ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

МОСКОВСКИЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ (ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

П.В. Бондарев, А.В. Измайлов, А.И. Толстой

ФИЧЕСКАЯ ЗАЩИТА ЯДЕРНЫХ ОБЪЕКТОВ

Под редакцией Н.С. Погожина

Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений

Москва 2008

УДК 654/924(075)
ББК 67.401.213я7
Б81

Бондарев П.В.
Физическая защита ядерных объектов: Учебное пособие для вузов/ П.В. Бондарев, А.В. Измайлов, А.И. Толстой; Под ред. Н.С. Погожина. – М.: МИФИ, 2008. – 584 с.: илл.

В учебном пособии рассмотрены основы построения и проектирования систем физической защиты (СФЗ) ядерных объектов. Определены основные функции СФЗ и ее основные подсистемы. Рассмотрены особенности отдельных подсистем СФЗ. Описаны методы оценки и анализа и методы обеспечения информационной безопасности СФЗ.

Предназначено студентов, обучающихся по специальности «Безопасность и нераспространение ядерных материалов» и специализирующихся в рамках магистерской образовательной программы «Физическая защита, учет и контроль ядерных материалов». Также учебное пособие может быть полезно аспирантам и специалистам, работающим в данном направлении.

Пособие подготовлено в рамках
Инновационной образовательной программы

Рецензент проф. РГГУ В.Б. Кравченко

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ

АСБТ	–	автоматизированная система обеспечения безопасности транспортирования
БС	–	биометрическая система
БСТ	–	базовая станция
ВЗ	–	внутренняя зона
ВМ	–	видеомагнитофон
ГО	–	глубина обзора
ЖВЦ	–	жизненно-важные центры
ЗЗ	–	защищенная зона
ЗИ	–	защита информации
ЗОД	–	зона ограниченного доступа
ИБ	–	информационная безопасность
ИТСФЗ	–	инженерно-технические средства физической защиты
КСП	–	контрольно-следовая полоса
КП	–	контрольная панель
КТСФЗ	–	комплекс инженерных и технических средств физической защиты
КУД	–	контроль и управление доступом
МК	–	матричный коммутатор
МН	–	модель нарушителей
НСД	–	несанкционированный доступ
ОВЗ	–	особо важная зона
ОС	–	операционная система
ПБ	–	политика безопасности
ПЗС	–	прибор с зарядовой связью
ПНСД	–	последствия несанкционированных действий
ПТН	–	подсистема телевизионного наблюдения
ПУ	–	преграждающее устройство

ПУП – пульт управления
ПЦО – пункт централизованной охраны
ПФЗ – предметы физической защиты
ПЭМИН – побочные электромагнитные излучения и наводки
РЭС – радиоэлектронные средства
САЗ – система активной защиты
СВТ – средства вычислительной техники
СКЗИ – средства криптографической защиты информации
СКУД – система контроля и управления доступом
СПДН – схема последовательности действий нарушителя
СО – средство обнаружения
СПИ – система передачи извещений
СТН – система телевизионного наблюдения
СТР – специальные требования и рекомендации
СО – средства обнаружения
СУиК – система учета и контроля
СФЗ – система физической защиты
СФЗУиК – системы физической защиты, учета и контроля
УВИП – устройство ввода идентификационных признаков
ТВЛ – телевизионные линии
ТД – точка доступа
ТК – телекамера
ТФОП – телефонная сеть общего пользования
ТСР – транкинговая система радиосвязи
ТСФЗ – технические средства физической защиты
УАТС – учрежденческие АТС
УМ – уязвимые места
УПУ – устройство преграждающее управляемое
УУ – управляющее устройство
ФБ – физический барьер
ФЗ – физическая защита

ЦПН	–	центральный пульт наблюдения
ЧТЗ	–	частное техническое задание
ЧЭ	–	чувствительный элемент
ШС	–	шлейф сигнализации
ЭЛТ	–	электронно-лучевая трубка
ЯМ	–	ядерные материалы
ЯО	–	ядерный объект

Предисловие

Основой для учебного пособия послужил опыт преподавания в МИФИ учебного цикла «Проектирование систем физической защиты ядерно-опасных объектов» в рамках учебного плана магистратуры «Физико-технические проблемы атомной энергетики» по образовательной программе «Физическая защита, учет и контроль ядерных материалов» и учебного плана специальности «Безопасность и нераспространение ядