рис. 4.1. Структурные схемы СОТ

4.3. Телевизионные камеры в системах охранных телевизионных

Телевизионная камера (ТВК) является важнейшим элементом СОТ, так как именно она создает видеосигнал, который в дальнейшем используется видеосистемой для анализа, детекции и хранения

видеоинформации. От выбора камеры зависит, что и как будет видеть на экране видеомонитора оператор в постоянно меняющихся условиях наблюдения. Если необходимо не только следить за общей обстановкой в охраняемой зоне, но и идентифицировать людей, определять номер автомобиля и т.д., проектировщик должен выбрать камеру с действительно необходимыми функциями и техническими характеристиками.

Телевизионная камера (ТВК) – это устройство, преобразующее оптическое изображение охраняемой зоны (свет) в электрический видеосигнал.

Чтобы понять устройство ТВК вспомним некоторые положения теории света и устройство человеческого глаза.

Основная «проблема», с которой сталкиваются ученые, изучающие свет, заключается в том, что свет имеет двойственную природу: он ведет себя как волна (нематериальная природа) – это явления интерференции, дифракции, рефракции и отражения – и обладает также свойствами материальной природы – широко известный фотоэффект.

1678 г. – «Трактат о свете» – волновая теория света Христиана Гюйгенса.

Начало XVIII в. – корпускулярно-волновая теория Исаака Ньютона.

1803 г. – эксперимент, подтверждение волновой теории Томасом Юнгом.

1873 г. – свет – это электромагнитная волна (Джеймс Кларк Максвелл).

1887 г. – открыто явление фотоэффекта (Генрих Герц).

1905 г. – теоретическое обоснование фотоэффекта (Альберт Эйнштейн).

Итак, свет – это электромагнитное излучение. Человеческий глаз может реагировать на это излучение и различать частоты, которые воспринимаются глазом как цвет. Электромагнитное излучение включает все частоты, или длины волн. Видимый свет занимает лишь небольшое «окно» этого диапазона, от 380 нм до 780 нм. Чтобы легче было запомнить, мы приближенно примем границы диапазона равными 400 нм и 700 нм. 400 нм соответствует фиолетовому цвету, а 700 нм – красному. По мере увеличения длины волны цвет непрерывно переходит от фиолетового к голубому, зеленому, желтому, оранжевому и красному. Для определения средней чувствительности человеческого глаза было проделано множество экспериментов и тестов, на основе которых было выяснено, что не все цвета оказывают одинаковое воздействие на сетчатку глаза.

Глаз наиболее чувствителен к зеленому цвету (около 555 нм). Другими словами, если собрать все длины волн с равной энергией, то зеленый будет иметь наибольший «выход» на сетчатке.

Почему максимум спектральной чувствительности лежит в зеленом цветовом диапазоне (около 555 нм)? Возможно, это связано с тем фактом,

что большая часть солнечной энергии, проникающей в атмосферу Земли, сконцентрирована на длинах волн порядка 555 нм.

Исключение составляют животные, которые видят в ночное время.

Остановимся на глазе человека, а для этого важно понимать его «конструкцию».

Существует ряд концептуальных аналогий между устройством глаза и ТВ-камеры.

Сетчатка – это «фоточувствительная область», состоящая из миллионов клеток – колбочек и палочек. Эти клетки можно рассматривать как часть нашей нервной системы. Колбочки чувствительны к средней и яркой интенсивности света и воспринимают цвета. Палочки чувствительны к низким уровням света и не способны различать цвета. Ночью мы видим благодаря палочкам, поэтому в темноте мы не можем различать цвета. Число колбочек в каждом глазе приблизительно составляет 10 млн, а палочек – около 100 млн. Колбочки сконцентрированы вокруг области прохождения оптической оси. Эта область окрашена желтым пигментом и называется желтым пятном. Желтое пятно является основной областью, которую обрабатывает наш мозг, и, хотя она очень мала, концентрация колбочек в ней составляет около 50 000. Среднее фокусное расстояние глаза (то есть расстояние между хрусталиком и сетчаткой при разглядывании бесконечно удаленного объекта) составляет около 17 мм. Такое фокусное расстояние дает резкое изображение в пространственном угле, равном примерно 30°. Это также и размер области, где больше всего колбочек. Именно поэтому угол в 30° считается стандартным углом зрения.

Концентрация колбочек возрастает по направлению к центру оптической оси, достигая максимума лишь на 10°. Каждая из клеток-колбочек соединяется с мозгом отдельным зрительным нервом, по которому электрические импульсы посылаются в мозг. Конечно, глаз видит и под гораздо большим углом, так как сетчатка охватывает пространственный угол почти в 90°, и колбочки есть и вне желтого пятна, но к одному нерву в этом случае подсоединена группа колбочек. Эта часть сетчатки называется областью периферического зрения.

ТВК построена по принципу человеческого глаза:

– «Хрусталик» – «Оптическая система – набор линз».

– «Радужная оболочка» – «Диафрагма».

– «Сетчатая оболочка» – «ПЗС-матрица» (светочувствительный материал).

1624 г. Первые приборы наблюдения. Г. Галилей. Подзорные трубы.

1839 г. Фотография (Ньепс, Луи Дагер).

Гелиограф (астрономия) – телескоп для наблюдения за Солнцем.

Экспони́рование – процесс облучения светочувствительного материала актиничным электромагнитным излучением.

1920 – 1927 г. «Рассекатель изображения». Фило Фарнсворт. Передающая вакуумная телевизионная трубка.

1931 г. – иконоскоп. Владимир Козьмич Зворыкин.

Первые камеры изготовлялись из стеклянных трубок и светочувствительного люминофорного покрытия на внутренней поверхности стекла. Сегодня мы называем их передающими трубками. Работают передающие трубки по принципу фоточувствительности, основанному на фотоэффекте. Свет, проецируемый на люминофорный слой трубки (называемый мишенью), обладает энергией, достаточной, чтобы вызвать выбивание электронов из кристаллической решетки люминофора. Число выбиваемых электронов пропорционально свету, и таким образом формируется электрическое представление световой проекции.

Работа всех передающих трубок основывается на принципе сканирования электронным лучом мишени внутри трубки под действием электромагнитного поля. Луч отклоняется электромагнитным полем, генерируемым электронной системой камеры. Когда электронный луч попадает в конкретную часть потенциального рельефа, электрический ток теряет заряд пропорционально количеству света. Этот очень слабый ток – порядка пикоампер (1 пА) – подается на видеоусилитель с очень высоким входным сопротивлением, который и формирует напряжение видеосигнала. После того как сигнал сформирован, электронная система телекамеры добавляет синхроимпульсы, и на выходе телекамеры мы получаем полный видеосигнал, называемый композитным видеосигналом.

Недостатки ТВК с ЭЛТ.

1. Большие габаритные размеры.

2. Влияние ЭМ помех на ЭМ отклоняющую систему вызывает искажения картинки.

3. Необходимость высокого напряжения (до 1000 В) для придания ускорения электронному лучу и задания его траектории. Поэтому в телекамерах приходится использовать высоковольтные компоненты, что всегда представляет собой потенциальную проблему для устойчивости электронных схем.

4. Люминофор постоянно подвергается электронной бомбардировке, и слой со временем изнашивается (срок – 2 года). В результате мы можем увидеть такую картину: движущиеся люди похожи на призраков, они полупрозрачны и сквозь них просвечивают «впечатанные» изображения.

5. Геометрические искажения, обусловленные тем, что луч падает на мишень под различными углами.

1970 г. – появление ПЗС-матриц.

Новая ПЗС-технология позволила исключить все эти проблемы. Однако вначале невозможно было достичь разрешающей способности, соответствующей хорошей передающей трубке.

ПЗС-матрицы по сути своей являются светочувствительными аналоговыми сдвиговыми регистрами.

Последовательное переключение напряжения на электродах перемещает потенциальную яму, а следовательно, и находящиеся в ней электроны, в определённом направлении. Так происходит перемещение по одной строке матрицы.

Внешний вид ПЗС-камеры и камеры с ЭЛТ.

Современная ТВК состоит из:

1) объектива – оптического устройства или набора линз, рассчитанных для взаимной компенсации аберраций и собранных в единую систему внутри оправы для создания действительного оптического изображения;

2) фоточувствительного элемента ПЗС- или КМОП-матрицы;

3) программно-аппаратных средств обработки сигналов в формат, предназначенный для вывода на устройства отображения (аналоговый или цифровой сигнал).

ПЗС-матрица (CCD – Charge-Coupled Device) – специализированная аналоговая интегральная микросхема, состоящая из светочувствительных элементов (пикселей), выполненная на основе кремния, использующая технологию приборов с зарядовой связью.

КМОП-матрица (CMOS – Complementary-symmetry/metal-oxide semiconductor) – светочувствительная матрица, выполненная на основе КМОП-технологии – комплементарная логика на транзисторах «металл-оксид-полупроводник». В КМОП-матрицах используются полевые транзисторы с изолированным затвором с каналами разной проводимости.

Основные параметры ТВК.

ТВК имеет очень большой набор характеристик и параметров, но для выбора ТВК специалисту достаточно знать основные из них.

Параметры ПЗС-матрицы.

1. Формат матрицы – размер фоточувствительной области матрицы выражается в дюймах. Основными форматами являются: 1/4", 1/3", 1/2", 2/3" и 1".

Чем больше оптический формат, тем меньше геометрические искажения изображения. В особенности это сказывается при больших углах зрения. В СОТ высокого качества изображения обычно используются камеры формата 1/2", 2/3" и 1".

Как и диагональ телевизора, размер ПЗС-матрицы измеряется в дюймах. Этот параметр (формат ПЗС-матрицы) приводится в паспорте на камеру и необходим для правильного выбора объектива – если объектив поставляется отдельно, что очень редко для камер бюджетного диапазона. При прочих равных условиях предпочтительнее выбирать камеру с большей матрицей – пиксел большего размера позволяет захватить большее количество света. Поэтому даже в том случае, когда количество пикселов у двух камер одинаково, изображение, записанное пикселами

большего размера чётче. (Правда, сказанное справедливо только для высоких уровней освещённости, так как уровень шумовых токов у такой матрицы также значительно выше). В то же время, как правило, камера с ПЗС-матрицей меньшего формата дешевле. Помимо цены и малых габаритов, малоформатные телекамеры имеют еще одно преимущество – уменьшенное энергопотребление (примерно пропорционально формату).

2. Разрешающая способность (Resolution). Она характеризует способность видеосистемы различать мелкие детали и удаленные предметы. Разрешающая способность видеокамер измеряется в так называемых телевизионных линиях (ТВЛ) – количестве различимых на экране видеомонитора вертикальных черных и белых штрихов минимальной толщины (то есть речь идет о разрешающей способности по горизонтали, поскольку по вертикали число элементов жестко привязано к телевизионному стандарту. Общепринятыми являются стандарты CCIR для черно-белых и PAL для цветных камер. Оба стандарта подразумевают 625 строк по вертикали). Чем выше значение разрешающей способности, тем более мелкие детали и более удаленные предметы можно наблюдать. Как правило, этот параметр не превышает число пикселей в строке, умноженное на 0,75.

Разрешающая способность по вертикали – максимальное число горизонтальных линий, которое способно передать оборудование. Разрешающая способность по вертикали ограничена количеством строк в кадре и определяется видом телевизионного стандарта (PAL или NTSC). 625 строк.

Разрешающая способность по горизонтали – это максимальное число вертикальных линий, которое способно передать оборудование. Фактически разрешение по горизонтали в основном и интересует потребителей, так как разрешающая способность по вертикали у стандартных камер одинакова. Чем больше вертикальных линий умещается по всей ширине строки, тем больше на изображении проработаны мелкие детали.

Камеры могут быть низкого разрешения (до 200 ТВЛ), обычного разрешения (200–380 ТВЛ), высокого разрешения (381–570 ТВЛ), специальные (свыше 570 ТВЛ).

Измерить разрешение ТВК можно с помощью тестовой таблицы.

3. Цветность. Черно-белая или цветная. Цветные ПЗС-матрицы имеют аналогичную чёрно-белым структуру, но перед ячейками формируются микрофильтры основных цветов R, G, B (следовательно, у цветных видеокамер количество результирующих ячеек будет в 3 раза меньше, чем у черно-белых) и ИК-фильтр.

4. Чувствительность (Sensitivity). Чувствительность измеряется в люксах (лк) и определяет качество работы камеры в условиях низкой освещенности. Параметр может приводиться в документации.

5. Минимальная освещенность – Minimum illumination. Это такой уровень освещённости на объекте, измеренный в стандартных условиях, при котором можно различить переход от черного к белому. Чем меньше её значение, тем выше качество видеокамеры (обстановка на объекте становится все темнее, а изображение остается еще различимым).

В черно-белых видеокамерах высокой чувствительности в условиях недостаточной освещённости происходит переключение в режим пониженной разрешающей способности или возрастания времени накопления зарядов на элементах матрицы. Наиболее чувствительные (0,001-0,01 люкс) камеры могут использоваться для ночных наблюдений без ИК-подсветки. Для эффективной работы таких камер вполне достаточно лунного света. Для помещений минимальная чувствительность камер может составлять 0,5 лк.

Цветные видеокамеры имеют значительно меньшую чувствительность в видимом диапазоне, а также у них отсутствует чувствительность в инфракрасной области спектра. Поэтому при низкой освещенности цветные видеокамеры автоматически переходят в режим черно-белого изображения.

6. Отношение сигнал/шум – signal to noise.

Следует учитывать, что при недостаточной освещенности объектов (в тёмное время суток) амплитуда полезного видеосигнала камер обычно падает. Поэтому важно при оценке минимальной освещенности обращать внимание на указанное отношение сигнал/шум на выходе видеокамеры. Оно говорит о качестве выходного сигнала камеры. Параметр «отношение сигнал/шум» (S/N = signal to noise) измеряется в децибелах. Его значение не должно быть ниже 30 дБ, иначе шумы на экране начинают сильно влиять на качество видеосигнала («снег» на изображении). При отношении сигнал/шум 45 дБ шум практически не заметен. При 40 дБ шум уже заметен, 30 дБ сильные шумы, 20 дБ изображение теряется в шумах. Следует, конечно, учитывать, что в технических характеристиках камер значения сигнал/шум указываются для оптимальных условий.

Отношение сигнал/шум ПЗС-телекамеры определяется как отношение сигнала к шуму, производимому матрицей и электроникой телекамеры. Чтобы получить реальное отношение сигнал/шум телекамеры, все внутренние цепи (так или иначе влияющие на сигнал) должны быть отключены.

7. Синхронизация – привязка видеосигнала к фазе сетевого напряжения, или внешнего источника синхроимпульсов, или другого видеосигнала. Камеры, питающиеся от сети переменного тока (220 В/50 Гц или 24 В/50 Гц), синхронизируются от питающей сети. Камеры, питающиеся от источника постоянного тока (12 В), должны иметь вход внешней синхронизации, сигнал на который подается от специального устройства – синхронизатора.

8. Электронный затвор (Electronic Shutter) – свойство камеры регулировать время накопления заряда на ПЗС-матрице позволяет обеспечить постоянную среднюю яркость изображения, получить приемлемое качество изображения быстродвижущихся объектов и обеспечивает работоспособность камеры в условиях высокой освещенности.

Обычные электронные затворы обеспечивают регулировку выдержки в диапазоне от 1/50 с до 1/10000 – 1/15000 с. Лучшие электронные затворы позволяют получить выдержки порядка 1/100000 с, что позволяет отрабатывать изменения уровня освещённости в 2000 раз.

9. Автоматическая регулировка усиления. Так как в процессе работы видеокамера преобразует интенсивность светового потока в размах напряжения и может работать в широком диапазоне освещённостей, для выравнивания амплитуды выходного видеосигнала по всему диапазону применяется автоматическая регулировка усиления. Благодаря режиму АРУ, имеется возможность осуществлять непрерывную съемку планов с разной яркостью, значительно выравнивая её значения на экране монитора. Автоматическая регулировка усиления позволяет повысить резкость изображения при чрезмерной освещённости (ослабить эффект засветки).

10. Компенсация встречной засветки (Backlight Compensation). Как видно из названия, функция находит применение при необходимости откорректировать изображение, когда какой-либо объект в поле зрения камеры представлен на ярком фоне. Это может быть человек в тёмном коридоре на фоне открытого дверного проёма либо едущий навстречу камере автомобиль с включёнными фарами и т.д. В режиме компенсации встречной засветки видеокамера позволяет выровнять по яркости изображение в целом – ослабить чересчур яркие участки и передать на монитор картинку примерно одинаковой яркости по всему кадру.

11. Гамма-коррекция – изменение выходного сигнала видеокамеры таким образом, чтобы на мониторе получилось изображение с верной контрастностью. В некоторых моделях чёрно-белых видеокамер имеется специальная схема, позволяющая увеличить число градаций при передаче полутонов чёрного и серого цветов. При максимальном значении коэффициента гамма-коррекции (1,0) полутона изображения получаются наиболее контрастными, «глубокими». При минимальном (0,4) – обеспечивается воспроизведение наиболее «мягких» полутонов.

12. Баланс белого (White Balance). Параметр цветных видеокамер. Изменение освещённости может приводить к значительным искажениям цветопередачи, если камера не содержит специальной схемы «баланса белого». Схема обеспечивает пропорциональное изменение электронными методами коэффициентов усиления в каналах красного и синего цвета относительно зелёного. Такое решение позволяет верно передавать цвет объекта независимо от источника освещения. Недорогие

цветные камеры имеют лишь автоматический «баланс белого» для данного источника света. Внутри более качественных камер, как правило, имеются регулировки для адаптации к разным источникам света.

Параметры оптического объектива.

Варио- (варифокальный) объектив – объектив, в котором фокусное расстояние может изменяться вручную в определенном диапазоне. Объектив имеет устройство контроля фокуса и некоторые функции управления диафрагмой.

Объектив с трансфокатором – объектив, в котором фокусное расстояние может изменяться дистанционно сигналами телеуправления в определенном диапазоне. Объектив имеет устройство контроля фокуса и некоторые функции управления диафрагмой.

Объектив «Pin-hole» («игольное ушко») – объектив с фиксированным фокусным расстоянием, имеющий очень маленькое отверстие и предназначенный для скрытого наблюдения. Объектив обычно не имеет никакого управления фокусом, но предполагает некоторые функции управления диафрагмой.

13. Фокусное расстояние и угол зрения.

14. Светосила, относительное отверстие.

Диафрагма – средство для контроля размера апертуры объектива и, следовательно, количества света, проходящего через него.

Диафрагма ручная – диафрагма, в которой изменения размера апертуры объектива проводятся ручным методом.

Автодиафрагма – диафрагма, автоматически изменяющая размер апертуры объектива в ответ на изменения освещенности сцены.

Апертурный угол – угол между крайним лучом конического светового пучка на входе (выходе из) оптической системы и ее оптической осью.

Апертура объектива – диаметр D светового пучка на входе в объектив и целиком проходящего через его апертурную диафрагму. Эта величина определяет дифракционный предел разрешения объектива. Угол, под которым видны самые мелкие детали на объекте D(мм)/140, – в угловых секундах.

15. Глубина резкости (Depth of field) – диапазон расстояний, на которых объекты наблюдения остаются хорошо сфокусированными. Короткофокусные объективы имеют большую глубину резкости. С увеличением расстояния до объекта увеличивается глубина резкости. Длиннофокусный объектив даже при съёмке удалённых объектов имеет ограниченную глубину резкости.

Основные типы ТВК:

– аналоговые и цифровые;
– корпусные и бескорпусные;
– для внутреннего и уличного применения;
– стационарные;

– поворотные;
– купольные;
– для применения в особых условиях;
– черно-белого и цветного изображения;
– повышенной чувствительности;
– высокого разрешения;
– для скрытого наблюдения.

Вопросы для самостоятельной работы

1. Система охранная телевизионная – это..?
2. Основные задачи СОТ.
3. Обобщенная структурная схема аналоговой СОТ.
4. Обобщенная структурная схема комбинированной СОТ.
5. Обобщенная структурная схема цифровой СОТ.
6. Формат ПЗС-матрицы.
7. Разрешающая способность.
8. Чувствительность.
9. Отношение «сигнал/шум».
10. Виды объективов.
11. Фокусное расстояние.
12. Глубина резкости.
13. Автоматическая регулировка усиления.
14. Электронный затвор.
15. Компенсация встречной засветки.
16. Гамма-коррекция.
17. Баланс белого.
18. Эффективный диаметр объектива.
19. Диафрагма.
20. Апертура объектива
21. Видеомагнитофон. Назначение. Основные ТТХ.
22. Видеопринтер. Назначение.
23. Видеомонитор. Назначение. Основные ТТХ.
24. Квадратор (Делитель экрана). Назначение. Основные ТТХ.
25. Мультиплексор. Назначение. Основные ТТХ.
26. Видеокоммутатор. Назначение.
27. Видеорегистратор. Назначение. Основные ТТХ.
28. Сетевая камера. Назначение. Основные ТТХ.
29. Видеосервер. Назначение. Основные ТТХ.

ТЕМА 5
СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Учебные и воспитательные цели:

Образовательные: изучить назначение и особенности построения систем контроля и управления доступом.

Развивающие: расширить базовые знания обучающихся в области особенностей организации безопасности с использованием систем контроля и управления доступом; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

5.1. Назначение и особенности построения систем контроля и управления доступом.

5.2. Принцип действия и основные требования к системам контроля и управления доступом.

5.3. Организация учета рабочего времени с помощью систем контроля и управления доступом.

5.1. Назначение и особенности построения систем контроля и управления доступом

Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Обобщенная структурная схема СКУД приведена на рис. 5.1.

Рассмотрим основные вопросы и задачи, решаемые с использованием систем контроля и управления доступом.

Прежде всего, СКУД, как техническое средство, затрудняющее доступ посторонних лиц на территорию предприятия, организации, фирмы и т.п., обеспечивает повышение уровня безопасности, улучшение уровня защиты персонала и материальных ценностей.

Повышение порядка на территории объекта означает, что сотрудники и посетители могут пройти только в те помещения, доступ в которые им разрешен. При этом порядок на территории – немаловажный фактор и для организации охраны: значительно проще организовать охрану объекта, на котором царит порядок.

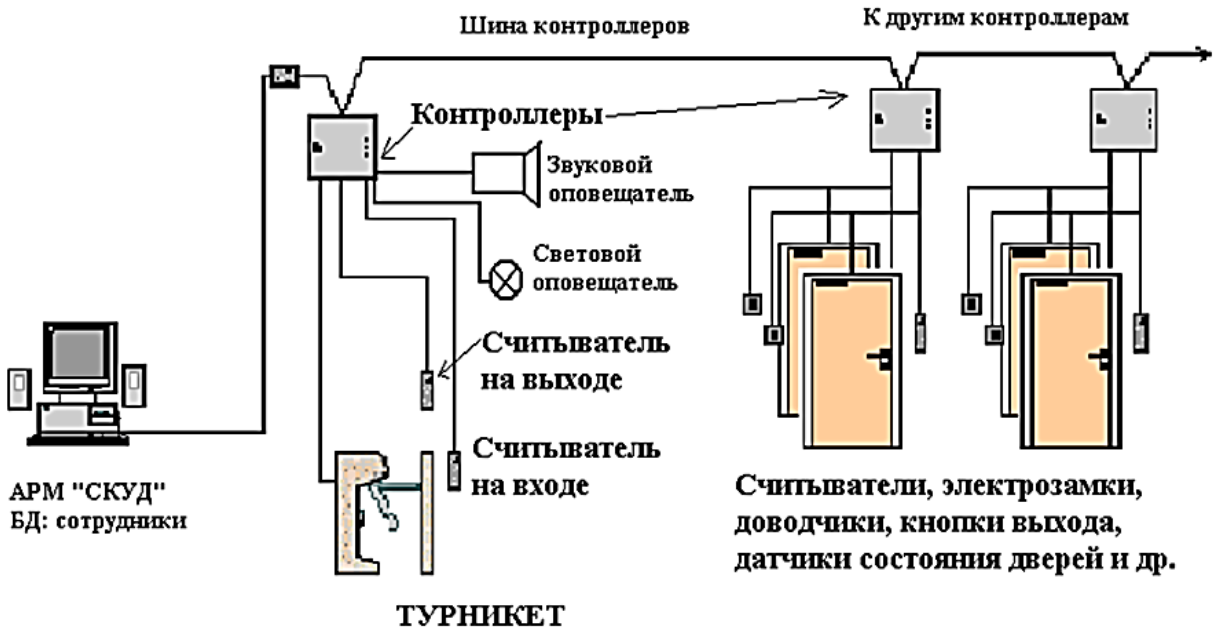


Рис. 5.1. Обобщенная структурная схема СКУД

Организация учета. Поскольку все проходы в системе фиксируются, на основании данных СКУД возможно получение информации о времени нахождения сотрудников на предприятии. Та же информация, соотнесенная с рабочими графиками сотрудников, позволяет организовать автоматизированный учет рабочего времени, что, в свою очередь, дает объективные данные для решения задачи автоматизации планирования ресурсов.

Помимо этого, развертывание на объекте СКУД ведет к естественному оснащению субъектов (физических лиц) и ряда объектов (автотранспорт, грузы, иные материальные ценности) средствами идентификации (увязка идентификационных признаков с их носителем). Это делает возможным решение целого ряда дополнительных вопросов: создание системы внутренних расчетов; автоматизация логистики и т.п.

Современные СКУД, как часть интегрированной системы управления объектом, могут увязывать перемещение и активность кодоносителей с реакцией других составных частей:

– системы управления автоматики (вентиляция, освещение);
– системы видеонаблюдения, архивирования;
– системы охранно-пожарной сигнализации.

Теперь рассмотрим, какие задачи при этом решаются.

1. Территориальное ограничение.

СКУД ограничивает замкнутую территорию (здание, зону), доступ в которую / из которой возможен только под контролем СКУД. Данная задача решается введением устройств преграждающих управляемых (УПУ) в точках доступа и дополнительных заграждений и зон контроля в местах возможного проникновения субъектов.

2. Персонализация субъектов и объектов.

Привязка идентификатора (идентификационного признака) к операнду доступа (субъекту или объекту доступа) в базе данных СКУД. Задача решается введением устройств ввода идентифицирующих признаков (УВИП) в точках доступа, занесением связки «кодоноситель-операнд» в базу данных и, возможно, раздачей кодоносителей.

3. Пространственно-временные ограничения.

СКУД ограничивает доступ в зависимости от текущего времени и даты и информации о предыдущем состоянии-положении операнда. Данная задача решается преимущественно средствами программного обеспечения СКУД на различных уровнях, в зависимости от реализации.

Вопрос применения СКУД возникает перед теми, кто сталкивается с проблемами обеспечения безопасности и ограничения доступа посторонних лиц на территорию предприятия, учреждения, офиса или объекта, а также контроля доступа сотрудников предприятий в обособленные помещения (повышенной опасности, мест хранения ценностей, оружия и т.д.).

Широкое развитие СКУД получили в 1990-х годах. Контроль доступа стал актуальной необходимостью вследствие повысившейся активности террористов и роста преступности. Одних этих причин достаточно для организации мер в сфере безопасности для противодействия этим угрозам. Однако есть другие факторы и угрозы, защита от которых может быть обеспечена с помощью контроля доступа. Ограничение доступа в опасные помещения, контроль над перемещением персонала по объекту, позволяют повысить технику безопасности и снизить риск технологических аварий. Контроль над перемещением персонала по объекту может повысить дисциплину, автоматизировать учет рабочего времени, обеспечить охрану технологических и коммерческих секретов от промышленного шпионажа, предотвратить преступления и кражи на рабочем месте и т.д.

Автоматизация процесса контроля доступа может снизить человеческий фактор. Исследования показывают, что на проходных предприятий, где существуют массовые потоки людей, в часы пик человек-контролер допускает до 25% ошибок, то есть может пропустить посторонних. После четырех часов работы величина ошибки возрастает до 40%. Поэтому автоматизированные электронные системы управления доступом работают в крупных аэропортах, банках, гостиницах, ядерных научных центрах, военных базах и т.д.

СКУД – самое интенсивно развивающееся направление в технике обеспечения безопасности. Это связано с целым рядом факторов.

Во-первых, СКУД могут обеспечить полную автоматизацию контроля и управления доступом, что в общем случае приводит к экономии средств на обеспечение безопасности.

Во-вторых, СКУД могут решать такие задачи, как учет рабочего времени, быстрое определение местонахождения сотрудника, управление лифтами, освещением, вентиляцией и т.д.

В-третьих, СКУД позволяет решить вопрос повышения безопасности на объекте в течение всего времени суток, так как она обеспечивает эффективный контроль над помещениями, сотрудниками и посетителями, в то время как системы охранной сигнализации функционируют, как правило, только в нерабочее время. Кроме того, СКУД позволяет сотрудникам, обладающим необходимыми полномочиями, чувствовать себя свободно и иметь возможность перемещаться по зданию или территории объекта без помех.

5.2. Принцип действия и основные требования к системам контроля и управления доступом

В основе работы СКУД заложен принцип сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с информацией, заложенной в памяти системы.

Каждый из пользователей (сотрудников) получает индивидуальный идентификатор. Это может быть пароль или кодовое число, которые необходимо запомнить, или некоторый предмет, в который, или на который, с помощью специальной технологии занесена кодовая информация.

В качестве такого предмета может быть использована пластиковая карта, брелок, браслет или другой подобный предмет. Идентификатор может быть закреплен также на определенном предмете и транспортном средстве.

Пароль, кодовое число, а также предмет-идентификатор относятся к классу присвоенных идентификационных признаков. При этом идентифицируется не сам человек, а присвоенный ему признак.

В качестве идентификационных признаков могут использоваться также биометрические данные человека (отпечатки пальцев, геометрия кисти руки, голос и т.д.). Биометрическая идентификация определяет человека по его собственным идентификационным признакам.

Работа СКУД происходит следующим образом. У входа в контролируемое помещение устанавливаются специальные устройства (устройства ввода идентификационных признаков), которые предназначены для считывания информации с идентификатора или ввода биометрических показателей человека. Далее информация поступает на устройства управления (контроллеры и компьютеры системы), которые на основании анализа данных о владельце реагируют соответствующим образом и обеспечивают управление преграждающими и исполнительными устройствами: открывают или блокируют дверь, включают сигнал тревоги, регистрируют присутствие человека на рабочем месте и т.д.

Понятие идентификатора и идентификации является основным понятием для СКУД. Термин «идентификация» означает опознавание, поиск по признаку. Идентификация может производиться по следующим основным признакам:

– идентификация по запоминаемому коду – по коду, вводимому вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств;

– идентификация по вещественному коду – по коду, записанному на физическом носителе (идентификаторе), в качестве которого применяются различные ключи, карты, брелоки и т.д.;

– биометрическая идентификация – идентификация, основанная на определении индивидуальных физических признаков человека.

СКУД по ГОСТ Р 51241 должны предотвращать на объекте несанкционированный доступ в контрольные зоны с ограниченным доступом, не создавая препятствий для прохода (проезда) в зоны со свободным доступом.

СКУД должны обеспечивать необходимые условия соблюдения внутриобъектового режима и выполнения соответствующих обязанностей персоналом объекта в зависимости от конкретных условий и особенностей процессов деятельности на объекте, пребывания на нем людей, транспортных средств.

5.3. Организация учета рабочего времени с помощью систем контроля и управления доступом

На крупных предприятиях и в крупных организациях важным аспектом нормальной деятельности является трудовая дисциплина сотрудников, которая связана с поздним приходом на работу или ранним уходом с работы в нарушение своего рабочего графика, с незаконным нахождением вне территории объекта и т.д. Поэтому в настоящее время для руководителей предприятий (организаций) все более актуальной становится проблема учета рабочего времени сотрудников.

Автоматизировать этот процесс позволяет система учета рабочего времени с помощью системы контроля и управления доступом, позволяющей регистрировать реальное время присутствия сотрудников на рабочих местах и создавать отчеты с различной степенью подробности.

Для ведения учета рабочего времени на объекте необходимо иметь следующие элементы системы контроля и управления доступом:

– пропуска-идентификаторы, содержащие персональные коды доступа пользователей системы;

– считыватели, устанавливаемые на входе в охраняемую территорию и идентифицирующие пользователей системы по персональным кодам;

– контроллеры, принимающие решение о разрешении прохода сотрудников на охраняемую территорию и управляющие замками, турникетами и прочими подобными устройствами;

– датчики прохода, позволяющие регистрировать проход пользователя системы через турникет. Такие датчики могут быть уже встроены в турникет;

– программное обеспечение, осуществляющее настройку оборудования и параметров системы контроля доступа. А именно: «Администратор БД», «БД», «Оперативная задача для мониторинга событий».

Программное обеспечение позволяет создавать как развернутые, так и краткие отчеты, по которым ведется контроль рабочего времени сотрудников. Такие отчеты могут быть выполнены по группе сотрудников или каждому сотруднику. При создании отчетов учитываются различные типы режимов рабочего времени: фиксированный, сменный, гибкий, суммированный. Кроме этого, ведется учет как фиксированных, так и плавающих перерывов на обед, праздничных дней, отпусков, отсутствия по болезни, прогулов, командировок и т. д.

Учет рабочего времени сотрудника может проводиться с различной степенью подробности:

– ежедневный, с показом всех приходов и уходов;

– ежедневный, только с приходом и уходом с работы;

– еженедельный, с разбивкой по дням или суммированный;

– ежемесячный, с разбивкой по неделям, дням или суммированный;

– годовой, с разбивкой по месяцам, неделям, дням или суммированный.

Предусмотрен также контроль опозданий и ранних уходов. При этом в настройках системы можно задать интервалы времени, в течение которых сотрудник считается вовремя пришедшим на работу.

Индивидуальные настройки системы.

Для каждого сотрудника возможна индивидуальная настройка параметров системы. Режим учета рабочего времени сотрудника может быть назначен с ежедневной детализацией, т.е. каждый день сотрудника может иметь разное время прихода, ухода, перерыва на обед и пр. Кроме этого, при создании отчетов можно задавать дополнительные параметры, влияющие на расчет рабочего времени, например, учитывать уходы сотрудника в течение рабочего дня как рабочее время.

Программа «Учёт рабочего времени» является сетевым приложением и позволяет просматривать данные с любого компьютера, включённого в сеть, где она установлена: охраны, бухгалтерии, руководства. Это приложение является составной частью АРМ и не может работать без его базы данных.

Особенности программы «Учёт рабочего времени»:

– возможность рассчитывать различные отчеты по сотрудникам предприятия: общий отчет об отработанном времени, список нарушителей трудовой дисциплины, отчет о сотруднике с детализацией по дням, подробный отчет о сотруднике, стандартную форму табеля за месяц;

– возможность регулирования уровня доступа к данным;

– поддержка мягких прогулов;

– поддержка свободного графика работы;

– поддержка запрета перехода через сутки;

– расчет отработанного времени по сложным графикам;

– подробно комментирует свои расчеты в протоколе работы;

– учитывает причины отсутствия сотрудников на работе;

– экспорт требуемых результатов работы в формат простого текста, HTML, Excel;

– цветовая подсветка цифр в отчётах;

– многооконный интерфейс.

Алгоритмы расчета основных дисциплинарных отчетов:

Пусть:

– T1 – время прихода на работу;

– T2 – время ухода с работы;

– TN – начало рабочего дня по графику;

– TK – конец рабочего дня по графику;

– R_In – допустимый интервал раннего прихода;

– P_In – допустимый интервал позднего прихода (опоздания);

– R_Out – допустимый интервал раннего ухода (ухода раньше окончания рабочего дня);

– P_Out – допустимый интервал позднего ухода.

Создаются следующие списки:

1. Список опоздавших. Делается выборка только входов сотрудника, начиная с [TN – 3 часа] до [TK]. Первая выбранная запись и есть T1. Если T1 > [TN + P_In], то этот сотрудник попадает в список опоздавших. P_In также может задаваться при настройке параметров отчета. Если для сотрудника введено отсутствие по уважительной причине на расчетный день, то он в отчет не попадает.

2. Список отсутствующих без уважительной причины. Делается выборка входов-выходов сотрудника, начиная с [TN – 4 часа] до [TK + 1 час]. Если выборка пустая (т.е. проходов не было), то сотрудник попадает в список отсутствующих. Иначе ищем последнюю запись в выборке. Если это выход до начала рабочего дня, то сотрудник попадает в список отсутствующих.

3. Список ушедших раньше окончания рабочего дня. Делается выборка входов-выходов сотрудника, начиная с [TN] до [TK + P_Out]. Для сотрудников, входящих в группу работающих за территорией предприятия, выборка делается с [TN – 2 часа] до [TK + 4 часа]. Если

выборка не пустая, ищем последнюю запись. Если это выход, то это и есть T2. Если T2 < [TK – R_Out], то сотрудник попадает в список ушедших раньше окончания рабочего дня. R_Out также может задаваться при настройке параметров отчета.

4. Список приходивших вне своего рабочего графика. Ищутся входы-выходы сотрудника в следующие периоды времени:

1) от начала календарного расчетного дня (или от окончания предыдущего рабочего дня, если это была ночная смена) до [TN – R_In];

2) от [TK + P_Out] до окончания календарного расчетного дня;

3) если для сотрудника введено отсутствие по уважительной причине на расчетный день, то за весь этот день.

Если входы-выходы в эти интервалы времени найдены, то сотрудник попадает в отчет.

Вопросы для самостоятельной работы

1. Назначение СКУД.
2. Состав и особенности построения СКУД.
3. Задачи, решаемые с использованием СКУД. Область применения СКУД.
4. Принцип действия СКУД.
5. Аутентификация.
6. Биометрическая идентификация.
7. Вещественный код.
8. Доступ.
9. Запоминаемый код.
10. Зона доступа.
11. Идентификатор доступа.
12. Идентификация.
13. Контроллер доступа.
14. Несанкционированный доступ.
15. Пользователь СКУД.
16. Правило двух (и более) лиц.
17. Правило двойной идентификации.
18. Правило Antipassback.
19. Правило NoOut.
20. Пропускная способность.
21. Устройства преграждающие управляемые.
22. Устройства исполнительные.
23. Устройство считывающее.
24. Перспективы развития СКУД.
25. Принцип организации учета рабочего времени с помощью СКУД.
26. Основные виды дисциплинарных отчетов, формируемых ПО СКУД при учете рабочего времени сотрудников.

ТЕМА 6
СИСТЕМЫ СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ

Учебные и воспитательные цели:

Образовательные: изучить назначение и особенности построения систем сбора и обработки информации в составе систем охранного мониторинга.

Развивающие: расширить базовые знания обучающихся в области системы сбора и обработки информации; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

6.1. Назначение и особенности построения систем сбора и обработки информации.

6.2. Классификация систем сбора и обработки информации.

6.3. Программное обеспечение систем сбора и обработки информации.

6.1. Назначение и особенности построения систем сбора и обработки информации

Система сбора и обработки информации (ССОИ) представляет собой аппаратно-программную систему, которая обеспечивает взаимодействие человека-оператора с объектовыми системами безопасности.

Средства обнаружения, размещенные на периметре, через шлейфы сигнализации передают информацию (тревожные сообщения, результаты контроля работоспособности СО и линий связи) на контроллеры, которые обеспечивают:

– прием информации от извещателей;

– контроль состояния шлейфов охранной сигнализации;

– контроль состояния линий связи с извещателями;

– передачу информации на решающее устройство.

Решающее устройство обеспечивает:

– идентификацию сигналов от СО;

– передачу тревожного сообщения на более высокий иерархический уровень;

– централизованное управление постановкой на охрану / снятием с охраны СО;

– управление внешними исполнительными устройствами;
– управление периферийными устройствами;
– контроль работоспособности СО;
– передачу информации на пульт оператора;
– управление документированием всей тревожной, обрабатываемой и командной информации в режиме реального времени.

Примерная функциональная схема ССОИ будет иметь вид, представленный на рис. 6.1.

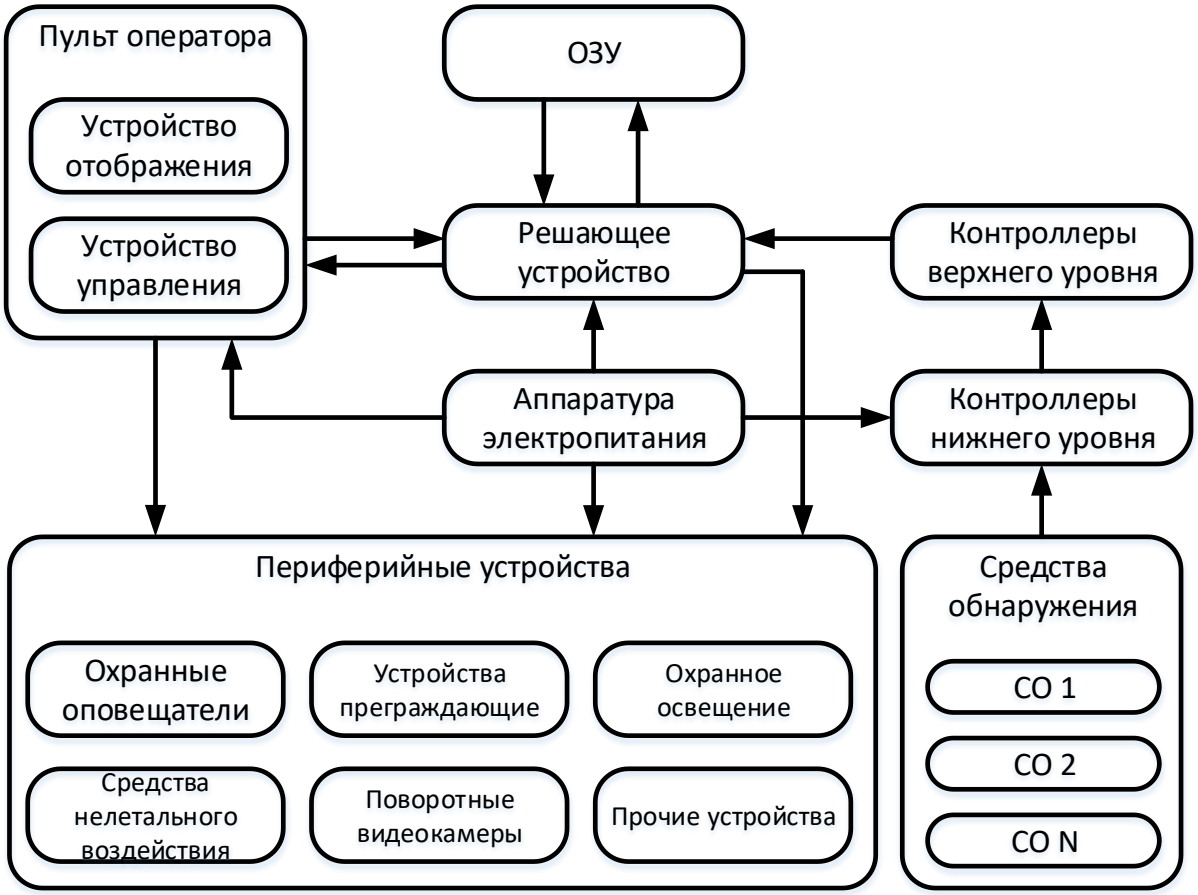


Рис. 6.1. Функциональная схема построения ССОИ

Устройство отображения информации обеспечивает графическое и звуковое отображение тревожной и вспомогательной информации.

Устройство управления позволяет оператору адекватно реагировать на отображаемую информацию и управлять работой извещателей, периферийных и исполнительных устройств.

Периферийная аппаратура обеспечивает:

– взаимодействие стационарной аппаратуры с извещателями через контроллеры нижнего уровня;

– информирование персонала (определенных категорий) через выносные сигнализаторы о поступлении тревожных и служебных сообщений;

– управление исполнительными устройствами через терминалы при потере связи со стационарной аппаратурой.

Аппаратура электропитания обеспечивает электропитание аппаратуры ССОИ, а в ряде случаев и СО.

6.2. Классификация систем сбора и обработки информации

Для классификации ССОИ могут применяться различные признаки, основными из которых являются:

1. Назначение.
2. Структура построения.
3. Энергообеспечение.
4. Степень защиты каналов сигнализации от несанкционированного внедрения.
5. Обеспечение контроля работоспособности аппаратуры.
6. Методы отображения информации.
7. Обеспечение регистрации информации.
8. Возможность управления исполнительными устройствами.
9. Возможность информационного обмена с другими системами (СКУД, СОТ и т.д.) с помощью стандартных интерфейсов.

Рассмотрим подробнее классификацию ССОИ по перечисленным выше признакам.

По назначению (рис. 6.2).

Назначение ССОИ определяется оперативно-тактическими задачами системы охраны, в которой она применяется.

Камуфлирование ССОИ предполагает маскировку стационарной пультовой аппаратуры под технические устройства бытового назначения.

Область применения ССОИ ориентирована на важность охраняемого объекта. Определение необходимых уровней защиты тесно связано с категорированием объектов. В настоящее время категорирование объектов проводится в соответствии с методическими рекомендациями Р 063-2017 «Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации».

Наивысшие категории объектов требуют высокого уровня оснащения техническими средствами охраны (ТСО):

– создания многорубежной охраны, включая ТСО, работающие на разных физических принципах;

– наличия развитой ССОИ;

– интеграции с системами СКУД, СОТ, СУЖ и т.д.;

– реализации функций автоматического определения направления движения нарушителя и т.д.

Рис. 6.2. Классификация ССОИ по назначению

Условия работы – условия, в которых функционирует ССОИ. Они включают в себя:

– климатические условия;

– уровень электромагнитных, акустических, вибрационных и других помех;

– воздействие флоры, фауны и т.д.

По структуре построения (рис. 6.3).

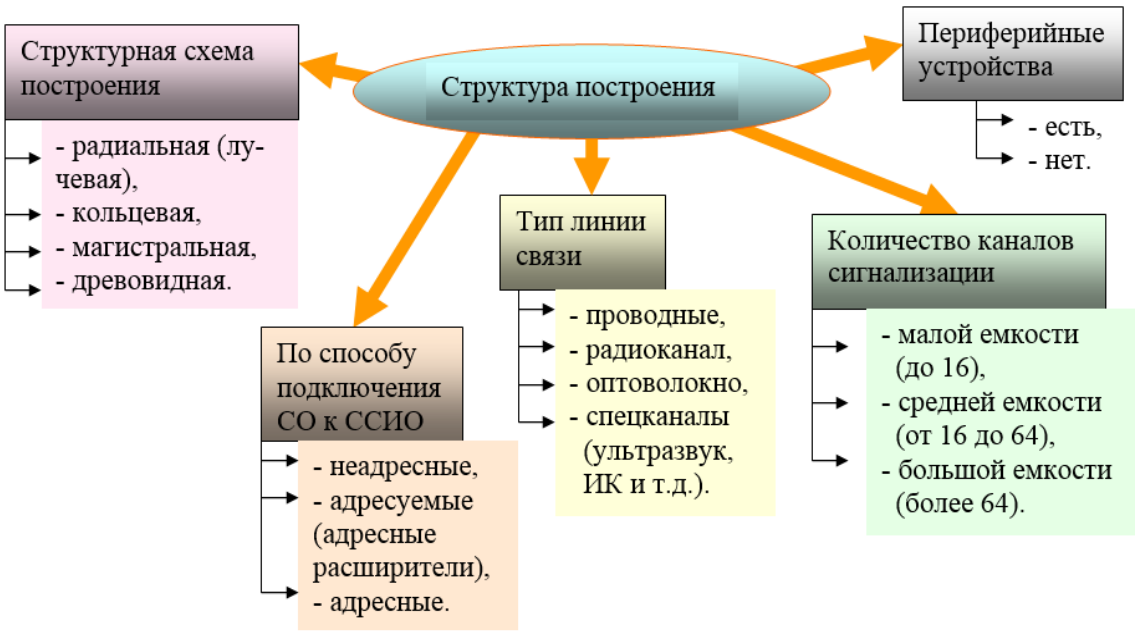


Рис. 6.3. Классификация ССОИ по структуре построения

В зависимости от структурной схемы построения ССОИ подразделяются на системы:

1. С радиальной (лучевой) структурой (рис. 6.4).
СО подключаются к ССОИ с помощью индивидуальных линий связи.

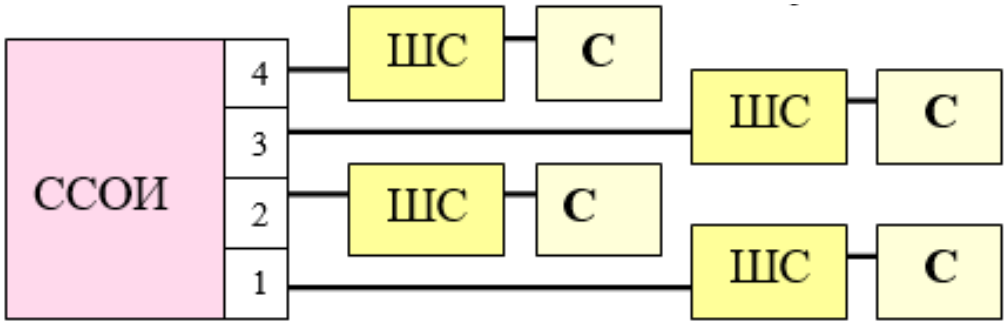


Рис. 6.4. ССОИ с радиальной (лучевой) структурой:
С – средства обнаружения охранной, пожарной, тревожной сигнализации

Каждое СО подключается к своему ШС. Каждый ШС подключается непосредственно к стационарной аппаратуре ССОИ.

2. С кольцевой (петлевой) структурой (рис. 6.5).

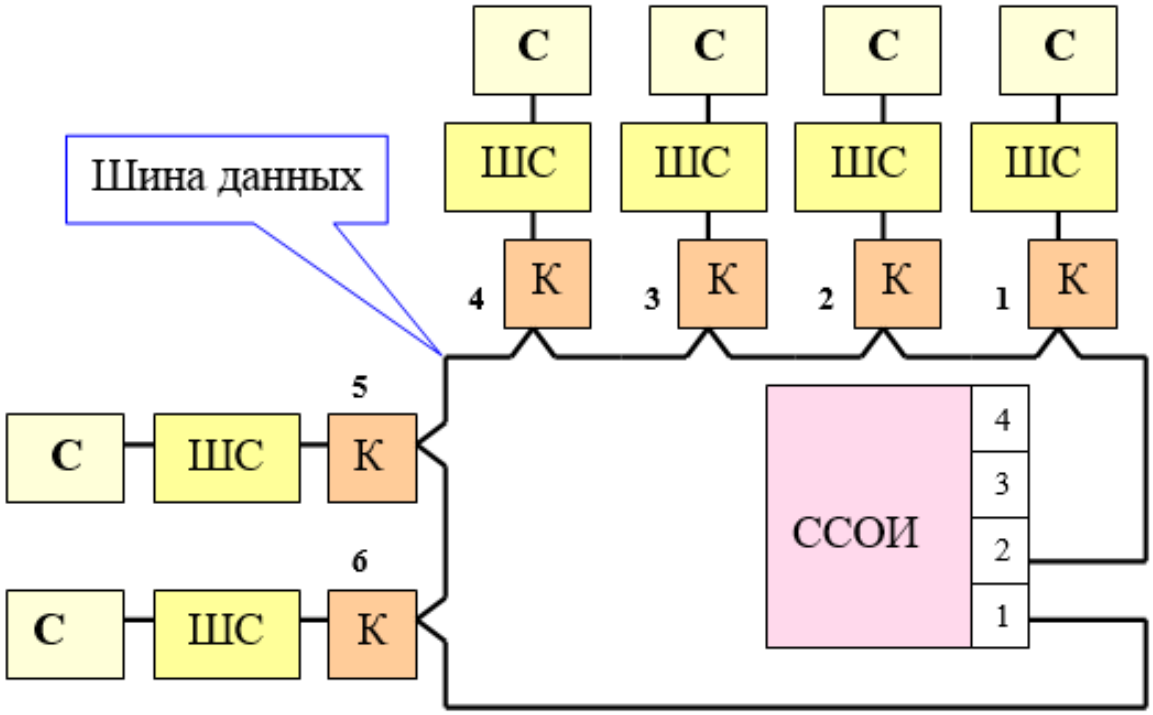


Рис. 6.5. ССОИ с кольцевой (петлевой) структурой:
С – средства обнаружения охранной, пожарной, тревожной сигнализации,
К – контроллер

В этом случае:
– каждое СО через свой ШС подключается к контроллеру;

– контроллер предназначен для подключения ШС со своими С к общей шине данных. В общем случае к контроллеру может подключаться несколько ШС со своими С. Каждый контроллер имеет свой адрес;

– шина данных имеет топологию кольца, замкнутого через соседние порты стационарной аппаратуры ССОИ.

Преимуществом кольцевой структуры ССОИ является сохранение работоспособности системы (получение информации от СО) при единичном обрыве общей шины данных.

Недостатком кольцевой структуры ССОИ можно считать сокращение информационной емкости системы за счет использования двух портов приемного устройства ССОИ для замыкания кольца.

3. С магистральной структурой (рис. 6.6).

В ССОИ с магистральной структурой контроллеры со своими ШС и СО подключаются к шине данных, имеющей топологию магистрали (линии). Один конец шины данных подключается к одному порту приемного устройства ССОИ, а другой к оконечному устройству – терминатору.

В отличие от кольцевой магистральная структура ССОИ позволяет в два раза повысить информационную емкость системы, но при этом обрыв шины данных приведет к потере информации от СО, расположенных между местом обрыва и терминатором.

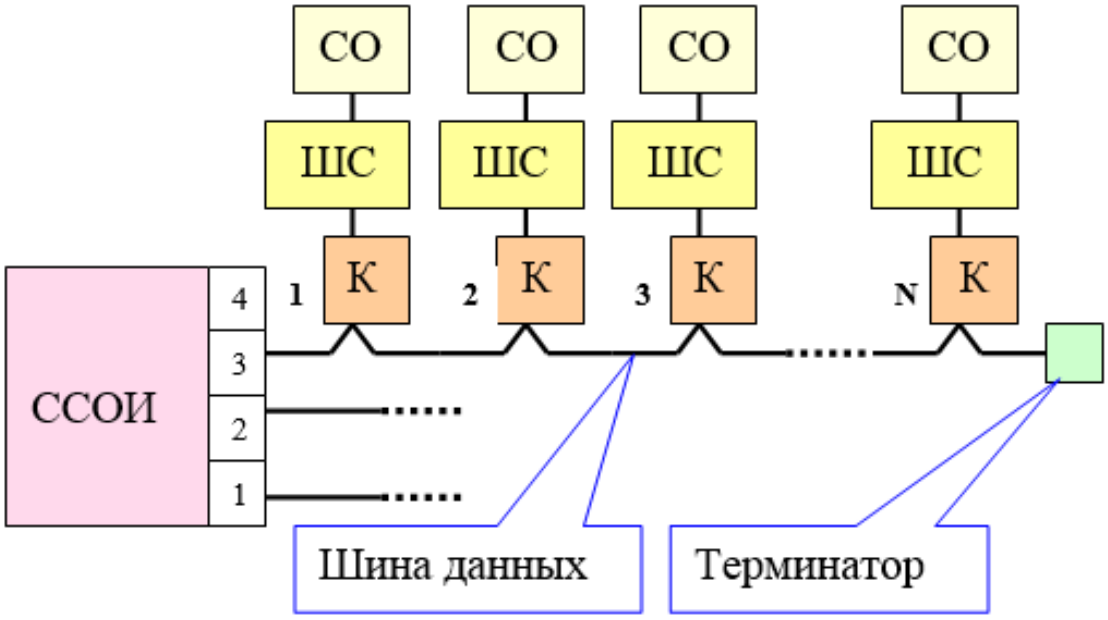


Рис. 6.6. ССОИ с магистральной структурой

4. С древовидной структурой (рис. 6.7).

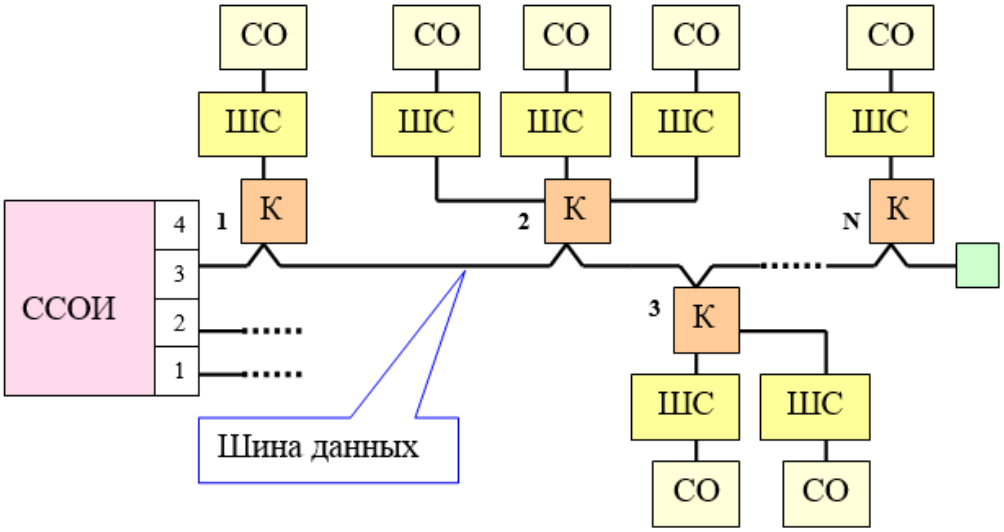


Рис. 6.7. ССОИ с древовидной структурой

Древовидную структуру ССОИ можно рассматривать как магистральную, в которой используются контроллеры, обеспечивающие возможность подключения сразу нескольких ШС со своими СО. При этом все СО, подключенные к одному шлейфу, будут иметь один адрес.

В зависимости от способа подключения СО к ССОИ подразделяются на системы:

1. Неадресные ССОИ.

В неадресных ССОИ используются:

– неадресные СО (извещатели);

– неадресные шлейфы сигнализации (ШС).

СО напрямую по неадресному ШС подключаются к приемному устройству ССОИ – прибору приемно-контрольному (ППК). При этом ППК различает место срабатывания СО (проникновения нарушителя) с точностью до ШС (до охраняемой зоны по ГОСТ Р 50775-95).

Неадресные шлейфы сигнализации (ШС) представляют собой четырехпроводные линии. По двум проводам подается питание на СО, а с помощью других двух проводов контролируется состояние «сухого контакта» СО на замыкание, обрыв (рис. 6.8) или «открытого коллектора» на изменение тока в цепи.

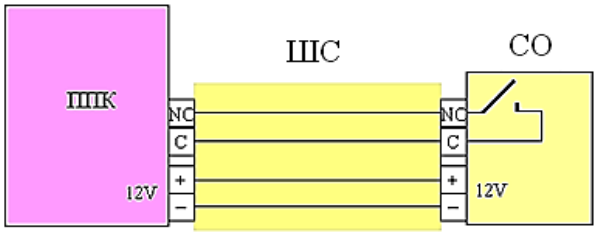


Рис. 6.8. Неадресный шлейф сигнализации

Неадресные ССОИ, как правило, имеют радиальную структуру и применяются на объектах низших категорий.

2. Адресуемые ССОИ (рис. 6.9).

В адресуемых ССОИ используются:

– неадресные СО;
– адресные ШС;
– контроллеры (адресные расширители);
– шина данных (обычно RS 485).

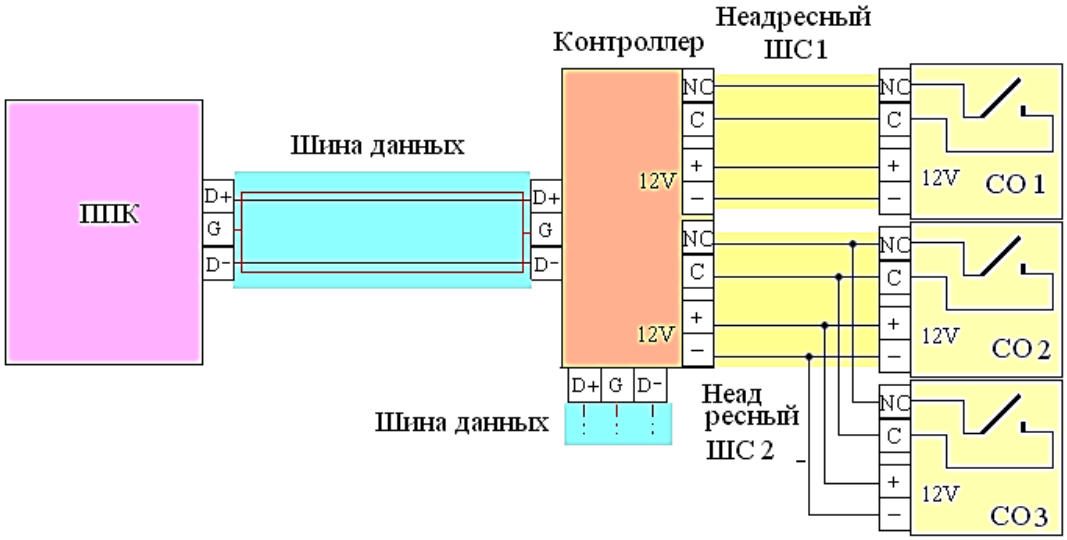


Рис. 6.9. Адресуемые ССОИ

В адресуемых системах используются неадресные извещатели, но они подключаются к ППК через контроллер (адресный расширитель). Адресный расширитель передает на ППК свой адрес и адреса подключенных к нему ШС. ППК фиксирует адрес контроллера и адрес ШС, в котором сработал любой подключенный к нему извещатель.

Таким образом ППК различает место срабатывания СО (проникновения нарушителя) с точностью до ШС.

3. Адресные ССОИ.

В адресных ССОИ используются:

– адресные СО (извещатели);
– адресные шлейфы сигнализации (ШС).

В адресных системах используются адресные извещатели, которые имеют свой собственный адрес и при срабатывании передают его по ШС на ППК. Таким образом, место срабатывания СО (проникновения нарушителя) определяется с точностью до извещателя.

Адресный ШС, основанный на технологии LSN, позволяет включить в себя до 127 адресных устройств:

– СО;

– модулей контроля и управления исполнительными устройствами;
– оповещателей;
– выносных клавиатур.

Адресные шлейфы сигнализации (ШС) представляют собой двухпроводные линии, по которым осуществляется питание СО и одновременно передается код адреса, информация о состоянии СО и команды управления.

Принцип технологии LSN поясняет рис. 6.10.

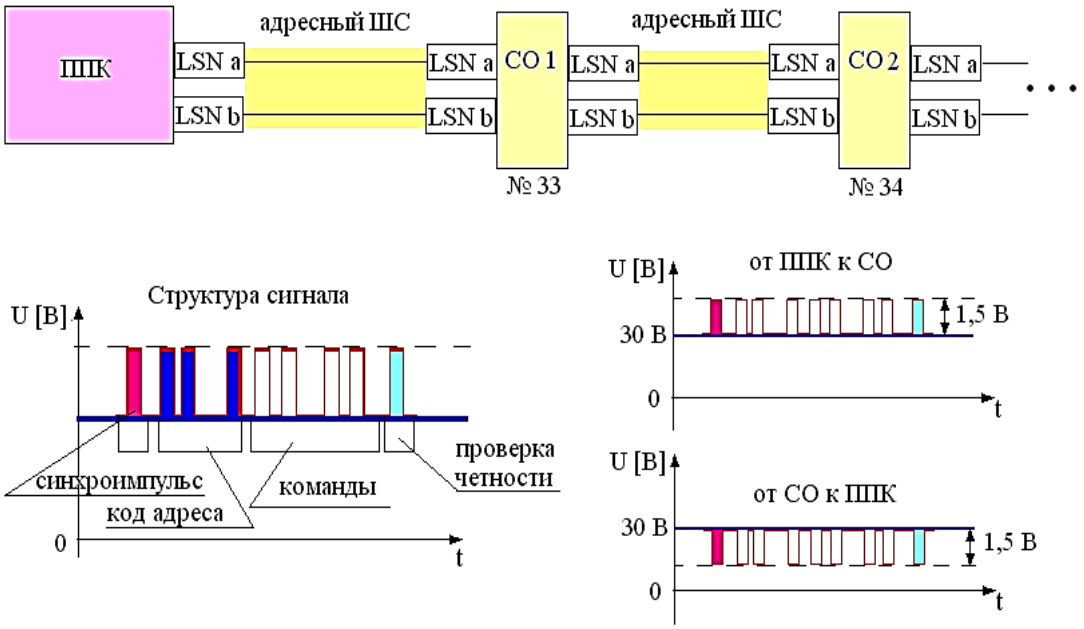


Рис. 6.10. Принцип технологии LSN

В зависимости от типа линии связи ССОИ подразделяются на системы:

– с проводными линиями связи;
– с радиоканалами связи;
– с оптоволоконными линиями связи;
– со специальными линиями связи (ультразвуковые, ИК и т.д.).

В качестве проводных линий связи используются:

– свободные (специально выделенные для передачи информации) линии связи;
– занятые линии связи:

– телефонные;
– электросеть;
– телевизионные кабели.

По занятым линиям связи полезная информация передается за счет использования методов модуляции ВЧ-несущей составляющей сигналов.

В зависимости от количества шлейфов сигнализации/адресов (от информационной емкости) ССОИ подразделяются на системы:

– малой информационной емкости – до 8 ШС (адресов);
– средней информационной емкости – от 9 до 64 ШС (адресов);
– большой информационной емкости – свыше 64 ШС (адресов).

По организации энергообеспечения (рис. 6.11).

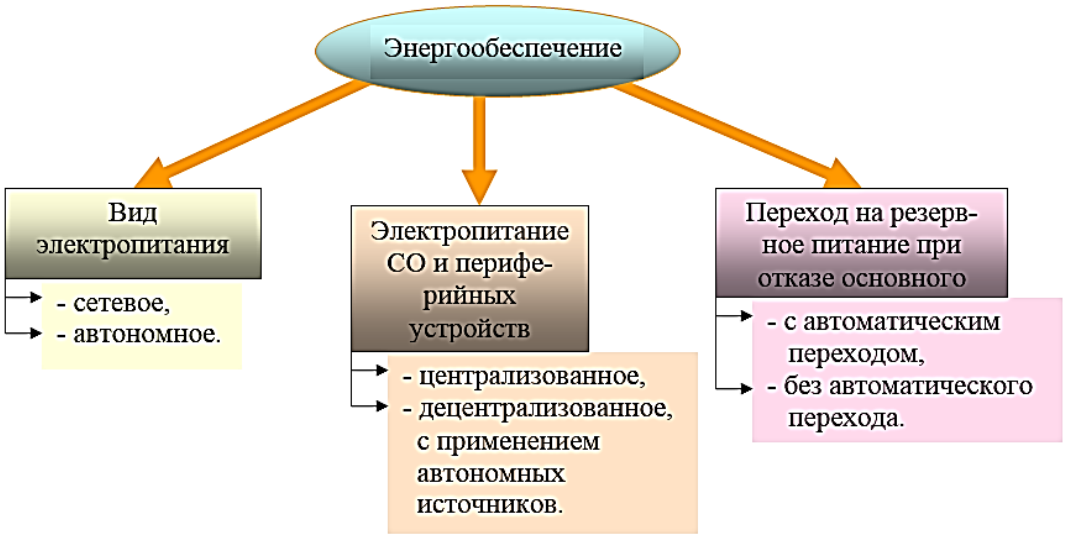


Рис. 6.11. Классификация ССОИ по организации энергообеспечения

По степени защиты каналов сигнализации от несанкционированного доступа (рис. 6.12).

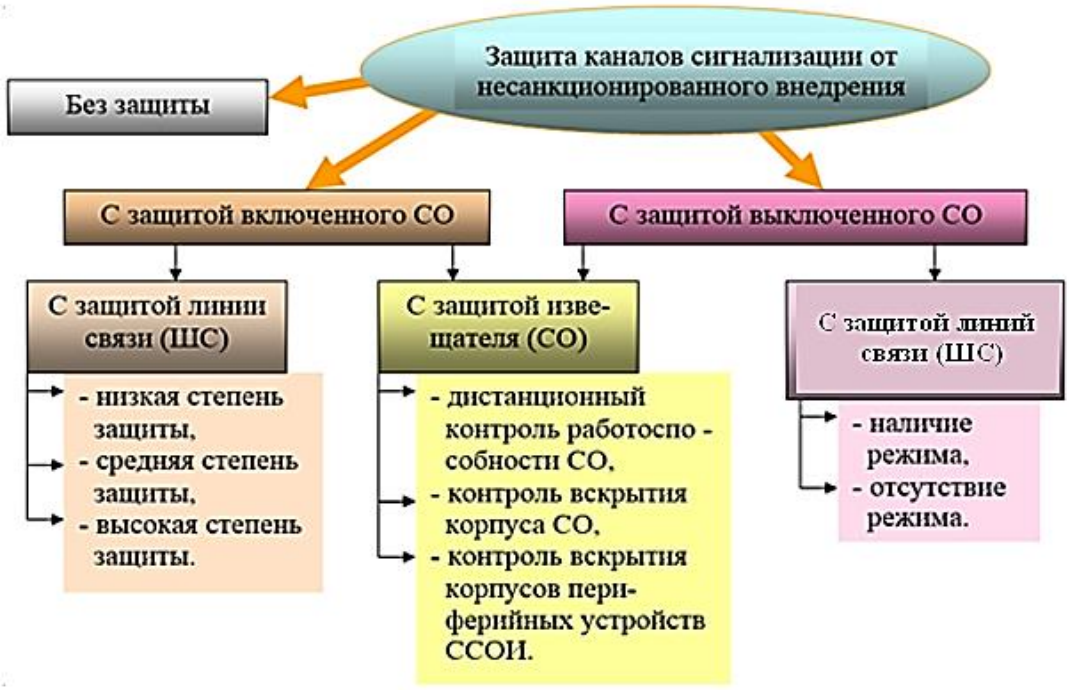


Рис. 6.12. Классификация ССОИ по степени защиты каналов сигнализации от несанкционированного доступа

В современных ССОИ наиболее подвержены несанкционированному доступу неадресные ШС. Подавляющее большинство СО, применяющихся в настоящее время, являются неадресными, поэтому задача защиты неадресных ШС от несанкционированного доступа имеет важное значение.

При включенном СО может защищаться само СО и (или) линия его связи с ССОИ (это в основном – ШС).

Защита шлейфа сигнализации при включенном СО.

1. Низкая степень защиты (рис. 6.13).

Такой способ защиты заключается в измерении общего сопротивления ШС и выходных цепей СО с установленными вблизи СО резисторами ($R_{изм}$). Это позволяет различать такие состояния, как норма, обрыв, короткое замыкание (КЗ) или тревога, но не позволяет отличить тревогу от короткого замыкания.

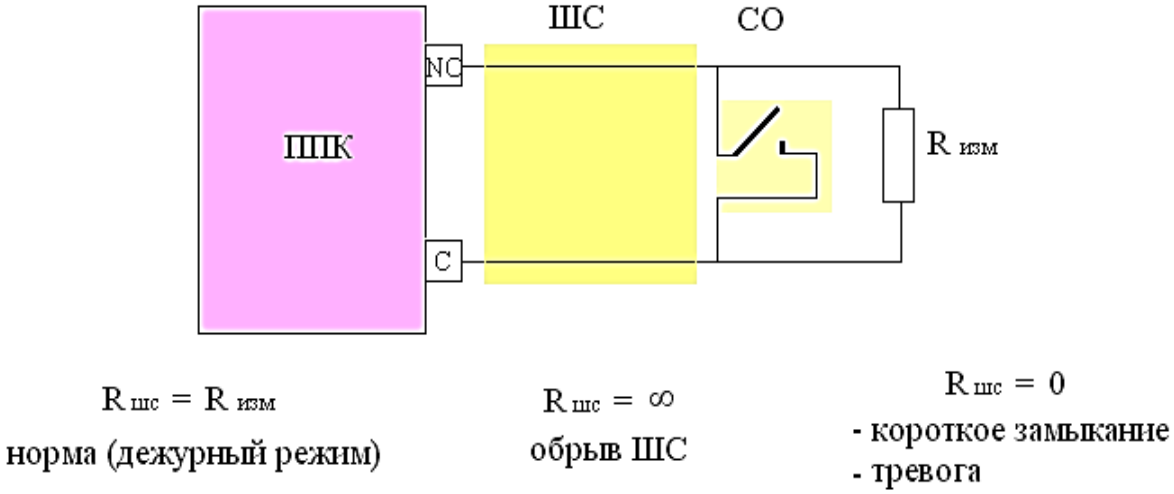


Рис. 6.13. Низкая степень защиты неадресного ШС

Подготовленный нарушитель способен легко подобрать и подсоединить резисторный имитатор к ШС, поэтому степень защиты невелика.

2. Средняя степень защиты (рис. 6.14).

Вместо активного измерительного резистора ($R_{изм}$), как в предыдущем случае, используется конденсатор ($C_{изм}$). Контроль состояния ШС осуществляется по анализу параметров импульсных сигналов, распространяющихся в шлейфе.

По степени защиты ШС от несанкционированного доступа данный способ идентичен предыдущему.

3. Высокая степень защиты (рис. 6.15).

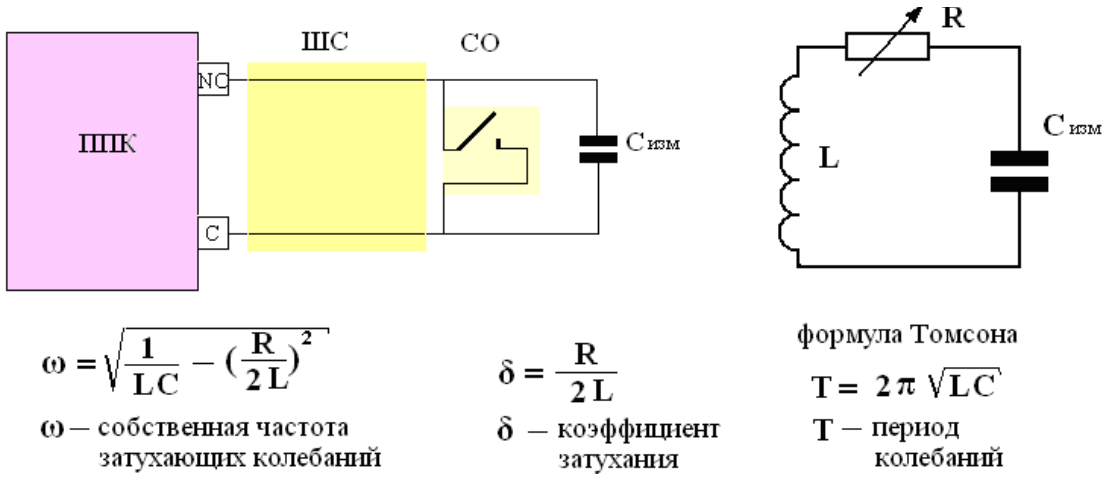


Рис. 6.14. Средняя степень защиты неадресного ШС

Наиболее высокую степень защиты ШС от несанкционированного внедрения обеспечивает метод генерирования в сигнализационной линии псевдослучайной последовательности импульсов. Она представляет собой периодически повторяющуюся (по определенному закону) последовательность импульсов, которая при исследовании ее статистическими методами способна передавать информацию о состоянии ШС и СО.

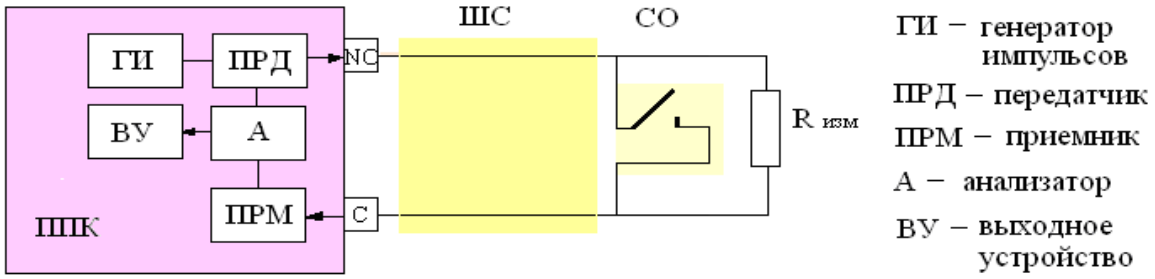


Рис. 6.15. Высокая степень защиты неадресного ШС

В этом случае в состав ППК должны дополнительно входить устройства, обеспечивающие техническую реализацию данного способа защиты.

Высокая степень защиты ШС от несанкционированного доступа обеспечивается практической невозможностью имитации нарушителем псевдослучайной последовательности импульсов.

Защита извещателя (СО).

Заключается в присущих многим ССОИ функциях:

а) дистанционного контроля работоспособности СО путем:

– передачи по ШС зондирующего сигнала на СО;

– приема от СО ответного сигнала;

– обработки ответного сигнала;

– принятия решения о работоспособности контролируемого СО;

б) контроля вскрытия корпуса СО;

в) контроля вскрытия корпусов периферийных устройств ССОИ (контроллеров, терминалов, ретрансляторов, шифроустройств и т.д.).

Защита извещателя (СО) практически во всех ССОИ осуществляется независимо от включенного или выключенного состояния извещателя.

Защита шлейфа сигнализации при выключенном СО.

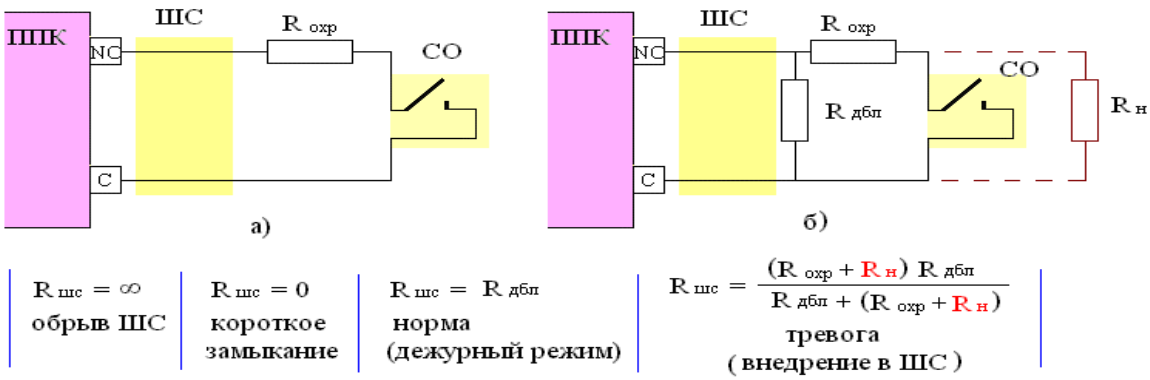
В зависимости от наличия или отсутствия в ССОИ режима контроля за состоянием соединительных линий канала сигнализации при снятом с охраны (выключенном) СО ССОИ делятся на системы:

– без режима «Деблокирование»;

– с режимом «Деблокирование».

Конкретный вариант технической реализации режима «Деблокирование» определяется особенностями той или иной ССОИ.

Простейший вариант реализации режима «Деблокирование» за счет подключения измерительного резистора $R_{дбл}$ приведен на рис. 6.16.



а) без режима «Деблокирование» б) с режимом «Деблокирование»

Рис. 6.16. Простейший вариант реализации режима «Деблокирование» за счет подключения измерительного резистора $R_{дбл}$

В схемах на рис. 6.16, а и 6.16, б при снятом с охраны СО контакты реле разомкнуты. В связи с этим контроль за состоянием ШС (рис. 6.16, а) не осуществляется и имеется возможность внедрения в линию. Вв схеме (рис. 6.16, б) контроль осуществляется с помощью измерительного резистора $R_{дбл}$ и любое воздействие на канал сигнализации (КЗ, обрыв, включение добавочного сопротивления $R_н$) приведет к изменению общего сопротивления линии $R_{шс}$, что вызовет сигнал тревоги.

Эта схема успешно работает и в случае постановки СО на охрану (рис. 6.17).

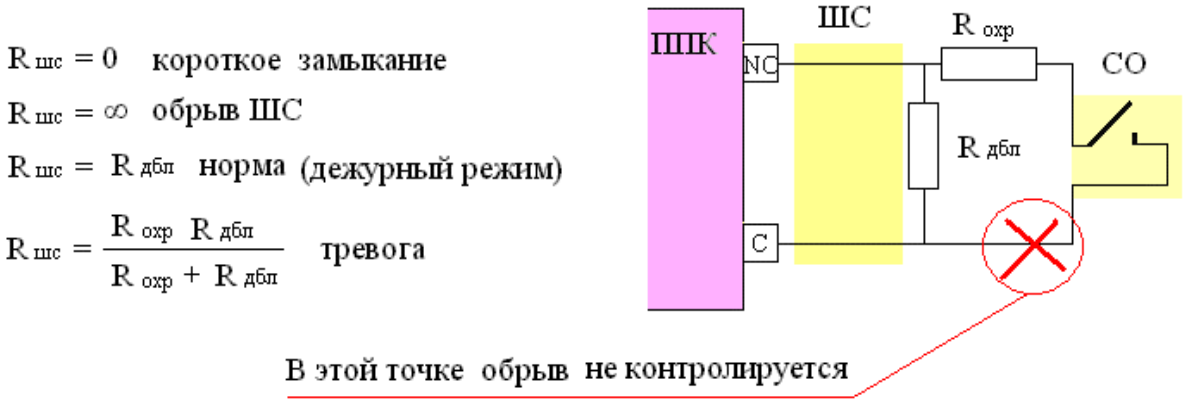


Рис. 6.17. Вариант реализации режима «Деблокирование» при постановке СО на охрану

Контроль работоспособности аппаратуры ССОИ в самом общем случае может быть:

1. Полным.

Проверяется работоспособность СО, соединительных линий и всей стационарной и периферийной части ССОИ.

2. Частичным.

Проверяется только выбранная (заданная) часть аппаратуры. Отсутствует контроль одного или более элементов из указанного выше ряда.

3. Автоматическим.

Осуществляется автоматическая поверка работоспособности элементов ССОИ. Автоматический контроль может быть:

– непрерывным,
– периодическим.

4. Автоматизированным.

Осуществляется по команде оператора.

Автоматический и автоматизированный контроль могут быть:

– с диагностикой причин неисправности,
– без диагностики причин неисправности.

Таким образом, классификация ССОИ по способам обеспечения контроля работоспособности аппаратуры будет иметь вид, представленный на рис. 6.18.

По методам отображения информации.

Под отображением информации в ССОИ понимается такое ее представление, которое обеспечивает наиболее удобное восприятие информации личным составом службы охраны (человеком-оператором).

Отображение информации может быть (рис. 6.19):

1. Визуальное:

а) вид визуальной информации:

– видеоизображение (с ВДД);

– графическое (план объекта на мониторе с указанием тревожного сектора (извещателя));

– индикационное;

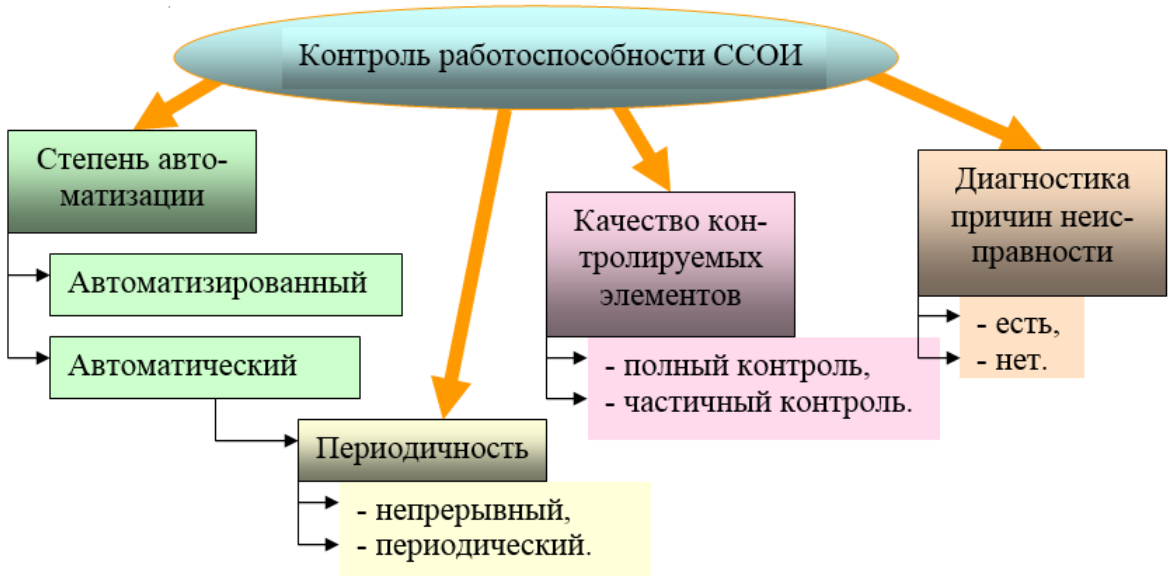


Рис. 6.18. Классификация ССОИ по способам обеспечения контроля работоспособности аппаратуры

б) степень детализации визуальной информации:

– интегральные сообщения. Дают представление о текущем состоянии различных компонентов системы. Они поступают в режиме реального времени. Например, это сообщения:

– о текущих режимах работы ССОИ;

– о состоянии каналов сигнализации;

– об исправности наиболее ответственных узлов и т.д.;

– детальные сообщения. Дают более полную оперативную информацию. Имеют последовательную форму отображения, т.е. информация выводится на мониторы (индикаторы) по мере ее поступления и отработки оператором. Например, кроме номера тревожного шлейфа сигнализации выводится наименование соответствующего объекта, его расположение и т.д.

2. Акустическое:

– тональное (сигналы);

– речевое.

3. Текстовое:

– на табло;

– на мониторе;
– на бумаге.
4. Тактильное (в редких случаях).

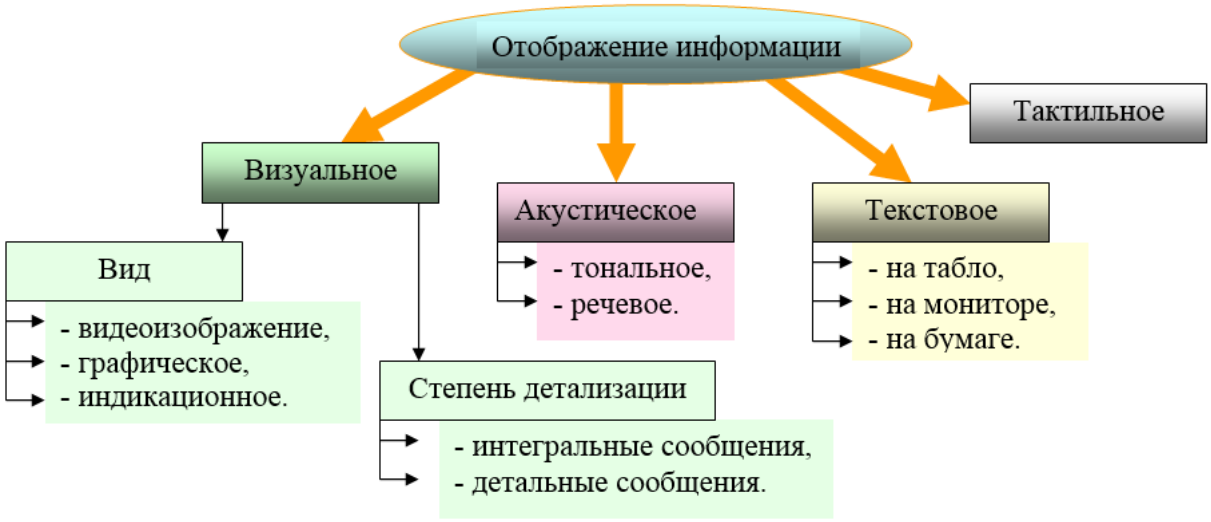


Рис. 6.19. Виды отображения информации

Устройства отображения информации должны отображать информацию (рис. 6.20):

а) о состоянии каналов в общей форме:
– номер канала;
– режим (включен, выключен);
– состояние (тревога);

б) о состоянии каналов в подробной форме:
– номер канала;
– номенклатуру контролируемых устройств (количество средств обнаружения, кнопки контроля, замки);
– состояние контролируемых устройств (тревога, норма, КЗ, обрыв ШС);

в) оперативные тревожные сигналы:
– номер канала;
– контролируемое СО, с которого поступает сигнал;
– направление движения нарушителя;

г) сигналы об изменении состояния аппаратуры в целом и отдельных ее блоков:
– переход на резервный источник питания;
– вкл. – откл. отдельных постовых пультов;
– неисправность отдельных блоков;

д) сигналы, выводимые из памяти;

е) текущее время и дату.

Тревожные сигналы и сигналы об изменении состояния аппаратуры должны иметь приоритет над остальными сигналами.

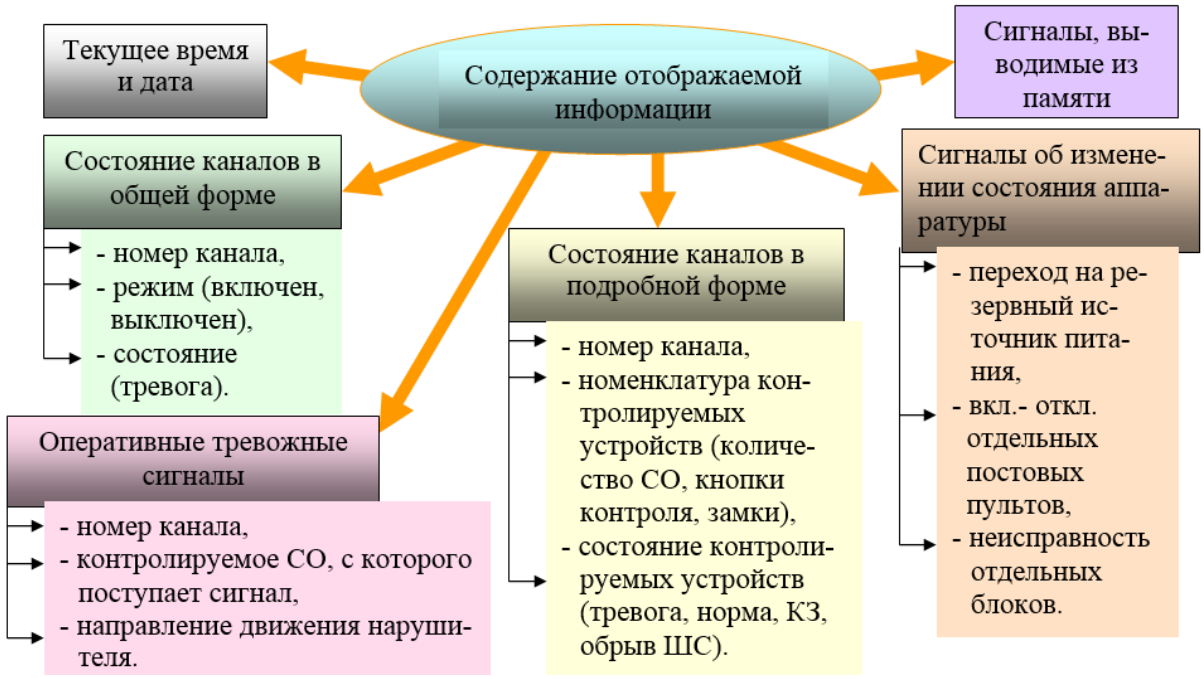


Рис. 6.20. Содержание отображаемой информации

Устройства отображения информации по способу представления информации подразделяются на следующие типы:

1. Точечные. Выполнены на светодиодах.

2. Цифровые. Выполнены на цифровых многоразрядных вакуумных люминесцентных индикаторах.

3. Знаковые. Выполнены на знакосинтезирующих вакуумных люминесцентных индикаторах.

Информация представляется в буквенно-цифровом виде, удобном для восприятия. Однако небольшое количество знакомест в одном индикаторе ограничивает сервисные возможности.

4. Знакографические. Выполнены на цветных и черно-белых видеоконтрольных устройствах (ВКУ). По методам отображения информации ССОИ делятся на системы:

– с параллельным отображением информации;

– с последовательным отображением информации;

– с комбинированным отображением информации.

По обеспечению регистрации информации (рис. 6.21).

ССОИ разделяются по возможности хранения и документирования оперативной информации.

Документирование (распечатка оперативной информации на бумаге) может осуществляться в трех режимах:

– в режиме реального времени (по приходе информации);

– распечатка содержимого ОЗУ/базы данных (при наличии в составе ССОИ ОЗУ);

– распечатка в режиме реального времени с возможностью распечатки содержимого ОЗУ/базы данных с ПЭВМ.

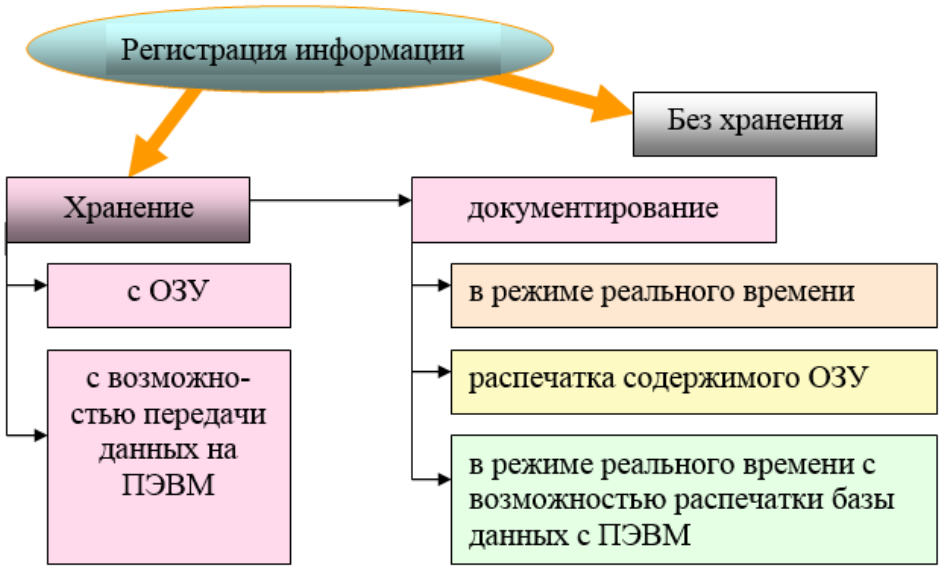


Рис. 6.21. Классификация ССОИ по обеспечению регистрации информации

По возможности (организации) управления исполнительными устройствами.

ССОИ могут управлять исполнительными устройствами. Исполнительные устройства могут быть:

– индивидуальные (для каждого канала, СО, зоны);

– общие (для всех каналов).

Кроме того, исполнительные устройства могут управляться:

– в автоматическом режиме (включаются без участия оператора по заранее заданным сигналам от определенных СО);

– в ручном режиме (включаются оператором);

– в комбинированном режиме (часть исполнительных устройств включаются автоматически и часть – в ручном режиме).

По возможности информационного обмена с другими системами.

Практически все современные ССОИ предполагают наличие информационного обмена с системами охранной безопасности (СКУД, СОТ, СОТС, СПС, СУЖ). Это позволяет создать интегрированные

системы безопасности. Для обмена данных в них используются, как правило, стандартные интерфейсы (RS-232 и RS-485), поскольку это обеспечивает возможность легкой интеграции систем различного назначения.

6.3. Программное обеспечение систем сбора и обработки информации

Программное обеспечение (ПО) ССОИ, как правило, состоит из двух частей: универсального и специализированного.

Универсальное ПО представляет собой программную среду, в которой формируется специализированное ПО. В качестве универсального ПО часто используется среда Windows.

Специализированное ПО обеспечивает:

1. Конфигурирование системы: состав, связи, режим работы технических средств и их размещение на графических планах.

2. Ведение базы данных абонентов, операторов рабочих мест, работу с архивом сообщений, формирование и печать отчетов.

3. Обмен информацией с контроллерами, управление периферийной аппаратурой, архив сообщений, взаимодействие с внешними системами: СОТ, СКУД, СУЖ, СОТС, СПС и др.

4. Обмен по сети Ethernet между сервером и автоматизированными рабочими местами (АРМ) ССОИ.

5. Изготовление пропусков на основе Prox-карт, печать учетных карточек о пропусках.

6. Формирование отчетов о состоянии трудовой дисциплины и табелей учета использования рабочего времени.

В качестве системы управления базами данных (СУБД) обычно используется SQL-сервер (Interbase, Microsoft SQL, Oracle и др.). Такое решение обеспечивает высокий уровень защищенности информации, хорошие возможности по интеграции системы в автоматизированные системы управления более высокого уровня.

Модульный принцип построения программного обеспечения позволяет создавать АРМ с заданной функциональностью за счет инсталляции соответствующих модулей. Для повышения уровня защиты от несанкционированных действий на каждом АРМ может устанавливаться соответствующий аппаратно-программный комплекс типа SecretNet.

Структура программного обеспечения ССОИ ИСБ представлена на рис. 6.22.

Программное обеспечение ССОИ обычно включает следующие модули:

– программный модуль «Сеть», обеспечивающий межмашинный обмен пакетами данных с использованием протокола TCP/ IP;

– программный модуль «Конфигуратор», обеспечивающий настройку и конфигурирование аппаратуры системы;

– программный модуль «Администратор», обеспечивающий ввод и редактирование информации, необходимой для управления доступом, передачу этой информации на сервер, накопление в архиве и выдачу из него сообщений, формируемых в системе, и печать отчетов на принтере;

– программный модуль «Табельный учет», обеспечивающий ведение автоматизированного табельного учета рабочего времени на предприятии;

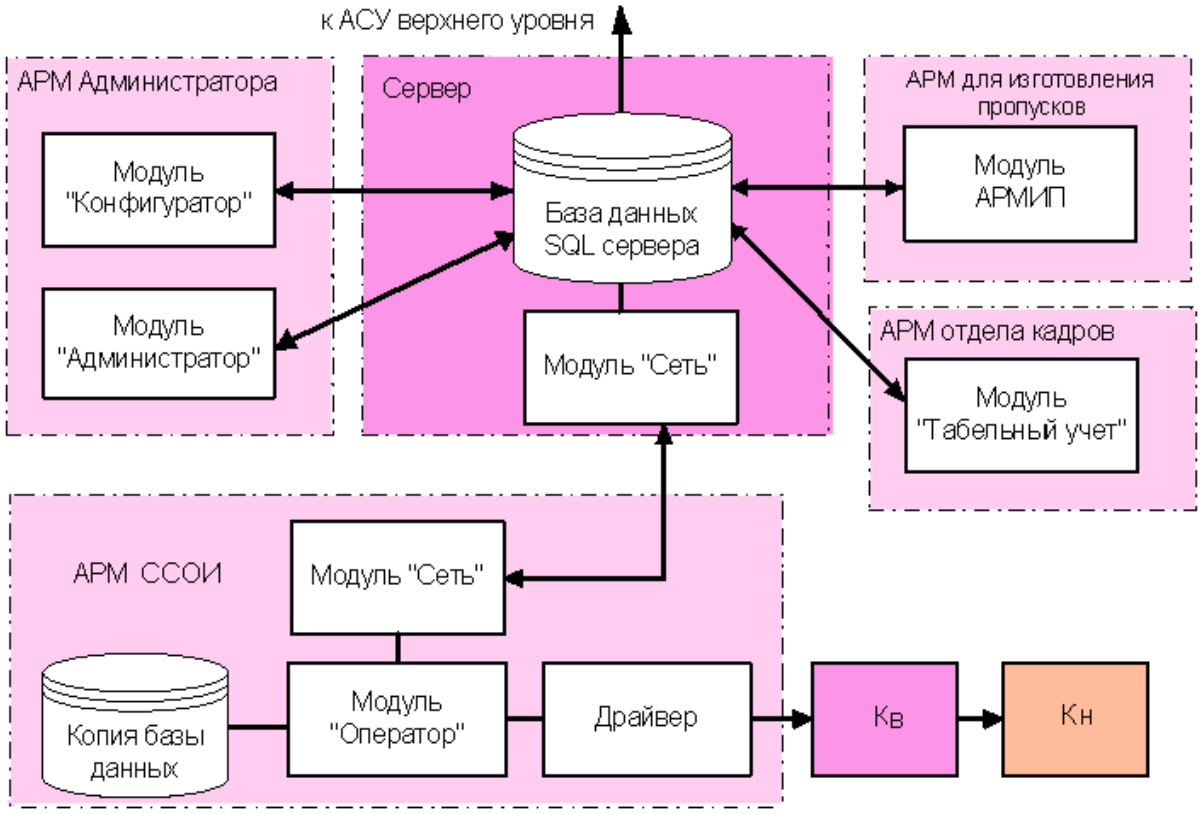


Рис. 6.22. Структура программного обеспечения ССОИ

– программный модуль «АРМИП», обеспечивающий изготовление электронных пропусков;

– программный модуль «Оператор», обеспечивающий ведение оперативного контроля за ситуацией на охраняемом объекте и управления всеми подсистемами в ИСБ;

– драйвер, обеспечивающий обмен данными между модулем «Оператор» и контроллерами.

Модуль «Конфигуратор» обеспечивает:

– ведение списка АРМ с указанием сетевых адресов;

– ведение списка зон, контролируемых системой;

– описание аппаратной структуры системы с заданием системных адресов, зон размещения, режимов работы технических средств;

– ведение списка точек доступа с установкой параметров, определяющих алгоритм прохода;

– размещение технических средств на графических планах объекта и формирование иерархии графических планов объекта.

Модуль «Администратор» обеспечивает:

– ведение базы данных абонентов;

– ведение списка операторов системы с заданием полномочий по доступу к информации;

– ведение списков «вскрывающих»;

– формирование графиков работы;

– рассылку на АРМ операторов изменений в базе данных абонентов, списке операторов, списках «вскрывающих»;

– формирование и печать отчетов о работе системы по архиву сообщений;

– синхронизацию времени по всем АРМ;

– создание резервных копий базы данных и архива сообщений за заданный период.

Модуль «Сеть» обеспечивает:

– двухсторонний обмен информацией между сервером и АРМ операторов;

– отображение состояний каналов обмена между сервером и АРМ операторов.

Модуль «Оператор» обеспечивает:

– обмен информацией в реальном времени с контроллерами и терминалами;

– отображение состояния технических средств периферийной аппаратуры;

– меню для подачи команд управления на технические средства;

– регистрацию всех сообщений от периферийной аппаратуры и команд оператора в суточном архиве сообщений;

– рассылку информации о проходах абонентов на другие АРМ операторов для обеспечения функции antipassback;

– автоматический вывод фото абонентов на монитор при проходах через КПП или точки доступа с видеоверификацией;

– автоматический контроль работоспособности технических средств.

Модуль «АРМИП» (рабочее место изготовления пропусков) обеспечивает:

– ввод персональных данных абонентов;

– разработку макетов пропусков;

– ввод фото абонентов с использованием цифрового фотоаппарата или сканера;

– печать пропусков на пластиковые Prox-карты с использованием специализированного принтера;

– печать карточек учета выдачи пропусков;

– утверждение в электронном виде изготовленных пропусков для разрешения использования в системе.

Модуль «Табельный учет» обеспечивает:

– формирование и печать за заданный период отчетов по сотрудникам с указанием общего времени работы, времени присутствия в любой из контролируемых зон, опоздания на работу, ухода с работы ранее запланированного времени;

– формирование и печать интегральных показателей состояния трудовой дисциплины (количество опоздавших, количество отсутствующих, количество ушедших раньше с работы) в разрезе подразделений;

– формирование табеля учета использования рабочего времени;

– экспорт табеля учета использования рабочего времени в текстовый формат с использованием ANSI-кодировки.

Из вышесказанного видно, что решение основных задач по обеспечению функционирования ИСБ обеспечивает модуль «Оператор» за счет выполнения функций:

– обмена информацией в реальном времени с контроллерами и терминалами;

– отображения состояния технических средств периферийной аппаратуры;

– подачи команд управления на технические средства;

– регистрации всех сообщений от периферийной аппаратуры и команд оператора в суточном архиве сообщений.

Для обеспечения этого выполняется программирование контроллеров верхнего и нижнего уровня. В процессе программирования указываются:

1. Для контроллеров верхнего уровня:

– адресация контроллеров верхнего уровня;

– порядок опроса контроллеров верхнего уровня;

– перечень команд, выполняемых непосредственно контроллерами верхнего уровня, как реакция на события, возникающие на шлейфах СО

(команды идентификации и автоматической загрузки определенных логических функций);

– удобный (понятный для оператора) интерфейс информационного обмена между контроллером верхнего уровня и модулем «Оператор».

2. Для контроллеров нижнего уровня:

– адресация контроллеров нижнего уровня;

– порядок опроса контроллеров нижнего уровня;

– конфигурация контроллеров нижнего уровня;

– перечень команд, выполняемых непосредственно контроллерами нижнего уровня, как реакция на события, возникающие на шлейфах СО и линиях связи (команды идентификации и автоматической загрузки определенных логических функций);

– генерирование команд, выполняемых контроллерами нижнего уровня в автономном режиме (дистанционный контроль СО и ШС).

При построении системы сбора и обработки информации (ССОИ) в составе ИСБ необходимы знания в области построения компьютерных сетей передачи данных.

Вопросы для самостоятельной работы

1. Назначение ССОИ.
2. Основные функции ССОИ.
3. Основные требования к дежурно-диспетчерским подсистемам ИСБ.
4. Классификация ССОИ.
5. Классификация ССОИ в ИСБ по назначению.
6. Классификация ССОИ в ИСБ по структуре построения.
7. Классификация ССОИ в ИСБ по энергообеспечению.
8. Классификация ССОИ в ИСБ по степени защиты каналов сигнализации от НСД.
9. Классификация ССОИ в ИСБ по методу отображения информации, а также по обеспечению регистрации информации.
10. Назначение и состав программного обеспечения ССОИ в ИСБ.

ТЕМА 7
СИСТЕМЫ МОНИТОРИНГА ПОДВИЖНЫХ ОБЪЕКТОВ

Учебные и воспитательные цели:

Образовательные: изучить назначение и особенности построения систем мониторинга подвижных объектов.

Развивающие: расширить базовые знания обучающихся в области тактики применения систем мониторинга подвижных объектов; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог.

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

7.1. Понятие и задачи, решаемые системами мониторинга подвижных объектов.

7.2. Структура систем мониторинга подвижных объектов и назначение элементов.

7.3 Этапы развития систем мониторинга подвижных объектов.

7.1. Понятие и задачи, решаемые системами мониторинга подвижных объектов

Спутниковый мониторинг подвижных объектов (МПО) (транспортных средств – ТС) осуществляется с помощью систем мониторинга подвижных объектов (СМПО), построенных на основе аппаратуры спутниковой навигации, оборудования и технологий сотовой и/или радиосвязи, вычислительной техники и цифровых карт.

Спутниковый МПО используется для решения задач транспортной логистики в системах управления перевозками и автоматизированных системах управления автопарком.

Принцип работы заключается в отслеживании и анализе пространственных и временных координат транспортного средства. Существует два варианта мониторинга: on-line – с дистанционной передачей координатной информации и off-line – информация считывается по прибытии на диспетчерский пункт.

На транспортном средстве устанавливается мобильный модуль, состоящий из следующих частей: приёмник спутниковых сигналов, модули хранения и передачи координатных данных. Программное обеспечение мобильного модуля получает координатные данные от

приёмника сигналов, записывает их в модуль хранения и по возможности передаёт посредством модуля передачи.

Модуль передачи позволяет передавать данные, используя беспроводные сети операторов мобильной связи. Полученные данные анализируются и выдаются диспетчеру в текстовом виде или с использованием картографической информации.

В off-line варианте необходимость дистанционной передачи данных отсутствует. Это позволяет использовать более дешёвые мобильные модули и отказаться от услуг операторов мобильной связи.

Мобильный модуль может быть построен на основе приёмников спутникового сигнала, работающих в стандартах NAVSTAR GPS или ГЛОНАСС. В настоящее время в России на государственном уровне активно продвигается использование сигналов спутников ГЛОНАСС, разработка и производство клиентского оборудования мониторинга для этой системы. Принят ряд законодательных актов, которые форсируют внедрение ГЛОНАСС и ограничивают применение других систем. При этом, в сравнении с NAVSTAR GPS, система ГЛОНАСС пока работает менее надёжно и в совокупности с наземным оборудованием даёт большую погрешность вычисления местоположения абонента. В настоящее время клиентское оборудование ГЛОНАСС стоит дороже, имеет большие размеры и худшие параметры энергопотребления, представлено на рынке не так широко, как GPS. Этим объясняется сложность внедрения ГЛОНАСС-мониторинга в жизнедеятельность всего общества и вынужденное его использование государственными предприятиями России, особенно МВД России и другими силовыми структурами.

Для повышения надежности в России разрабатываются и внедряются мобильные модули с комбинацией приемников NAVSTAR GPS и ГЛОНАСС.

Задачи, решаемые СМПО.

Системы спутникового МПО решают следующие задачи:

– мониторинг включает определение координат местоположения транспортного средства, его направления, скорости движения и других параметров: расход топлива, температура в рефрижераторе и др. Системы спутникового мониторинга транспорта помогают водителю в навигации при передвижении в незнакомых районах;

– контроль соблюдения графика движения – учет передвижения транспортных средств, автоматический учет доставки опасных и ценных грузов в заданные точки и др.;

– сбор статистки и оптимизация маршрутов – анализ пройденных маршрутов, скоростного режима, расхода топлива и др. транспортных средств с целью определения лучших маршрутов;

– обеспечение безопасности – возможность определения местоположения помогает обнаружить угнанный автомобиль. В случае

аварии система спутникового мониторинга помогает передать сигнал о бедствии в службы спасения. С помощью подключенных датчиков появляется возможность передачи тревожного сообщения о нападении преступников на диспетчерский центр. Также на основе спутникового МПО действуют некоторые системы автосигнализации.

Использование систем спутникового МПО повышает качество и эффективность работы корпоративного транспорта, и в среднем на 20 – 25% снижает расходы на топливо и содержание автопарка.

7.2. Структура систем мониторинга подвижных объектов и назначение элементов

Обобщенная структура СМПО представлена на рис. 7.1.

СМПО включает следующие элементы:

– GPS или ГЛОНАСС контроллер или трекер (абонентское устройство), установленный на транспортном средстве, который получает данные от спутников и передаёт их на серверный центр мониторинга (диспетчерский центр – ДЦ) посредством GSM, CDMA или реже спутниковой и УКВ связи. Последние два актуальны для мониторинга в местах, где отсутствует полноценное GSM-покрытие, таких как Сибирь или Дальний Восток;

– серверный центр (ДЦ) с программным обеспечением для приёма, хранения, обработки и анализа данных;

– компьютер диспетчера, ведущего мониторинг автомобилей (клиентское рабочее место).

Большинство ГЛОНАСС/GPS контроллеров и трекеров (абонентских устройств) имеют схожие функциональные возможности:

– вычислять собственное местоположение, скорость и направление движения на основании сигналов спутников систем глобального позиционирования ГЛОНАСС/GPS;

– подключать внешние датчики через аналоговые или цифровые входы;

– считывать данные с бортового оборудования, имеющего последовательный порт или более специализированный интерфейс CAN;

– хранить некоторый объём данных во внутренней памяти на период отсутствия связи;

– передавать полученные данные на серверный центр (ДЦ), где происходит их обработка.

Ранее по причине слабого охвата территорий сетями мобильной связи GSM/3G широко использовались контроллеры, которые накапливали данные во внутренней памяти. По возвращении объекта в место основной дислокации (автопарк) данные переносились на сервер по проводным каналам либо через Bluetooth или Wi-Fi. Многие из существующих

ГЛОНАСС/GPS трекеров и контроллеров имеют открытый протокол взаимодействия с сервером.

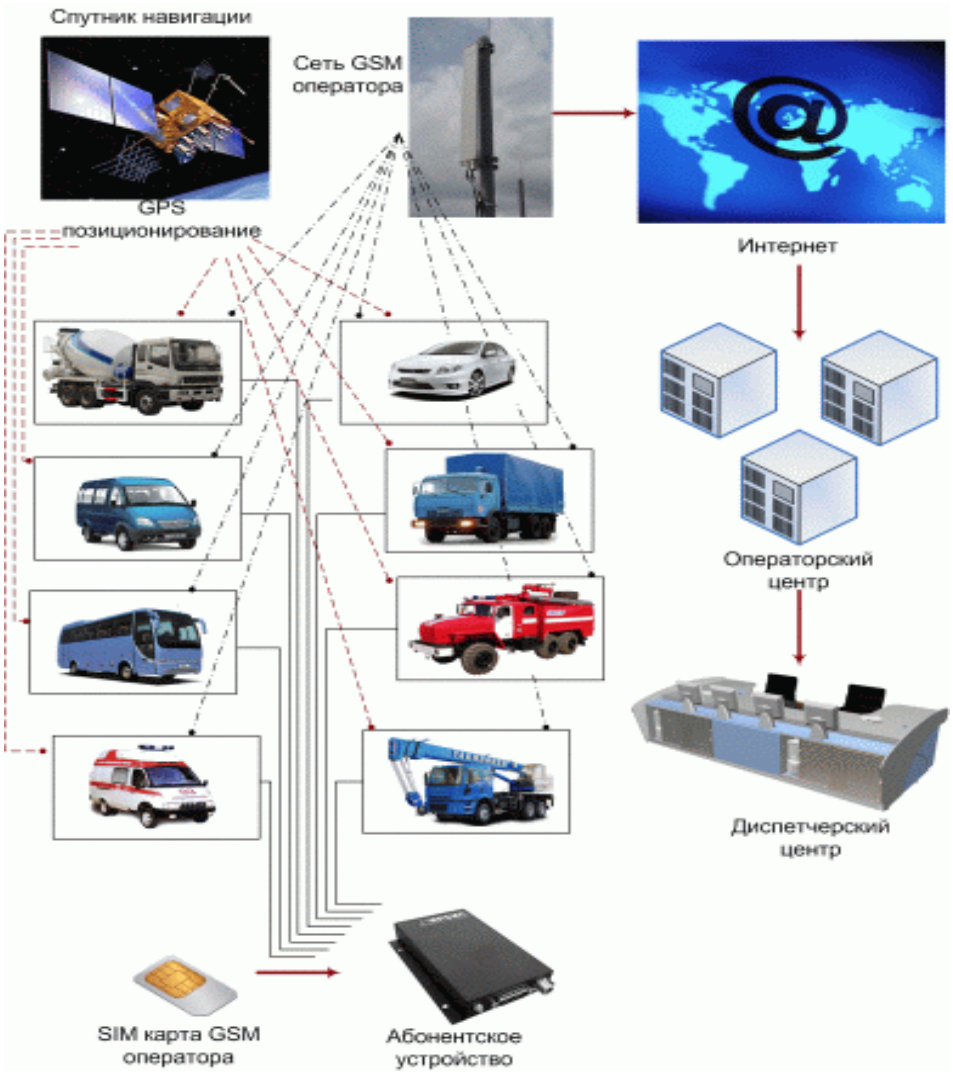


Рис. 7.1. Обобщенная структурная схема СМПО

Датчики.

Для получения дополнительной информации на транспортное средство устанавливаются дополнительные датчики, подключаемые к ГЛОНАСС/GPS контроллеру, например:

- датчик охранный;
- тревожная кнопка;
- датчик расхода топлива;
- датчик нагрузки на оси ТС;
- датчик уровня топлива в баке;
- датчик температуры в рефрижераторе;

– датчики, фиксирующие факт работы или простоя спецмеханизмов (поворот стрелы крана, работы бетоносмесителя), факт открывания двери или капота, факт наличия пассажира (такси).

Полученные данные могут либо накапливаться в локальном устройстве и затем переноситься в центральную базу по возвращении в парк, либо передаваться на ДЦ в режиме реального времени, обычно по каналам сотовой связи.

Датчики и трекер могут устанавливаться на транспортном средстве скрытым образом.

Программное обеспечение.

Самым существенным различием многих СМПО, представленных на рынке, является функциональность серверного и клиентского программного обеспечения, возможность разносторонне обрабатывать данные, генерировать отчёты.

Функции серверного центра может выполнять как обычный компьютер с установленным программным обеспечением для простых систем мониторинга, так и распределённая серверная система с использованием нескольких серверов, выполняющих разные задачи, способная вести одновременный мониторинг десятков тысяч ТС и обеспечивать подключение к ДЦ нескольких тысяч пользователей (диспетчеров) одновременно.

Диспетчерское программное обеспечение для спутникового мониторинга автомобилей можно условно разделить на несколько типов:

– ПО, содержащее все компоненты, включая карты и базу данных движения объектов на единственном компьютере;

– ПО, имеющее клиентскую часть, которая устанавливается на компьютеры диспетчеров;

– ПО, использующее web-интерфейс, что позволяет избежать установки каких-либо специальных компонентов и вести мониторинг с любого компьютера, подключённого к интернету.

Разновидностью последнего варианта является ПО, использующее трёхуровневую архитектуру, когда компоненты и функции центра обработки данных распределены между несколькими серверами: базы данных, картографической подсистемы, телекоммуникационным сервером и сервером приложения, обеспечивающего работу web-интерфейса пользователя.

В то время как первый и второй типы систем остаются надёжным решением для специальных применений, где использование каналов интернета невозможно из-за низкого качества «последней мили» или запрещено нормативными актами, последний тип систем имеет ряд преимуществ и позволяет компаниям-операторам увеличить охват рынка, ускорить внедрение мониторинга, переводя его в разряд платной услуги. Большинство производителей современных СМПО включают в свои

продукты возможность работы диспетчеров через web-интерфейс и построения распределённых систем серверов.

Важную роль в программном обеспечении для спутникового мониторинга играет картографическая основа. Чем более детализированные и качественные карты используются в системе, тем удобнее диспетчерам вести мониторинг и следить за местонахождением транспортных средств.

Как правило, в программах, имеющих клиентскую часть, карты устанавливаются непосредственно на компьютер пользователя. А web-системы используют онлайн-карты, которые благодаря Web-GIS серверу подгружаются по мере необходимости, что, безусловно, требует высокой скорости интернет-соединения. Web-GIS позволяет одновременно использовать такие карты, как Яндекс.Карты, Карты Google, OpenStreetMap, Карты Yahoo!, Карты Bing, Карты Gurtam и другие.

Функции программного обеспечения.

Программное обеспечение для спутникового мониторинга обычно имеет ряд интерфейсов. Вход пользователей в систему мониторинга чаще всего защищён паролем для предотвращения несанкционированного доступа к информации. В системах существует определённая иерархическая структура, при которой администратор системы мониторинга управляет правами доступа различных пользователей к различным объектам мониторинга и различным функциям программы.

Основные функции ПО современных СМПО:

– подключение и настройка трекеров (абоненских устройств) в системе;

– подключение и настройка датчиков в системе;

– мониторинг текущего положения ТС на карте;

– мониторинг состояния приборов и датчиков ТС;

– просмотр маршрута перемещения и пробега ТС за выбранный интервал времени;

– создание точек интереса и геозон на карте;

– контроль перемещения из/в геозоны;

– настройка уведомлений, высылаемых системой, когда происходят определённые события (превышение скорости, слив топлива и др.);

– настройка шаблонов отчётов, выполнение отчётов;

– построение графиков на основании данных системы;

– управление объектами мониторинга через SMS команды или CSD соединение;

– создание маршрутов и путевых точек, контроль соблюдения маршрута.

Дополнительные функции ПО СМПО:

– поиск ближайшего к заданной точке автомобиля;

– передача текстовых сообщений водителю ТС и обратно, от водителя к диспетчеру;

– обеспечение голосовой связи с объектом;

– ведение журнала техобслуживания ТС;

– определение периметра и площади объектов на карте;

– web-доступ в ПО СМПО с мобильного телефона или КПК;

– экспорт из отчетов в форматы, поддерживаемые иным ПО (Excel, Pdf, XML, CSV и др.);

– изменение иконок, отображающих объекты на карте.

7.3. Этапы развития систем мониторинга подвижных объектов

В зависимости от применяемых технических решений можно выделить пять поколений развития СМПО:

1. Самые первые СМПО были «оффлайновыми», то есть не позволяли осуществлять мониторинг в реальном времени и использовали технологии NAVSTAR GPS. GPS-трекер записывал все данные в память и передавал их на сервер по прибытии транспортного средства на базу через проводной или беспроводной интерфейс. Такая схема позволяла контролировать маршрут ТС только постфактум и не была способна помочь, например, при угоне автомобиля.

2. Во втором поколении для организации связи между абонентскими устройствами и сервером использовались SMS либо механизм CSD (технология передачи данных, разработанная для мобильных телефонов стандарта GSM. CSD использует один временной интервал для передачи данных на скорости 9,6 кбит/с в подсистему сети и коммутации (Network and Switching Subsystem NSS), где они могут быть переданы через эквивалент нормальной модемной связи в телефонную сеть). На сервер устанавливались один или несколько модулей сотовой связи, позволяющие принимать SMS или звонки с данными. Подобные системы отличались большим периодом времени между передачами данных местоположения и режимами получения данных по запросу. С массовым распространением мобильного интернета системы второго поколения практически вымерли.

3. В третьем поколении для организации связи между абонентскими устройствами и сервером использовались GPRS или EV-DO технологии.

EV-DO – «Evolution-Data Only» – технология передачи данных, используемая в сетях сотовой связи стандарта CDMA.

CDMA – «Code Division Multiple Access» – множественный доступ с кодовым разделением – технология связи, обычно радиосвязи, при которой каналы передачи имеют общую полосу частот, но разную кодовую

модуляцию. Наибольшую известность на бытовом уровне технология получила после появления сетей сотовой мобильной связи, ее использующих, из-за чего часто ошибочно исключительно с ней (сотовой мобильной связью) и отождествляется.

Это позволило снизить расходы на передачу данных местоположения и строить системы отображения всех объектов в режиме реального времени – on-line. В таких системах сервер устанавливается непосредственно у клиента в локальной сети офиса, что обеспечивает лучшую оперативность и защищенность данных, однако требует регулярной поддержки сервера силами клиента. Обслуживание сервера требует определенной квалификации обслуживающего персонала на стороне клиента. На рабочие места пользователей устанавливается специализированное программное обеспечение. В некоторых системах допускается аренда ресурсов сервера, предоставляемых поставщиком услуг мониторинга.

4. Системы четвёртого поколения также используют один из механизмов мобильного интернета для связи между абонентскими устройствами и сервером, но отличаются от третьего централизацией серверного обеспечения у поставщика услуги и использованием web-технологий. В этом случае сервер размещается у компании-поставщика, его мощности делятся между многими клиентами, а защищённый доступ к данным осуществляется через веб-приложение с любого компьютера, подключённого к интернету. Так как один сервер способен работать одновременно с тысячами объектов, значительно снижается стоимость внедрения и обслуживания системы. Одновременно может быть обеспечена более высокая надёжность хранения данных, так как компании-операторы способны построить сервер на базе качественного оборудования с многократным резервированием, содержать штат технических специалистов для круглосуточного обслуживания. Недостатком систем четвёртого поколения является полная централизация. Хотя вероятность аппаратного сбоя или наступления форс-мажорных обстоятельств в таких системах крайне низка, зато последствия сбоя могут стать весьма дорогостоящими и клиенту сложно оценить последствия утечки информации через технические службы оператора.

5. Системы мониторинга пятого поколения представляют собой глобальное развитие и централизацию систем предыдущего поколения в логически единый, распределённый центр мониторинга – ДЦ, работающий по принципу облачных технологий (вычислений). В таком варианте данные GPS и ГЛОНАСС устройств, собираемые коммуникационными серверами, стекаются в логически объединенный сервер базы данных и далее распределяются между промежуточными серверами, которые обеспечивают взаимодействие с пользователем. При такой архитектуре системы пользователи из разных регионов, стран и даже континентов получают информацию от ближайшего регионального центра с

минимальной задержкой, получая от оператора программное обеспечение как услугу (англ. software as a service, сокр. SaaS). Некоторые платформы для спутникового мониторинга транспорта и управления им позволяют не только использовать стандартный интерфейс, но и персонализировать рабочее место под себя, тем самым благодаря концепции облачных вычислений клиент получает рабочие места как услугу. Внедрение подобных систем даёт возможность глобального управления транспортными потоками в реальном времени, а пользователи могут экономить время, ресурсы и оптимально планировать маршруты.

Облачные вычисления (англ. cloud computing), в информатике – это модель обеспечения повсеместного и удобного сетевого доступа по требованию к общему пулу (набору готовых к использованию объектов) конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и/или обращениями к провайдеру.

СМПО, представленные в России, можно условно разделить на несколько групп:

– трекеры с минимальным набором программного обеспечения, часто бесплатным, которое позволяет решать базовые задачи персонального мониторинга;

– программно-аппаратные комплексы, представляющие собой законченные решения. В этом случае спутниковое оборудование и программное обеспечение разработаны унифицированными и переход с одной на другую систему затруднен;

– программные комплексы, совместимые с различными контроллерами и трекерами, предоставляемые в аренду с ДЦ в формате Software as a service;

– программные комплексы для серверной установки, способные поддерживать различные виды GPS и ГЛОНАСС оборудования одновременно, позволяющие клиентам иметь различные контроллеры в своём автопарке;

– комплексные услуги по мониторингу ТС, которые оказываются специализированными компаниями. В таком случае клиент платит ежемесячную абонентскую плату за использование системы. Отдельно оплачивается приобретение и установка контроллеров на транспортные средства, при этом некоторые компании предлагают аренду контроллеров, тем самым снижая единовременные затраты для компании, которая планирует вести мониторинг своего автопарка.

Следует также учитывать, что системы мониторинга могут быть как самостоятельными решениями, так и модулем в более сложной системе. Немаловажное значение имеют возможности выполнения системой

бухгалтерской, складской, логистической функций или интеграции СМПО с другими автоматизированными системами управления предприятием (ERP-системами).

Некоторые СМПО в настоящее время состоят «на вооружении» органов внутренних дел для оперативного управления мобильными нарядами полиции, а также для охраны объектов транспортной инфраструктуры государства и перевозимых опасных и ценных грузов: СМПО «Алмаз» (ООО «Кодос-Б», Москва), СМПО «Аркан-СМ» (ЗАО «БалтАвтоПоиск», г. Санкт-Петербург), СМПО «Приток-МПО» (ООО «Охранное бюро «Сократ», г. Иркутск) и др.

Вопросы для самостоятельной работы

1. Задачи, решаемые СМПО.
2. Обобщенная структура и состав СМПО.
3. Какие датчики устанавливаются на транспортное средство для получения дополнительной информации при мониторинге?
4. Основные функции ПО современных СМПО.
5. Перечислите и охарактеризуйте основные этапы развития СМПО.
6. Аппаратура спутниковой навигации (АСН).
7. Глобальная навигационная спутниковая система (ГНСС).
8. Альманах ГНСС.
9. Защищенность объектов и грузов.
10. Навигационная аппаратура потребителя (НАП).
11. Навигационно-мониторинговая система (НМС).
12. Навигационное обслуживание потребителя ГНСС.
13. Навигационный космический аппарат (НКА).
14. Мониторинг объектов и грузов.
15. Определение местоположения потребителя ГНСС.
16. Орбитальная группировка навигационных космических аппаратов ГНСС.
17. Подсистема космических аппаратов (ПКА).
18. Подсистема контроля и управления (ПКУ).
19. Подсистема потребителей.
20. Потребитель ГНСС.
21. Спутниковая навигация.
22. Терминал мобильный (ТМ), терминальное устройство (ТУС).
23. Центр мониторинга.
24. Электронная карта (ЭК).

ТЕМА 8
ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Учебные и воспитательные цели:

Образовательные: изучить назначение и основы построения интегрированных систем безопасности.

Развивающие: расширить базовые знания обучающихся в области организации системы безопасности на основе интегрированных систем безопасности; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог;

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

8.1. Назначение, основные эксплуатационные возможности и уникальные свойства ИСБ.

8.2. Обобщенная функциональная и иерархическая структурная схемы ИСБ.

8.3. Основные требования к проектированию ИСБ.

8.1. Назначение, основные эксплуатационные возможности и уникальные свойства ИСБ

Для охраны объектов подразделениями вневедомственной охраны наибольшее применение находят системы централизованной охраны, отличительной особенностью которых является то, что силы быстрого реагирования (ГЗ) сосредоточены на ПЦО, который одновременно обеспечивает охранную безопасность большого числа объектов с помощью ПЦН.

СОБ в этом случае состоит из объектового комплекса технических средств ОПС (КТС ОПС), СПИ и ПЦН.

Дежурный ПЦО с помощью ПЦН осуществляет дистанционный контроль состояния ТСО, установленных на охраняемых объектах. Передача извещений осуществляется с помощью СПИ, как правило, по специально прокладываемым проводным линиям связи, телефонным линиям ГТС или по радиоканалу. При поступлении на ПЦН тревожного извещения от УОО СПИ одного из объектов дежурный ПЦО отдает устный приказ о выезде на этот объект вооруженной ГЗ или других сил быстрого реагирования, а при необходимости и ИТР обслуживающих организаций (ФГУП «Охрана» Росгвардии) для ремонта ТСО.

Анализ предметной области показал, что подразделениями ВО и ФГУП «Охрана» Росгвардии, а также частными охранными организациями

защита объектов от криминальных и террористических угроз осуществляется с помощью следующих технических СОБ: СОТС, СПС, СОТ, СКУД, работающих автономно или централизованно.

Каждая СОБ имеет ряд уникальных функций и в сочетании с требуемым уровнем ИТУ обеспечивает необходимый уровень защиты объекта заданной категории.

Будучи объединенными на объекте, взаимодействующие традиционные СОБ образуют ИСБ, у которой появляется возможность разработки различных сценариев действий одной подсистемы в ответ на события в другой. ИСБ приобретает свойство эмерджентности. Таким образом, эмерджентность ИСБ характеризует появление нового качества охраны при агрегировании традиционных СОБ. Это свойство и является системообразующим фактором в области обеспечения комплексной безопасности объектов.

Следовательно, практическая реализация системного подхода к обеспечению комплексной безопасности объектов, подлежащих охране, неразрывно связана с идеей разработки и применения ИСБ.

Подразделения вневедомственной охраны используют ИСБ, которые входят в соответствующий «Список…». Данный «Список…» сформирован для реализации единой технической политики в обеспечении надёжной охраны объектов, квартир и других мест хранения личного имущества граждан на территории Российской Федерации.

Анализ современных ИСБ, входящих в «Список…», а именно: «Стрелец-Интеграл», «Орион», «Пахра», «Рубеж-08», позволил сформировать перечень основных *эксплуатационных возможностей ИСБ.* Итак, современные ИСБ обеспечивают:

– модульную структуру, позволяющую обеспечивать безопасность как малых, так и очень больших объектов, в том числе территориально распределенных;

– контроль и управление доступом на охраняемые объекты с учётом полномочий каждого сотрудника;

– контроль охранной и тревожной сигнализации на объекте;

– контроль пожарной сигнализации на объекте;

– видеонаблюдение, видеоконтроль и видеорегистрацию тревожных ситуаций с графических планов объектов;

– отображение событий на графических планах объектов;

– разработку сценариев действий (правил реакции) одной системы в ответ на события в другой;

– управление установками пожарной безопасности;

– управление инженерными системами здания;

– имитостойкость протокола передачи данных в сетях;

– возможность передачи информации по любым каналам связи;

– возможность взятия под охрану, снятия с охраны объектов с помощью электронных карт, ключей;

– речевое предупреждение дежурного о тревожных событиях, возможность записи и воспроизведение сообщений;

– отображение состояния зон, разделов, точек доступа, приемно-контрольных приборов, считывающих устройств, видеокамер на графических планах помещений с подробными текстовыми пояснениями;

– разграничение полномочий дежурных операторов, администраторов за счёт многоуровневой системы паролей и возможного подключения биометрических систем ограничения доступа к программам автоматизированных рабочих мест (АРМ);

– протоколирование всех событий, происходящих в системе;

– ведение единой базы данных пользователей;

– развитую диагностику работоспособности всех блоков и устройств системы;

– удаленное администрирование системы;

– сохранение общей надежности системы при интеграции подсистем;

– высокую живучесть системы, то есть сохранение ее работоспособности при выходе из строя отдельных подсистем и блоков, а также сохранение работоспособности отдельных подсистем (в рамках их функций) при выходе из строя сервера ИСБ или при потере связи с ним;

– автономную работу контроллеров подсистем при нарушении связи с сервером ИСБ.

Современные ИСБ характеризуются не только большим числом элементов, но и, главным образом, сложностью структуры. В связи с этим сложность современных ИСБ нужно рассматривать не только как количественное увеличение комплектующих систему элементов, а и как новое качественное свойство, присущее только этим системам. То есть ИСБ позволяют вывести качество охраны объектов на принципиально новый более надежный уровень.

Так как качество – это совокупность свойств продукции, обусловливающих ее пригодность удовлетворять определенные потребности в соответствии с ее назначением, а свойство продукции – объективная особенность продукции, которая может проявляться при ее создании, эксплуатации или потреблении, то сформулируем *уникальные свойства ИСБ*:

1. Единая система сбора, обработки и представления данных, мониторинга и управления всеми входящими системами, в том числе в безоператорном режиме.

2. Возможность разработки сценариев действий в ответ на различные события в системе за счет специализированного ПО.

Под событием в системе понимается все, что происходит в системе, например, обнаружение движения правонарушителя системой охранного

телевидения, выдача тревожного извещения от извещателя СОТС или СПС, факт прохода через точки доступа, контролируемые СКУД, и т.п.

Действием является все, что можно сделать в системе, например, разблокировать дверь для беспрепятственной эвакуации, включить камеру на запись, выдать предупреждение оператору, поставить/снять ШС на охрану/с охраны, запретить проход по всем дверям и т.д.

В ответ на событие или некий набор событий можно определить соответствующий набор действий системы – сценарий действий (реакций). Более того, применяя специальный язык сценариев, можно определить сколь угодно сложную реакцию системы на возможные события.

Например, рассмотрим следующий сценарий действий в ИСБ. При возникновении пожара (очага возгорания) «срабатывают» пожарные извещатели СПС. Тревожные извещения передаются на сервер ИСБ, который выдает тревожный сигнал оператору. Во избежание ложных тревог СОТ выводит на монитор оператора изображение от ближайших к очагу возгорания видеокамер и анализирует изображение посредством алгоритмов распознавания образов огня или дыма. В случае подтверждения угрозы пожара по команде оператора или без его участия (если отсутствует ответ или определенные действия со стороны оператора в течение определенного времени) формируются команды другим системам ИСБ, например:

– включается система речевого и светового оповещения;

– СКУД разблокирует выходы для беспрепятственной эвакуации людей;

– СУЖ выключает приточную вентиляцию, обслуживающую данную зону, лишая очаг возгорания притока кислорода;

– для удаления дыма из коридоров, холлов, лестниц (вдоль маршрутов эвакуации) СУЖ включает систему дымоудаления;

– СУЖ отключает линии электропитания в районе очага возгорания и включает систему аварийного освещения;

– СУЖ включает систему пожаротушения и так далее.

Такой сценарий может быть реализован только за счет взаимодействия отдельных подсистем ИСБ и единой логики управления. Именно наличие таких взаимосвязей и событийных моделей позволяет говорить о действительно интегрированной системе. При этом не должно быть абсолютно никаких ограничений на описание логики работы системы – все, что может потребоваться на конкретном объекте в конкретных условиях, можно описать средствами ИСБ.

1. Интегрируемость. Возможность интеграции любого оборудования и подсистем независимо от типа оборудования, его производителя, места размещения, технических характеристик и общей топологии системы.

2. Модульность и открытые интерфейсы. Система может быть легко расширена как за счет включения новых модулей, так и за счет ин-

теграции системы с уже существующими компьютеризированными системами предприятия.

3. Масштабируемость. Отсутствие ограничений на масштаб охраняемого объекта и возможность подключения любого количества автоматизированных рабочих мест.

4. Многоуровневая (иерархическая) структура. Позволяет рационально распределить потоки информации между подразделениями охраняемого предприятия и тем самым минимизировать объем передаваемых данных. Каждое подразделение получает только те сообщения, которые соответствуют служебным обязанностям и уровню ответственности. На высший уровень, например руководителю предприятия, передаются только наиболее важные сообщения. Сообщения средней важности остаются на соответствующем уровне иерархии и не передаются на более высокий уровень. Сообщение может быть передано на более высокий уровень системы только в том случае, если по истечении допустимого времени отсутствует реакция ответственного персонала.

Таким образом *интегрированная система безопасности объекта* – это специализированная сложная техническая система, объединяющая на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных технические средства, предназначенные для защиты объекта от нормированных угроз.

Однако данное определение не в полной мере раскрывает понятие ИСБ, поэтому в работе предложено новое развернутое.

Интегрированная система безопасности объекта – это совокупность совместно действующих средств и систем охранной безопасности, как правило, СОТС, СПС, СОТ, СКУД, СУЖ и, возможно, других систем, обладающих технической, программной, информационной, электромагнитной и эксплуатационной совместимостью, работающих по единому алгоритму взаимодействия, имеющих общие каналы связи, программное обеспечение, базы данных, предназначенная для обеспечения противокриминальной и антитеррористической защиты объекта, в том числе в безоператорном режиме.

8.2. Обобщенная функциональная и иерархическая структурная схемы ИСБ

Из сформулированного определения следует, что в ИСБ входят традиционные СОБ с известным составом и структурами. Поэтому обобщенная функциональная схема ИСБ будет выглядеть как показано на рис. 8.1.

ИСБ обладает достаточно сложной многоуровневой (иерархической) структурой, обусловленной сложностью входящих в нее СОБ, программного обеспечения и коммуникационного оборудования СПД,

поэтому для последующего анализа необходимо разработать иерархическую структурную схему ИСБ (рис. 8.2).

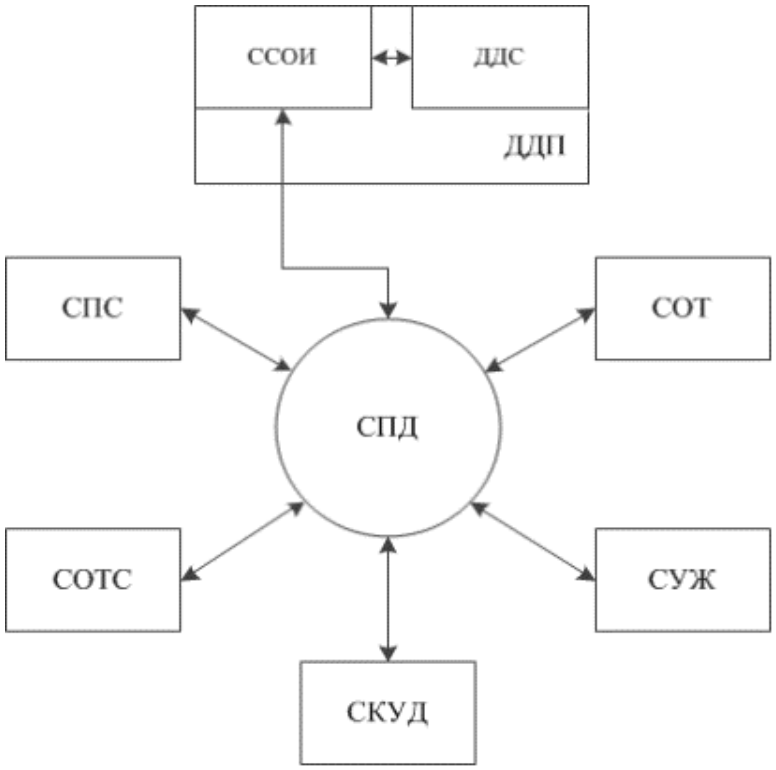


Рис. 8.1. Обобщенная функциональная схема ИСБ

На рис. 8.2 использованы следующие обозначения:

– АРМ – автоматизированное рабочее место оператора ИСБ (АРМ удаленного администрирования, АРМ бюро пропусков, АРМ оператора, АРМ начальника службы охраны и т.д.);

– TCP/IP – сеть передачи данных по протоколу TCP/IP;

– локальный контроллер – контроллер, с помощью которого можно автономно (без серверного ПЭВМ) управлять системой и вести протоколирование событий.

Первый (высший) уровень иерархии представляет собой компьютерную сеть типа клиент-сервер на основе сети Ethernet с протоколом обмена TCP/IP и с использованием сетевых операционных систем (ОС) Windows XP или типа Unix. Этот уровень обеспечивает связь между сервером ИСБ и АРМ операторов. Выбор ОС профессионального класса обусловлен тем, что здесь необходим высокий уровень надежности и защита от несанкционированного доступа к информационным ресурсам ИСБ. На данном уровне обеспечивается управление всей ИСБ посредством специализированного программного обеспечения.

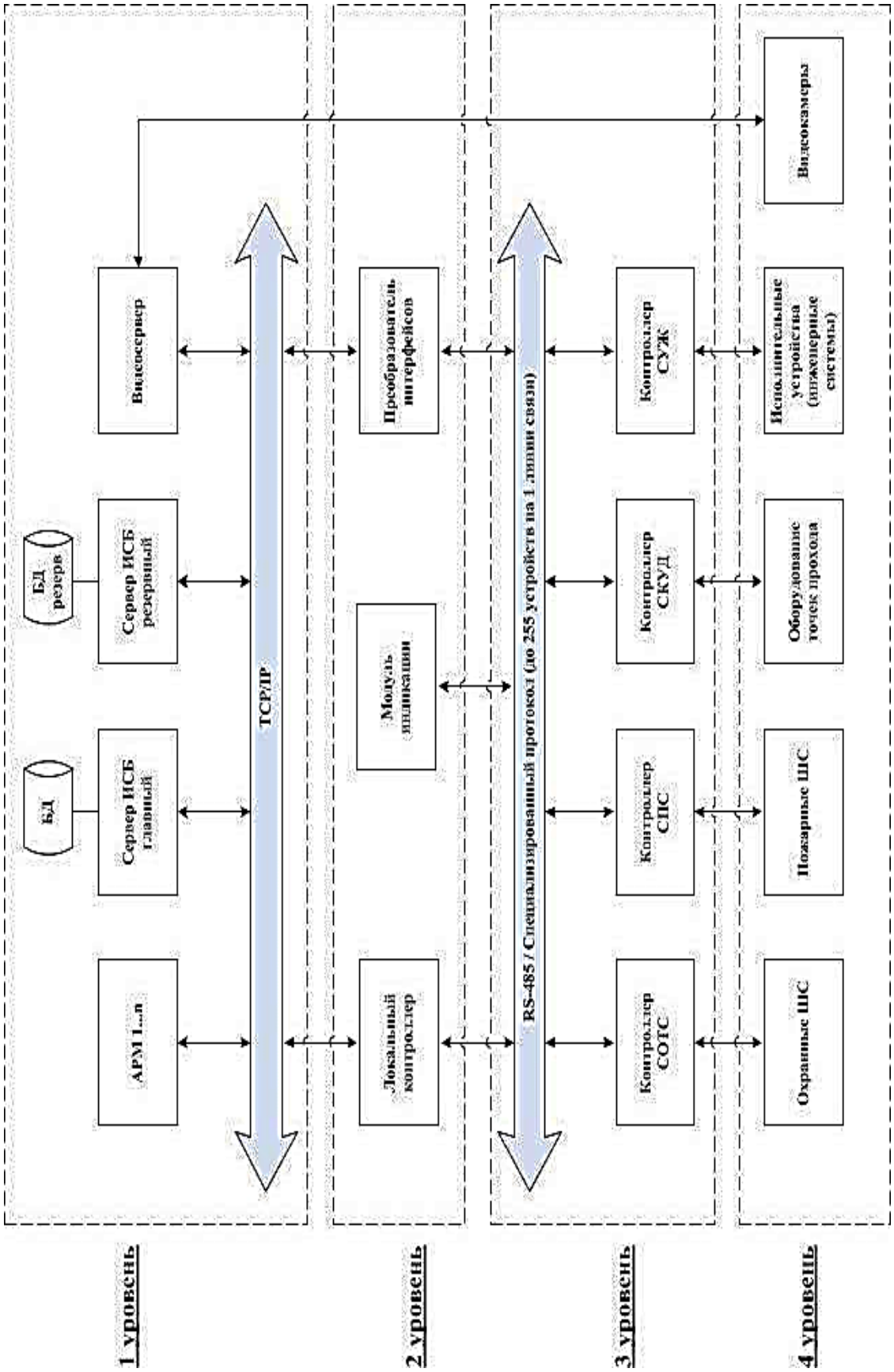


Рис. 8.2. Иерархическая структурная схема ИСБ

Второй уровень иерархии – связь между локальными контроллерами и компьютерами первого уровня (вертикальный уровень связи). На вертикальном уровне наиболее часто используется интерфейс TCP/IP или RS-232. Если в ИСБ не используются локальные контроллеры для локального управления (резервирования функций сервера ИСБ) объектовым оборудованием, то используются преобразователи интерфейсов типа RS-485/TCP/IP, которые предназначены лишь для обеспечения связи третьего уровня с первым.

Третий уровень иерархии – связь между однородными контроллерами каждой из подсистем третьего уровня с локальными контроллерами или с преобразователями интерфейсов второго уровня (горизонтальный уровень связи – протоколы RS-485 или специализированные); а также связь между локальными контроллерами или преобразователями интерфейсов с компьютерной сетью первого уровня (вертикальный уровень связи – протокол TCP/IP).

В контроллерах третьего уровня некоторых ИСБ реализован прямой выход на первый уровень в протоколе TCP/IP.

Четвертый уровень иерархии – связь между контроллерами подсистем ИСБ третьего уровня с периферийными устройствами четвертого уровня. Здесь располагаются: устройства считывания, электрозамки, различные исполнительные устройства, в том числе инженерных систем зданий, оповещатели, модули пожаротушения, радиальные ШС, адресные ШС, входные цепи для контроля датчиков различных подсистем управления, видеокамеры и т.п.

8.3. Основные требования к проектированию ИСБ

Важнейшую роль при создании ИСБ на объекте играет процесс проектирования, так как именно на этапе проектирования закладываются все необходимые качественные и количественные характеристики, в том числе и надежностные. При проектировании важным вопросом является выбор подсистем и технических средств, из которых будет создаваться ИСБ. Под техническими средствами ИСБ понимаются технические изделия (продукция серийного производства, специально предназначенная для построения ИСБ), а также система в целом, как продукция единичного производства, создаваемая для каждого объекта путем проектирования, монтажа, пусконаладки и сдачи в эксплуатацию, функциональным назначением которой является обеспечение безопасности от нормированных угроз. ИСБ представляет собой сложную техническую систему, и при ее создании приходится использовать различное оборудование, как по функциональному назначению, так и, возможно, оборудование разных производителей. Следовательно, на этапе проектирования ИСБ определяется способ (платформа) интеграции оборудования.

Учитывая тот факт, что основными системами, входящими в ИСБ и предназначенными для самого раннего обнаружения несанкционированного проникновения правонарушителя на объект или очага возгорания, являются

СОТС и СПС, основные требования к проектированию ИСБ можно сформулировать следующим образом:

1. Состав, структура построения и функции системы, комплекса должны быть технически и экономически обоснованы.

2. Допускается разделение всей системы, комплекса в целом на функционально самостоятельные составные части (рубежи, участки, зоны, разделы, контуры и т.п.). При этом построение системы, комплекса должно обеспечивать возможность ее, его модификации (расширения функциональных возможностей) и устойчивую работоспособность (отказ какого-либо из функциональных участков не должен приводить к отказу всей системы, комплекса в целом).

3. Проектируемые система или комплекс должны удовлетворять требованиям рациональности, целостности, комплексности, перспективности и динамичности:

– *рациональность* выбираемого варианта системы или комплекса достигают его условной оптимизацией, означающей минимизацию затрат на реализацию при заданной эксплуатационной надежности;

– *целостность* выбираемого варианта обеспечивают наилучшим сочетанием и взаимодействием его составных частей, имеющих ограниченные тактико-технические возможности и ресурс;

– *комплексность* выбираемого варианта предполагает его сбалансированность с учетом общей целевой задачи при оснащении объекта, реальных (в т.ч. финансовых) возможностей пользователя;

– *перспективность* выбираемого варианта означает, что он должен обеспечивать условия для своего развития с учетом возможных изменений в процессе эксплуатации;

– *динамичность* выбираемого варианта заключается в гарантированном выполнении им целевых функций в течение заданного срока службы с учетом износа и восстанавливаемости ТСО.

Вопросы для самостоятельной работы

1. Раскройте понятие и назначение интегрированной системы безопасности.
2. В чем отличие интегрированной системы безопасности от комплексной системы безопасности?
3. Какая статья УК РФ квалифицирует преступные посягательства на материальные ценности объектов в форме кражи?
4. Какие ИСБ входят в Список технических средств, рекомендованных подразделениям вневедомственной охраны?
5. Перечислите основные эксплуатационные возможности ИСБ.
6. Перечислите уникальные свойства ИСБ.
7. Раскройте понятие эмерджентности.
8. Охарактеризуйте уровни иерархии в ИСБ.
9. Перечислите основные требования к проектированию ИСБ.
10. Охарактеризуйте основные информационные потоки в ИСБ.

ТЕМА 9
АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС «БЕЗОПАСНЫЙ ГОРОД»

Учебные и воспитательные цели:

Образовательные: изучить назначение и основы построения аппаратно-программного комплекса «Безопасный город».

Развивающие: расширить базовые знания обучающихся в области организации аппаратно-программного комплекса «Безопасный город»; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог;

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

9.1. Общие сведения об АПК «Безопасный город».

9.2. Особенности проектирования и создания АПК «Безопасный город».

9.3. Требования к Ситуационному центру АПК «Безопасный город».

9.4. Требования к распределенной сети видеонаблюдения АПК «Безопасный город».

9.5. Требования к сети стационарных пунктов экстренной связи «Гражданин-полиция» АПК «Безопасный город».

9.1. Общие сведения об АПК «Безопасный город»

АПК «Безопасный город» – это аппаратно-программный комплекс, включающий в себя системы автоматизации деятельности единой дежурно-диспетчерской службы (ЕДДС), муниципальных служб различных направлений, системы приема и обработки сообщений, системы обеспечения вызова экстренных и других муниципальных служб различных направлений деятельности, системы мониторинга, прогнозирования, оповещения и управления всеми видами рисков и угроз, свойственных данному муниципальному образованию.

Задачами внедрения и развития АПК «Безопасный город» являются:

– организация эффективной работы ЕДДС муниципального образования как элемента системы управления РСЧС для предупреждения и реагирования на кризисные ситуации и происшествия, происходящие на территории муниципального образования;

– организация работы ЕДДС как органа повседневного управления и инструмента для глав муниципальных образований в качестве ситуационно-аналитического центра, с которым взаимодействуют все муниципальные и экстренные службы;

– консолидация данных обо всех угрозах, характерных для каждого муниципального образования и их мониторинг в режиме реального времени на базе ЕДДС;

– автоматизация работы всех муниципальных и экстренных служб муниципального образования и объединение их всех в единую информационную среду на базе ЕДДС.

Практическая реализация названных задач обеспечивается путем:

– информатизации процессов управления муниципальными экстренными и коммунальными службами, организациями и предприятиями, решающими задачи по обеспечению природно-техногенной, общественной безопасности, правопорядка и безопасности среды обитания;

– построения сегментов АПК «Безопасный город» на базе существующей инфраструктуры и дальнейшего развития их функциональных и технических возможностей;

– внедрения интеграционной платформы, реализованной на открытых протоколах, для всех автоматизированных систем, взаимодействующих в рамках АПК «Безопасный город», и разработанной с учетом специфики каждого конкретного муниципального образования;

– разработки регламентов межведомственного взаимодействия и нормативной базы для эффективного функционирования всех сегментов АПК «Безопасный город».

Базовым уровнем как построения и реализации АПК «Безопасный город», так и единой межведомственной информационной среды является муниципальный район и городской округ.

Все АПК «Безопасный город» реализуются в муниципальных районах (городских округах) в строго регламентированном порядке в составе комплексной системы безопасности жизнедеятельности субъекта Российской Федерации, как в организационном, так и в техническом и аппаратно-программном аспекте.

В целях реализации Концепции и в соответствии с Положением о единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций (РСЧС), утвержденным постановлением Правительства Российской Федерации от 30.12.2003 № 794, АПК «Безопасный город» и его сегменты должны быть реализованы на базе органа повседневного управления РСЧС в муниципальном районе и городском округе, которым является ЕДДС.

Во исполнение поручений Президента Российской Федерации от 27 мая 2014 года № Пр-1175 и Правительства Российской Федерации от 29 мая 2014 года № РД-П4-3968 на МЧС России возложены функции главного координатора по вопросам внедрения и развития АПК «Безопасный город» в субъектах Российской Федерации, а также функции главного распорядителя бюджетных средств, направленных на реализацию Концепции.

В рамках АПК «Безопасный город» комплексная информатизация процессов функционирования ЕДДС, городских и экстренных служб во взаимодействии с местными и региональными дежурно-диспетчерскими службами должна обеспечить:

– своевременное представление главе муниципального образования, руководителям местной администрации и других заинтересованных органов местного самоуправления полной, достоверной и актуальной информации об угрозе возникновения чрезвычайных ситуаций, других кризисных ситуаций и происшествий (КСП) на территории муниципального образования, оперативную подготовку дежурно-диспетчерскими службами и доведение до исполнителей обоснованных и согласованных предложений для принятия управленческих решений по предупреждению и ликвидации КСП;

– включение органов местного самоуправления, а также муниципальных организаций и предприятий, выполняющих различные задачи по обеспечению общественной безопасности, правопорядка и безопасности среды обитания, в единое информационное пространство антикризисного управления, эффективное вовлечение региональных управленческих кадров в процессы подготовки и принятия решений по предупреждению и ликвидации КСП на муниципальном уровне;

– улучшение качества принимаемых решений и планов на основе использования аналитических и количественных методов их оценки и оптимизации выбора рационального варианта;

– многократность использования первичной информации, упорядочивание потоков информации, увеличение достоверности и полноты используемых данных на основе их регулярной актуализации по утвержденным регламентам;

–повышение оперативности процессов управления мероприятиями по предупреждению и ликвидации КСП, сокращение общего времени на поиск, обработку, передачу и выдачу информации;

–обеспечение организационно-методической, информационно-лингвистической и программно-технической совместимости сегментов, подсистем и компонентов АПК «Безопасный город».

9.2. Особенности проектирования и создания АПК «Безопасный город»

Заказчиком работ по построению (развитию) АПК «Безопасный город» может быть определен:

– государственный орган (в том числе орган государственной власти) либо государственное казенное учреждение, действующее от имени субъекта Российской Федерации, уполномоченное принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени субъекта Российской Федерации и осуществляющее закупки;

– муниципальный орган или муниципальное казенное учреждение, действующие от имени муниципального образования, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени муниципального образования и осуществляющие закупки.

Заказчик обязан:

– разрабатывать, согласовывать и утверждать установленным порядком техническое задание на проектирование АПК «Безопасный город»;

– определять организацию-проектировщика (Исполнителя) по построению (развитию) АПК «Безопасный город» в соответствии с требованиями Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

Общими критериями для конкурсного отбора проектной организации, выполняющей комплекс работ по обследованию информационно-телекоммуникационной инфраструктуры, разработке проектной документации, специального программного и информационного обеспечения АПК «Безопасный город» являются:

– цена контракта;

– качественные, функциональные характеристики проектной документации;

– квалификация участника конкурсного отбора, в том числе по наличию финансовых средств, оборудованию и других материальных ресурсов, опыта работы, связанного с предметом контракта, деловой репутации, специалистов и иных работников определенного уровня квалификации.

В конкурсной документации заказчик обязан указать используемые при определении исполнителя работ по проектированию АПК «Безопасный город» критерии и их величины значимости. При этом предложенная цена контракта не должна стать доминирующим

показателем при выборе проектировщика и главным критерием должны являться оценка его квалификации и заявляемого качества работ.

Сумма величин значимости всех критериев, предусмотренных конкурсной документацией, должна составлять сто процентов.

В целях выполнения работ по проектированию АПК «Безопасный город» на высоком научно-техническом уровне предлагается применять следующие величины значимости критериев оценки заявок участников закупки:

– цена контракта – 30;

– качественные, функциональные характеристики проектной документации – 35;

– квалификация участника конкурсного отбора, в том числе по наличию финансовых средств, оборудованию и других материальных ресурсов, опыта работы, связанного с предметом контракта, деловой репутации, специалистов и иных работников определенного уровня квалификации – 35.

Проектно-сметная документация на создание АПК «Безопасный город» разрабатывается в соответствии с требованиями:

– ТЗ на создание АПК «Безопасный город»;

– постановления Правительства Российской Федерации от 16 февраля 2008 года № 87 «О составе разделов проектной документации и требований к их содержанию»;

– ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».

Перечень основных действующих и перспективных автоматизированных систем, сопрягаемых с АПК «Безопасный город», по следующим функциональным направлениям:

– Системы приема и обработки вызовов и сообщений, включая Систему 112 и автоматизированные системы приема и обработки вызовов, взаимодействующих ДДС.

– информационные и аналитические системы;

– системы обеспечения управления силами и средствами;

– системы мониторинга параметров энерго-, газо-, тепло-, водоснабжения;

– системы мониторинга и контроля качества услуг ЖКХ;

– системы управления градостроительной деятельностью;

– системы видеонаблюдения;

– системы видеофиксации нарушений ПДД;

– системы мониторинга состояния окружающей среды;

– системы обеспечения пожарной безопасности;

– системы мониторинга и раннего обнаружения лесных пожаров;

– системы мониторинга паводковой обстановки;

– системы пожарных сигнализаций;

– системы охранных сигнализаций;

– системы экстренного вызова и тревожных сигнализаций;

– системы оповещения и информирования;

– системы мониторинга состояния объектов инженерной инфраструктуры;

– системы космического мониторинга;

– системы экологического мониторинга;

– автоматизированные системы лабораторного контроля качества воздуха, воды, почвы;

– системы экстренного реагирования на транспортных средствах «ЭРА-ГЛОНАСС»;

– поисковые и навигационные системы (ГЛОНАСС/GPS);

– системы технического мониторинга объектов транспортной инфраструктуры;

– автоматизированные системы управления дорожным движением;

Конкретный перечень АС уточняется на этапе проектирования АПК «Безопасный город».

В пилотной зоне АПК «Безопасный город» должны быть интегрированы все существующие на территории муниципального образования автоматизированные системы из вышеуказанного перечня и в обязательном порядке системы оповещения, информирования, система-112, системы мониторинга.

ТЗ на создание АПК «Безопасный город» разрабатывается уполномоченным органом местного самоуправления или органом исполнительной власти субъекта Российской Федерации в части функциональных и технических требований к системам, обеспечивающим комплексную безопасность на уровне субъекта Российской Федерации, и согласовывается с территориальным органом управления МЧС России.

Согласованное с территориальным органом управления МЧС России ТЗ утверждается руководителем муниципального образования и уполномоченным органом исполнительной власти субъекта Российской Федерации и направляется на согласование в Совет главных конструкторов автоматизированной информационно-управляющей системы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций на базе ресурса Национального центра управления в кризисных ситуациях (СГК АИУС РСЧС), функционирующего на базе Всероссийского научно-исследовательского института по проблемам гражданской обороны и чрезвычайных ситуаций (федерального центра науки и высоких технологий).

Техническое задание на создание АПК «Безопасный город» является основным документом, определяющим требования к системе, в соответствии с которыми осуществляются работы по ее созданию и приемка в эксплуатацию.

Для создания АПК «Безопасный город» исполнитель должен выполнить работы по закупке оборудования, программного обеспечения, проведению монтажных и пуско-наладочных работ.

АПК «Безопасный город» должен пройти приемочные испытания на соответствие требованиям, согласованным Советом главных конструкторов АИУС РСЧС и утвержденным МЧС России.

Поставка оборудования и программного обеспечения АПК «Безопасный город» производится в соответствии с условиями контракта и ТЗ. Поставленное оборудование должно быть смонтировано и проведены инсталляция программного обеспечения и пуско-наладочные работы.

Работы по монтажу оборудования должны выполняться в соответствии с требованиями проектной документации на создание АПК «Безопасный город».

ЕДДС для размещения необходимого оборудования должен обладать соответствующими для его эксплуатациями условиями, а также иметь необходимое электроснабжение.

При производстве монтажа оборудования, а также при его профилактике и эксплуатации необходимо строго соблюдать действующие инструкции и правила по технике безопасности, эксплуатации и монтажу оборудования, установленные производителем.

Исполнитель после завершения монтажных работ представляет заказчику необходимые документы, включая официальное извещение об окончании работ и готовности АПК «Безопасный город» к эксплуатации.

Исполнение заданий на сопряжение организациями-разработчиками смежных КСА и комплексную отладку сегментов АПК «Безопасный город» в муниципальных образованиях производится в соответствии с утвержденным технорабочим проектом.

В проектно-сметной документации должны быть указаны аппаратно-программные средства и финансирование работ, необходимых для организации сопряжения в рамках АПК «Безопасный город».

По завершении монтажных и пуско-наладочных работ исполнитель проводит предварительные испытания на соответствие требованиям технического задания с оформлением протоколов и актов предварительных испытаний.

Материалы предварительных испытаний вместе с уведомлением о готовности к приемочным испытаниям направляются заказчику.

Заказчик издает приказ (распоряжение) о создании приемочной комиссии.

Испытания АПК «Безопасный город» проводятся в соответствии с программой и методикой приемочных испытаний, разработанных исполнителем. Программа и методика приемочных испытаний должна быть согласована с МЧС России и утверждена заказчиком.

9.3. Требования к Ситуационному центру АПК «Безопасный город»

Создание Ситуационного центра предусматривает выделение здания (помещений), реконструкцию и ремонт помещений в соответствии с требованиями проектной документации на него; оснащение мебелью, приобретение и входной контроль всего необходимого для функционирования СЦ оборудования, проведение всех работ по монтажу.

Ситуационный центр включает в себя следующие помещения: зал оперативного штаба, зал операторов видеонаблюдения, зал серверного оборудования и технического персонала.

Операторы видеонаблюдения привлекаются для поддержки принятия решений по управлению силами и средствами органов внутренних дел при организации мероприятий по борьбе с преступностью, обеспечению правопорядка и общественной безопасности на основе использования современных информационных и телекоммуникационных технологий.

Работа СЦ осуществляется как в повседневном режиме, так и в особых условиях (во время проведения массовых мероприятий, при проведении антитеррористических и профилактических мероприятий, при чрезвычайных ситуациях).

Переход СЦ из режима повседневной деятельности в режимы повышенной готовности, террористической акции или чрезвычайной ситуации обеспечивается действиями дежурных частей (сфера оперативного информирования) по специальным оперативным планам.

Видеосигналы, поступившие в СЦ, с помощью коммутаторов необходимо подавать на монитор телевизионного полиэкрана и экраны коллективного пользования.

Монитор телевизионного полиэкрана и экраны коллективного пользования должен обеспечивать отображение сигналов от необходимого количества видеокамер (ВК).

В СЦ, где организовано круглосуточное дежурство операторов видеонаблюдения и технического персонала, необходимо создать автоматизированные рабочие места (АРМ) из расчета: один оператор на 8 мониторов видеонаблюдения.

Каждое рабочее место СЦ оснащается ПЭВМ, объединенными в выделенную локальную сеть для обеспечения доступа дежурных смен операторов видеонаблюдения в ЕИТКС ОВД.

Для технического персонала СЦ создаются 2 стационарных АРМ и 4 мобильных комплекта.

Технические и программные решения системы должны быть разработаны и реализованы в полном соответствии с существующими стандартами в соответствующих областях деятельности на основе концепции открытых масштабируемых систем, что обеспечит возможность

развития и модернизации СЦ, совместимость решений по комплексу систем с будущим оборудованием и технологиями. При создании системы должен быть учтен достаточный запас для возможности расширения как функциональных возможностей, так и количественных характеристик системы.

Первичная подготовка и обучение персонала эксплуатации и использования технических средств осуществляется исполнителем до ввода в опытную эксплуатацию. Последующая подготовка и обучение персонала осуществляется заказчиком.

Установка и наладка всех систем должна производиться специалистами исполнителя с привлечением эксплуатирующего персонала заказчика. Техническое обслуживание и проведение ремонтно-восстановительных работ должно проводиться техническим персоналом заказчика с привлечением специалистов исполнителя.

Группа АРМ должна состоять из отдельных АРМ операторов, по возможности унифицированных по функциям и возможностям.

АРМ оператора должно состоять из следующих элементов:

– ПЭВМ для работы с информационно-аналитическими средствами СЦ, подготовки, вывода и представления информации;

– системный телефонный аппарат цифровой АТС городского УВД, телефонный аппарат.

Окончательное количество и состав АРМ операторов должны быть определены на этапе проектирования. К требованиям, накладываемым на средства представления информации, следует отнести требования к LCD проектору и проекционному экрану, требования к плазменным панелям.

В качестве ПЭВМ должны быть использованы стационарные ПЭВМ с современным уровнем производительности. Требования к ПЭВМ управления представлением информации аналогичны требованиям к ПЭВМ АРМ операторов. Дополнительные требования к ПЭВМ управления видеотрансляцией должны быть определены на этапе проектирования.

Основным требованием к ПЭВМ управления оборудованием является наличие необходимых интерфейсов и ПО для подключения к технологическим подсистемам управления оборудованием. Технические характеристики ПЭВМ должны быть определены на этапе проектирования системы управления в целом в зависимости от решаемых задач.

Необходимость, состав и характеристики системы управления должны быть определены на этапе проектирования после уточнения решений по оборудованию подсистем.

Локальная вычислительная сеть должна обеспечивать передачу данных для средств, входящих в состав программно-технического комплекса СЦ, а также сопряжение с другими сетями передачи данных. Локальная вычислительная сеть должна предоставлять средствам, входящим в состав программно-технического комплекса СЦ, интерфейсы

100BaseT или 1000BaseTX (определяется на этапе технического проектирования). Локальная вычислительная сеть должна обладать пропускной способностью, достаточной для одновременной работы средств СЦ.

Инфраструктура передачи данных должна учитывать каналы связи, создаваемые в рамках реализации программы МВД России «Создание ИСОД ОВД».

Протоколы, используемые сетью, необходимо определить на стадии рабочего проектирования. Для передачи данных использовать волоконно-оптические линии связи.

Оборудование передачи данных должно эксплуатироваться и обслуживаться инженерным персоналом имеющихся эксплуатационных служб подразделений связи с привлечением внешних специализированных сервисных организаций в части поддержки системно-технической платформы оборудования.

Используемое оборудование должно обеспечивать безопасность персонала при своей эксплуатации.

Конструкция используемого оборудования должна обеспечивать безопасность эксплуатирующего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007. Подключение электропитания должно выполняться в соответствии с требованиями Правил устройства электроустановок (ПУЭ).

9.4. Требования к распределенной сети видеонаблюдения АПК «Безопасный город»

Первая очередь распределенной сети видеонаблюдения (РСВ) на объектах города разворачивается в объеме 30 – 40% из общего числа зон контроля: участки территории с повышенной криминогенной обстановкой, объекты культуры и отдыха, спортивные сооружения, места массового пребывания граждан при проведении публичных мероприятий, объекты системы образования, объекты системы здравоохранения, объекты жизнеобеспечения, остановки общественного транспорта, рынки, торговые центры.

Стационарные и поворотные цветные видеокамеры уличного исполнения предназначены для обзора объектов и территории на участках, идентификации разыскиваемых лиц, обнаружения оставленных предметов. Стационарные черно-белые видеокамеры уличного исполнения предназначены для идентификации транспортных средств, обеспечения безопасности транспортных потоков, определения параметров дорожного движения. Установка всех уличных видеокамер должна осуществляться в антивандальном исполнении.

Размещение ВК, предназначенных для контроля территории города,

должно осуществляться в герметичных термокожухах, имеющих солнцезащитный козырек.

9.5. Требования к сети стационарных пунктов экстренной связи «Гражданин-полиция» АПК «Безопасный город»

Первая очередь распределенной сети стационарных пунктов экстренной связи «Гражданин-полиция» (ПЭС) на объектах города разворачивается в объеме 30 – 40% из общего числа зон контроля: места массового пребывания граждан, объекты системы образования, остановки общественного транспорта, рынки, торговые центры и т.д. Данная система должна обеспечивать:

– вызов гражданином представителей УМВД города;

– обзор участка перед местом установки кнопки экстренного вызова с помощью системы видеонаблюдения;

– протоколирование переговоров;

– архивацию событий;

– отображение на электронной карте города на мониторе оператора СЦ точки города, откуда поступило обращение гражданина.

Вопросы для самостоятельной работы

1. Дайте определение АПК «Безопасный город».
2. Каковы задачи АПК «Безопасный город»?
3. Какие функции выполняет ЕДДС?
4. Кто может выступать заказчиком работ по построению (развитию) АПК «Безопасный город» и какие требования к нему предъявляются?
5. Каков перечень основных действующих и перспективных автоматизированных систем, сопрягаемых с АПК «Безопасный город»?
6. Состав и требования к оборудованию ситуационных центров.
7. Какие предъявляются требования к распределенной сети видеонаблюдения АПК «Безопасный город»?
8. Какие предъявляются требования к сети стационарных пунктов экстренной связи «Гражданин-полиция» АПК «Безопасный город»?

ТЕМА 10
ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

Учебные и воспитательные цели:

Образовательные: подготовка обучающихся к организационно-управленческой деятельности посредством формирования у них знаний, умений и компетенций по вопросам представления о средствах визуального мониторинга, рентгенотелевизионных установках, средствах обнаружения взрывчатых веществ и взрывных устройств, нелинейных радиолокаторах, а также о средствах мониторинга источников радиационного излучения.

Развивающие: расширить базовые знания обучающихся в области противокриминальной и антитеррористической защиты объектов, обеспечения общественной безопасности; развивать у обучающихся ораторское искусство, умение обоснованно выражать свою точку зрения, способность вести профессиональный лексически и терминологически грамотный диалог;

Воспитательные: стимулирование активной познавательной деятельности и мотивации к выбранной профессии; формирование у обучающихся установки на самоанализ, самообучение и самосовершенствование.

Учебные вопросы:

10.1. Классификация антитеррористических средств.
10.2. Средства визуального мониторинга.
10.3. Рентгенотелевизионные установки.
10.4. Обнаружение взрывчатых веществ и взрывных устройств.
10.5. Нелинейные радиолокаторы.
10.6. Мониторинг источников радиационного излучения.

10.1. Классификация антитеррористических средств

Основными являются специальные средства силового (активного) противодействия. Речь, главным образом, идет о различных видах оружия, основными из которых являются штатное огнестрельное и холодное оружие. Российские пистолеты и автоматы известны всему миру. Нет особой нужды их рекламировать. Что касается остальных видов оружия, то на нашем российском рынке открытых предложений они представлены в основном зарубежными образцами. Это относится к пластиковому оружию, светошоковому оружию, в меньшей степени электрошоковому. Исключением является газовое оружие. Скромно пока выглядит рынок

отечественных вспомогательных приспособлений, таких, как приборы ночного видения, лазерные и ИК-прицелы и др.

Кроме этого, важную роль играют защитные средства, реализующие функцию пассивной защиты. Они включают в себя сертифицированные средства индивидуальной бронезащиты (с 1-го по 6-й классы стойкости); специальный бронированный транспорт; пуленепробиваемые конструкционные элементы, в т.ч. стекла; взрывозащищенные конструкции; специальные средства транспортировки и хранения взрывоопасных предметов (в т.ч. в виде передвижных камер, переносных контейнеров, взрывозащитных «колпаков» и пр.). Большинство этих средств защиты используют современные композиционные материалы, позволяющие реализовать высокую степень стойкости к поражающим воздействиям.

Особую роль играют средства антитеррористического мониторинга (досмотрово-поисковая техника), под которой понимается комплекс технических средств, используемый для поиска объектов, обнаружение которых органами чувств человека затруднено или невозможно, а также для контроля посетителей и пассажиров, их вещей (ручной клади, багажа и т. п.) при обеспечении безопасности различных учреждений, массовых мероприятий и общественного транспорта.

Досмотрово-поисковую технику можно классифицировать по ряду признаков: по обнаруживаемому параметру (или физическому признаку объекта), по объекту поиска или досмотра, по мобильности. Классификация поисковой и досмотровой техники по указанным признакам представлена на рис. 10.1.

Многие образцы технических средств, используемых для контроля и досмотра, можно отнести к интроскопам. Интроскопия (от лат. intro – внутри и греч. *skopeo* – смотрю, наблюдаю) – неразрушающее исследование внутренней структуры объекта и протекающих в нем процессов с помощью звуковых волн, электромагнитного излучения различных диапазонов, постоянного и переменного электромагнитного поля и потоков элементарных частиц. К этой группе относятся рентгеноскопическое оборудование, тепловизоры, радиоволновые средства визуального контроля и др.

Для обнаружения одного и того же объекта могут быть использованы приборы, осуществляющие поиск по разным физическим принципам. Например, для обнаружения людей используют газоанализаторы (например, прибор «Гиацинт»), тепловизоры (неохлаждаемый поисково-наблюдательный тепловизор «Катран-3»), средства регистрации акустических колебаний («Лаванда М»), радиоволновые средства (радар-обнаружитель людей за преградами РО-400).

Рис. 10.1. Классификация поисковой и досмотровой техники

В то же время тепловизоры используются для поиска пустот, принципы регистрации акустических колебаний – при поиске механических часовых замедлителей взрывных устройств, газоаналитические методы – при поиске наркотических средств и взрывчатых веществ.

10.2. Средства визуального мониторинга

Средства визуального мониторинга предназначены для обследования мест, осмотр которых невооруженным глазом затруднителен или невозможен. Средства визуального мониторинга можно разделить на специальные досмотровые зеркала, эндоскопы, специальные видеокамеры.

Досмотровые зеркала – вспомогательные технические средства, предназначенные для визуального осмотра мест, доступ к которым затруднен или ограничен: в помещениях, транспортных средствах, контейнерах с грузом на предмет обнаружения подозрительных предметов (ВУ, радиомаяков и других посторонних предметов, свободный оборот которых запрещен). Наиболее часто досмотровые зеркала применяются для автомобильного транспорта: днищ, колесных арок и других

труднодоступных мест. Типовой досмотровый комплект зеркал включает в себя набор сменных зеркал различных размеров и конфигурации и телескопическую штангу, на которой с помощью подвижных шарнирных соединений закрепляется осветитель и одно из зеркал. Осветитель в большинстве случаев светодиодный, за счет чего обеспечивается высокая яркость свечения и малое энергопотребление, что особенно важно в нестационарных условиях. Зеркала, входящие в досмотровые комплекты, имеют, как правило, круглую форму и размеры 60 – 220 мм в диаметре, а также прямоугольную форму с двумя наиболее распространенными типоразмерами: 50х90 мм и 60х110 мм.

Эндоскоп – это оптический прибор, предназначенный для визуального мониторинга объектов, имеющих сложную геометрию, к которым невозможен прямой доступ (рис. 10.2).

Рис. 10.2. Типовая структурная схема эндоскопа

Оптоволоконный эндоскоп состоит из объектива, совмещенного с источником света, световода и окуляра. Основным элементом эндоскопа является световод, изготовленный из множества оптоволоконных нитей. Свет по оптоволокну распространяется за счет многократного переотражения от внутренних стенок оптоволокна. Это позволяет свету распространяться вдоль него, даже если оно изогнуто. Светодовод является направляющей средой для световых волн. Объектив воспринимает световые лучи и проецирует их на вход световода. На противоположном конце световода расположен окуляр, через который можно производить наблюдение невооруженным глазом. В большинстве эндоскопов предусмотрена возможность подключения к окуляру объективов фотоаппаратов или видеокамер для осуществления документирования процесса досмотра. Рабочая часть эндоскопа имеет систему управления, позволяющую оператору с помощью системы тросов изменять угол поворота объектива.

Телевизионные эндоскопы отличаются от оптоволоконных тем, что изображение воспринимается миниатюрной видеокамерой, с помощью которой преобразуется в электрический сигнал. Сигнал передается на приемную сторону по проводнику. Существуют и беспроводные системы, в которых сигнал от видеокамеры передается по радиоканалу, а работа самой камеры управляется дистанционно. Цифровая платформа таких устройств позволяет достаточно легко документировать полученные изображения путем сохранения фотоснимков или видео, при этом текущие процессы будут отображаться на встроенном мониторе. Снимки и видео можно просматривать на телевизоре или сохранять в виде файлов на ПЭВМ.

10.3. Рентгенотелевизионные установки

Для исследования внутреннего состояния объектов применяют рентгенотелевизионные установки (РТУ). Данный вид имеет большой выбор специализированной малодозовой рентгено-просмотровой аппаратуры и рентгеновских интроскопов российского и зарубежного производства. Приборы для исследования внутреннего состояния различных объектов в качестве «поискового признака» используют разницу в плотности укрывающей среды и объекта поиска.

Рентгенотелевизионные установки позволяют в режиме реального времени рассмотреть внутреннюю структуру контролируемого объекта, идентифицировать инородные включения или дефекты. Возможности рентгенотелевизионных систем позволяют обнаружить отдельные элементы оружия и взрывных устройств, контейнеры с опасными вложениями и другие запрещенные к провозу предметы. Применение телевизионного канала в таких системах значительно расширяет функциональные возможности аппаратуры. Появляется возможность записи изображений на носитель для последующего анализа и обработки. Анализируя изображение, оператор может обнаружить спрятанное в радиоприемнике вещество органического происхождения. Мобильная аппаратура предназначена в основном для оснащения временных постов контроля и решения антитеррористических задач. Портативные РТУ применяются для обследования оставленных предметов, труднодоступных мест в зданиях, сооружениях, транспортных средствах и выявления предметов, запрещенных к перевозке. В качестве примера можно привести портативные *рентгенотелевизионные установки «Норка-М», «Шмель-90К»,* предназначенные для проверки почтовой корреспонденции, багажа, мебели, различных бытовых предметов в целях выявления взрывных устройств, контейнеров с опасными вложениями, а также скрыто установленных средств съема информации.

В *интроскопе Z-Scan* во время просмотра изображения область, подозреваемая на наличие взрывчатого вещества, выделяется красной овальной чертой, что обеспечивает оператору дополнительную возможность для выявления ВУ. Рентгеновские интроскопы с люминесцентным экраном предназначены главным образом для контроля почтовой корреспонденции, например *устройство для обследования и обезвреживания взрывоопасных почтовых отправлений У-03*. Эта установка оснащена ручными манипуляторами с комплектом сменного инструмента, системой вентиляции и удаления газообразных продуктов взрыва за пределами помещения. Оператору обеспечивается полная защита при случайном взрыве ВВ массой 300 граммов в тротиловом эквиваленте.

С другой стороны, появилась и ширится по номенклатуре новая рентгено-просмотровая техника, позволяющая контролировать не только массовую, но и так называемую электронную плотность, т.е. различать вещества по атомной их структуре. Достигается это новое качество путем регистрации и отработки не только прямого, но и рассеянного (с меньшей энергией) излучения. Про такие системы говорят, что они двухэнергетические. Практический результат их применения – возможность «видеть» обычные и пластические взрывчатые вещества (ВВ).

Переносной импульсный досмотровый комплекс *«Шмель-90/К»* предназначен для определения содержимого посылки, бандероли, ручной клади, оставленных без присмотра вещей. Он состоит из рентгеновского аппарата массой 6,2 килограмма, снабженного автономным питанием, и легкого рентгеновизуализирующего просмотрового устройства, которое работает в реальном масштабе времени и может фиксироваться в любом положении. Простота управления и небольшие габаритные размеры комплекса позволяют проводить контроль в труднодоступных местах. К достоинствам комплекса относятся:

– значительно меньшие габаритные размеры, масса и энергопотребление в сравнении с зарубежными комплексами непрерывного действия;

– эффективная биологическая защита, допускающая нахождение оператора в непосредственной близости от рентгеновского аппарата;

– специальное конструктивное решение, исключающее действие комплекса на компьютеры и средства связи.

10.4. Обнаружение взрывчатых веществ и взрывных устройств

Наиболее надежными с точки зрения обнаружения взрывоопасных предметов (ВОП) являются средства поиска, обеспечивающие обнаружение прямых признаков. К таким средствам относятся приборы газового анализа (или газоаналитические приборы), приборы, работа

которых основана на так называемых ядерно-физических методах, и специальные химические тесты.

Кроме того, для обнаружения взрывчатых веществ широко используются собаки, специально подготовленные по курсу минно-розыскной службы.

Известно, что все взрывчатые вещества имеют специфический запах. Например, нитроглицерин пахнет очень сильно, тротил – значительно слабее, а некоторые, в частности пластиды, – очень слабо. Однако все эти ВВ могут быть обнаружены с использованием специальных служебно-розыскных собак. Современные газоанализаторы, являясь своеобразной моделью «собачьего носа», тоже могут это делать, но не столь эффективно в отношении пластидов.

Газоанализаторы обнаруживают пары или микрочастицы взрывчатых веществ (ВВ) в пробах воздуха, отбираемых с помощью специальных приспособлений, и по принципу действия делятся на дрейф-спектрометры и газовые хроматографы. Например, портативный детектор МО-2, относящийся к дрейф-спектрометрам, позволяет надежно фиксировать взрывчатые вещества типа ТНТ, НГ, ЭГДН, гексогена, октогена и др. Газовый хроматограф «Эхо-М» представляет собой носимый автономный газоанализатор с сорбционным устройством концентрирования пробы и детектором электронного захвата.

Ввод анализируемой пробы в газоанализатор осуществляется либо за счет всасывания воздуха от поверхности или из щелей обследуемого объекта, либо путем предъявления захваченных на пробоотборник частиц или сорбированных паров ВВ.

Для газоаналитических приборов и собак существует проблема поиска ВВ в герметичных емкостях и поиска взрывоопасных предметов давней закладки в укрывающих средах. Тогда поиск непосредственно ВВ в полностью герметичных емкостях может быть осуществлен только приборами, построенными на использовании ядерно-физических методов.

Анализаторы следов ВВ – это экспресс-тесты, обеспечивающие решение задачи обнаружения и идентификации ВВ по их следовым количествам на поверхностях предметов, одежде и руках человека, в том числе и в течение длительного времени (до нескольких месяцев) после прекращения контакта ВВ с обследуемой поверхностью.

Процесс исследования является быстрым, наглядным и не требует дополнительного лабораторного оборудования. Присутствие следов ВВ определяется по характерному окрашиванию тестовой бумаги с отобранной пробой после ее обработки составами, входящими в комплекты.

Ядерно-физические методы обнаружения взрывчатых веществ основаны на определении элементного состава объекта с помощью зондирующего излучения нейтронами или гамма-квантами. Бета- и гамма-

излучения обладают большой проникающей способностью, поэтому могут эффективно использоваться для зондирования объектов значительных размеров. Физической основой обнаружения является различие элементного состава взрывчатого вещества и среды, в которой оно находится.

Среди известных ядерно-физических приборов интерес представляют нейтронные дефектоскопы, которые позволяют выявлять взрывчатые вещества как объект с повышенным содержанием водорода. Для этого используется слабый источник нейтронов, которые, попадая на ВВ, рассеиваются на атомах водорода и регистрируются приемником. Отечественные нейтронные дефектоскопы типа, «Светлячок» и «Исток-Н» имеют высокую производительность и конструктивно реализованы в портативном варианте. Они предназначены для обнаружения мест закладки недозволенных вложений из водородосодержащих веществ, в том числе взрывчатых и наркотических веществ, за обшивкой и плоскостями транспортных средств.

Резонансно-волновые средства поиска ВВ. Близким к ядерно-физическим методам является использование ядерного квадрупольного резонанса, который позволяет обнаруживать определенные элементы таблицы Менделеева. Так, все взрывчатые (и наркотические) вещества содержат ядра азота N^{14}, обладающие квадрупольными свойствами.

Облучая вещество радиоволной определенной частоты и получив ответный ЯКР-сигнал на данной частоте, можно однозначно говорить о наличии в исследуемом объекте именно данного элемента, т. е. метод ЯКР является не только обнаруживающим, но и идентифицирующим.

Часовые замедлители и исполнительные устройства взрывных устройств являются источником различных демаскирующих физических полей. Например, механические часовые устройства создают вокруг себя акустическое и сейсмическое поле и т.д. В качестве примера подобных устройств можно привести обнаружитель часовых и электронных взрывателей «Пифон-3М», обнаружитель исполнительных механизмов взрывных устройств «Анкер».

Для поиска взрывных устройств по косвенным признакам применяется широкий спектр различных средств обнаружения, а именно – средства визуального контроля, металлоискатели, рентгенотелевизионные установки, нелинейные локаторы.

Технические средства защиты от ВУ и ВВ, их нейтрализации можно разделить на четыре группы:

– постановщики радиопомех, используемые при работе с подозрительными предметами;
– разрушители подозрительных предметов;
– локализаторы подозрительных предметов;
– взрывозащитные средства.

10.5. Нелинейные радиолокаторы

Для обнаружения радиоэлектронных устройств с нелинейными вольтамперными характеристиками (полупроводниковые элементы – диоды, транзисторы, интегральные микросхемы и т. п.) предназначены нелинейные радиолокаторы.

Средства и системы нелинейной локации применяют для обнаружения устройств, содержащих полупроводниковые элементы, в том числе взрывных устройств с радиовзрывателями и электронными таймерами, подслушивающих устройств и скрытых видеокамер, средств съема компьютерной информации и т. п. Объекты поиска могут располагаться в полупроводящей среде (грунте, воде, растительности), внутри автомобилей, в строительных конструкциях зданий, предметах интерьера и т. п. Кроме того, приборы нелинейной локации обеспечивают обнаружение скрыто установленных технических средств съема информации.

В настоящее время существует несколько типов нелинейных радиолокаторов. При выборе локатора важное значение имеет характер предстоящей задачи. При необходимости работы на открытом пространстве или в необорудованном помещении с толстыми стенами целесообразно использовать импульсный локатор большой мощности. При работе в небольших помещениях рекомендуется использовать локатор непрерывного излучения малой мощности, в котором решены проблемы экологической безопасности и электромагнитной совместимости. Локаторы непрерывного излучения: «Энвис», «Обь-1», «Обь-3» и «Обь-2С» необходимо использовать в помещениях, где установлено большое количество электронной техники. Нелинейные локаторы: «Люкс-650», NR-680Y, NR-900E и NR-900 обеспечивают эффективный поиск электронных устройств в элементах интерьера и строительных конструкциях, в том числе кирпичных и бетонных. В целях досмотра труднодоступных мест следует использовать систему «Дозор» – портативное телевизионное устройство с применением нелинейной локации.

10.6. Мониторинг источников радиационного излучения

Наиболее эффективным средством противодействия радиационному терроризму является прежде всего проведение специального контроля на входах и въездах охраняемых объектов. Это обеспечивается за счет установки транспортных и пешеходных радиационных мониторов, фиксирующих изменения текущего значения радиационного фона.

Знание радиационной обстановки в месте проведения операции позволяет правильно установить порог срабатывания прибора, что хотя и

может привести к уменьшению чувствительности, но повышает надежность регистрации.

Принято выделять три ступени радиационного уровня:

– нормальный фон, соответствующий мощности дозы 0,1-0,2 мкЗв/ч (10-20 мкР/ч);

– допустимый фон – 0,2-0,6 мкЗв/ч (20-60 мкР/ч);

– повышенный фон – 0,6-1,2мкЗв/ч (60-120 мкР/ч).

При осуществлении индивидуального радиационного контроля широкое применение находят компактные дозиметры, основным отличием которых от профессиональных приборов является значительно меньшая чувствительность и, как следствие, большее время измерения.

Из многочисленного класса приборов, использующих различные методы регистрации ионизирующих излучений, наиболее часто используются два: газоразрядный счетчик Гейгера – Мюллера и гамма-сигнализаторы *«Радуга», «Клен».* Оба типа приборов просты в обращении и не требуют специальной подготовки пользователя.

Особенность счетчиков Гейгера – Мюллера заключается в их возможности регистрировать различные типы ионизирующих излучений, большой величине выходного сигнала, разнообразии форм и конструкций, достаточно высокой чувствительности и невысокой стоимости.

Достоинством гамма-сигнализаторов является высокая чувствительность к гамма-квантам, а также способность различать и измерять их энергию. Однако их стоимость гораздо выше стоимости счетчиков Гейгера – Мюллера.

Следует отметить, что все рассмотренные устройства позволяют лишь обнаружить радиационное излучение, но не дают возможности ответить на вопрос, какие радиоактивные изотопы стали его причиной. Для этого необходима сложная спектрометрическая аппаратура.

Вопросы для самостоятельной работы

1. Классификация антитеррористических средств.
2. Классификация досмотровой техники.
3. Средства визуального мониторинга.
4. Особенности применения эндоскопов.
5. Классификация рентгенотелевизионных установок.
6. Обнаружение взрывчатых веществ.
7. Демаскирующие признаки взрывных устройств.
8. Обнаружение взрывных устройств.
9. Методы и средства для поиска взрывных устройств по косвенным признакам.
10. Нелинейные радиолокаторы.
11. Мониторинг источников радиационного излучения.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности должно носить комплексный характер и, конечно же, реализация данного принципа во многом зависит от формирования и реализации единой технической политики в области создания, промышленного освоения, контроля за качеством, внедрения и эксплуатационного обслуживания систем охранного мониторинга, поставляемых для подразделений правоохранительных органов в целях охраны имущества и объектов, с использованием инновационных технологий, а также участия в выработке и контроле за исполнением требований к противокриминальной и антитеррористической защищенности объектов и имущества.

Основной целью реализации единой технической политики является повышение противокриминальной и антитеррористической защищенности охраняемых объектов и имущества.

В современных условиях роль систем и комплексов охранного мониторинга в указанной сфере деятельности чрезвычайно высока. Многочисленные исследования в области имущественной безопасности показали, что широкое использование технических средств, систем и комплексов в совокупности с физической охраной и реагированием позволяет если не исключить полностью, то свести к минимуму так называемый «человеческий фактор» в этой цепочке. Именно поэтому необходимо все больше уделять внимание созданию и внедрению в охранную деятельность технических средств и систем на основе последних научных достижений, информационных и коммуникационных технологий.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Конституция Российской Федерации от 12 декабря 1993 г. (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/9004937.

2. О противодействии терроризму (с изменениями на 26 мая 2021 года) : федеральный закон от 6 марта 2006 г. № 35-ФЗ [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/901970787.

3. Технический регламент о требованиях пожарной безопасности (с изменениями на 30 апреля 2021 года) : федеральный закон от 22 июля 2008 г. № 123-ФЗ [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/902111644.

4. О безопасности (с изменениями на 9 ноября 2020 года) : федеральный закон от 28 декабря 2010 г. № 390-ФЗ [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/902253576.

5. О полиции (с изменениями на 30 декабря 2021 года) : федеральный закон от 7 февраля 2011 г. № 3-ФЗ [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/902260215.

6. О войсках национальной гвардии Российской Федерации (с изменениями на 1 июля 2021 года) : федеральный закон от 3 июля 2016 г. № 226-ФЗ [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/420363387.

7. Об одобрении Концепции создания системы обеспечения вызова экстренных оперативных служб через единый номер «112» на базе единых дежурно-диспетчерских служб муниципальных образований : распоряжение Правительства РФ от 25 августа 2008 г. № 1240-р [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/902116522.

8. Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» (с изменениями на 5 апреля 2019 года) : распоряжение Правительства РФ от 3 декабря 2014 г. № 2446-р [Электронный ресурс]. – Режим доступа : https://docs.cntd.ru/document/420238601.

9. ГОСТ Р 50776–95 (МЭК 60839-1-4:1989). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию (с изменениями № 1, 2) = Alarm systems. Part 1. General requirements. Section 4. Code of practice : государственный стандарт Российской Федерации : издание официальное : принят и введен в действие Постановлением Госстандарта России от 22 мая 1995 г. № 256: введен впервые : дата введения 1996-01-01

/ разработан НИЦ «Охрана» ВНИИПО МВД России. – Москва : Издательство стандартов, 1995. – 25 с. – Текст : непосредственный.

10. ГОСТ Р 52436–2005. Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний = Control equipment of intruder and intruder-fire alarm systems. Classification. General technical requirements and test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2005 года № 414-ст : введен впервые : дата введения 2006-09-01 / разработан НИЦ «Охрана» ГУВО МВД России. – Москва : Стандартинформ, 2006. – 17 с. – Текст : непосредственный.

11. ГОСТ Р 52436–2005. Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний = Control equipment of intruder and intruder-fire alarm systems. Classification. General technical requirements and test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2005 года № 414-ст : введен впервые : дата введения 2006-09-01 / разработан НИЦ «Охрана» ГУВО МВД России. – Москва : Стандартинформ, 2006. – 17 с. – Текст : непосредственный.

12. ГОСТ Р 51241–2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний = Access control units and systems. Classification. General technical requirements. Test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. № 430-ст : введен взамен ГОСТ Р 51241–98 : дата введения 2009-09-01 / разработан ФГУ НИЦ «Охрана» МВД России, ЦОРДВО МВД России и ВНИИНМАШ. – Москва : Стандартинформ, 2009. – 39 с. – Текст : непосредственный.

13. ГОСТ Р 53704–2009. Системы безопасности комплексные и интегрированные. Общие технические требования = Complex and integrated security systems. General technical requirements : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 1140-ст : введен впервые : дата введения 2010-09-01 / разработан Международной Ассоциацией «Системсервис», ОАО «Концерн Росбезопасность», ФГУ «НИЦ «Охрана» МВД России, НВП «Болид», ГУ НПО «Специальная техника и связь» МВД России, кафедрой пожарной автоматики Академии ГПС МЧС России, Московским представительством ЗАО «Аргус-Спектр»,

комитетом по отраслевым нормативам и стандартам Ассоциации индустрии безопасности. – Москва : Стандартинформ, 2010. – 37 с. – Текст : непосредственный.

14. ГОСТ Р 53560–2009. Системы тревожной сигнализации. Источники электропитания. Классификация. Общие технические требования. Методы испытаний = Intruder alarm systems. Power supply units. Classification. General technical requirements. Test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 851-ст : введен впервые : дата введения 2010-09-01 / разработан ФГУ НИЦ «Охрана» МВД России и ЦОРДВО МВД России. – Москва : Стандартинформ, 2019. – 11 с. – Текст : непосредственный.

15. ГОСТ Р 54126–2010. Оповещатели охранные. Классификация. Общие технические требования и методы испытаний = Warning devices for intruder alarm systems. Classification. General technical requirements and test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 21 декабря 2010 г. N 822-ст : введен впервые : дата введения 2011-09-01 / разработан ФГУ НИЦ «Охрана» МВД России и ЦОРДВО МВД России. – Москва : Стандартинформ, 2019. – 15 с. – Текст : непосредственный.

16. ГОСТ Р 53325–2012. Техника пожарная. Технические средства пожарной автоматики. Общие технические требования и методы испытаний (с Изменениями № 1, 2, 3) = Fire techniques. Means of fire automatics. General technical requirements and test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2012 г. № 1028-ст : введен взамен ГОСТ Р 53325–2009 : дата введения 2014-01-01 / разработан ФГБУ ВНИИПО МЧС России. – Москва : Стандартинформ, 2014. – 173 с. – Текст : непосредственный.

17. ГОСТ Р 51558–2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний (с Изменением № 1) = Systems and components of video surveillance for security applications. Classification. General requirements. Test procedures : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 октября 2014 г. № 1371-ст : введен взамен ГОСТ Р 51558–2008 : дата введения 2016-01-01 / разработан ФКУ НИЦ «Охрана» МВД России, ЗАО «Нордавинд» и ФГУП ВНИИНМАШ. – Москва : Стандартинформ, 2020. – 28 с. – Текст : непосредственный.

18. ГОСТ Р 52435–2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний (с Изменением № 1) = Alarm intruder technical means. Classification. General technical requirements and test methods : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 октября 2015 г. № 1659-ст : введен взамен ГОСТ Р 52435–2005 : дата введения 2016-05-01 / разработан ФКУ «НИЦ «Охрана» Росгвардии и ФГУП ВНИИНМАШ. – Москва : Стандартинформ, 2016. – 43 с. – Текст : непосредственный.

19. ГОСТ Р 52551–2016. Системы охраны и безопасности. Термины и определения = Protection and security systems. Terms and definitions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2016 г. № 1743-ст : введен впервые : дата введения 2017-07-01 / разработан ФКУ «НИЦ «Охрана» МВД России и ФГУП «ВНИИНМАШ». – Москва : Стандартинформ, 2019. – 31 с. – Текст : непосредственный.

20. ГОСТ Р 57674–2017. Интегрированные системы безопасности. Общие положения = Integrated security systems. General : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2017 г. № 1142-ст : введен впервые : дата введения 2018-06-01 / разработан ФКУ «НИЦ «Охрана» Росгвардии, ЗАО НВП «Болид», ЗАО «Аргус-Спектр», НПФ ООО «Сигма», ООО «Кодос-Б», ООО НПП «АСБ «Рекорд». – Москва : Стандартинформ, 2019. – 10 с. – Текст : непосредственный.

21. ГОСТ Р 58403–2019. Системы беспроводные объектовые охранной сигнализации. Классификация. Общие положения = Alarm security wireless systems for object security. Classification. General : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 23 апреля 2019 г. № 165-ст : введен впервые : дата введения 2019-05-01 / разработан ФКУ «НИЦ «Охрана» Росгвардии. – Москва : Стандартинформ, 2019. – 18 с. – Текст : непосредственный.

22. Р 78.36.002-2010. Рекомендации «Выбор и применение систем охранных телевизионных». – Москва : ФГУ НИЦ «Охрана» МВД России, 2010. – 183 с.

23. Р 78.36.018-2011. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности. – Москва : ФКУ НИЦ «Охрана» МВД России, 2011. – 73 с.

24. Р 78.36.022-2012. Методическое пособие по применению

радиоволновых и комбинированных извещателей с целью повышения обнаруживающей способности и помехозащищенности. – Москва : ФКУ НИЦ «Охрана» МВД России, 2012. – 120 с.

25. Р 78.36.036-2013. Методическое пособие по выбору и применению пассивных оптико-электронных инфракрасных извещателей. – Москва : ФКУ НИЦ «Охрана» МВД России, 2013. – 195 с.

26. Р 78.36.044-2014. Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений. – Москва : ФКУ НИЦ «Охрана» МВД России, 2014. – 92 с.

27. 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». – Москва : ФКУ НИЦ «Охрана» МВД России, 2016. – 92 с.

28. Р 064-2017. Методические рекомендации «Выбор и применение технических средств и систем контроля и управления доступом». – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2017. – 92 с.

29. Р 068-2017. Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок. – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2017. – 110 с.

Основная:

1. Ворона, В. А. Теоретические основы обеспечения безопасности объектов информатизации : учебное пособие : рек. УМО ВО / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. – Москва : Горячая линия – Телеком, 2016. – 304 с. : ил. – ISBN 978-5-9912-0524-5 : 638-40.

2. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2013. – 272 с.

3. Ворона, В. А. Технические системы охранной и пожарной сигнализации / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 374 с.

4. Ворона, В. А. Технические средства наблюдения в охране объектов / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 184 с.

5. Средства анализа изображений в системах охранного телевидения : учебное пособие / С. А. Винокуров, С. А. Гречаный, М. В. Таравков, А. В. Сидоров. – Воронеж : Воронежский институт МВД России, 2017. – 78 с.

6. Аппаратно-программные комплексы охранного мониторинга : учебное пособие / С. А. Винокуров [и др.]. – Воронеж : Воронежский институт МВД России, 2020. – 209 с. – ISBN 978-5-88591-578-6 : 67-11.

Дополнительная:

1. Применение навигационной аппаратуры ГЛОНАСС сотрудниками органов внутренних дел и военнослужащими внутренних войск МВД России : учебное пособие : доп. МВД РФ / А. Н. Бабкин [и др.]. – Воронеж : Воронежский институт МВД России, 2013. – 194 с. – ISBN 978-5-88591-098-9 : 50-33.

2. Средства анализа изображений в системах охранного телевидения : учебное пособие / С. А. Винокуров, С. А. Гречаный, М. В. Таравков, А. В. Сидоров. – Воронеж : Воронежский институт МВД России, 2017. – 78 с.

3. Винокуров, С. А. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч. 1 / С. А. Винокуров, С. А. Гречаный, М. Ю. Покляченко. – Воронеж : Воронежский институт МВД России, 2019. – 165 с. – ISBN 978-5-88591-692-9 : 58-21.

4. Гречаный, С. А. / Повышение эффективности систем охранного телевидения за счет применения алгоритмов видеоаналитики [Электронные методические рекомендации] / С. А. Гречаный [и др.] – Воронеж : Воронежский институт МВД России, 2020. – 1 CD-ROM. – Загл. с титул. экрана. – Текст. Изображение. Устная речь : электронные.

5. Применение средств интеграции для обеспечения комплексной безопасности объектов : методические рекомендации / С. А. Винокуров, С. А. Гречаный, М. В. Таравков, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2020. – 227 с.

Учебное издание

Винокуров Станислав Анатольевич
Гречаный Сергей Анатольевич
Таравков Михаил Владимирович
Толстых Ольга Владимировна

Системы охранного мониторинга

Курс лекций

Редактор Н. Ф. Палихова
Компьютерная верстка М. В. Таравков

Подписано в печать 20.09.2021. Формат 60×84 $^{1}/_{16}$
Усл. печ. л. 9,3
Тираж 100 экз. Заказ № 245

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53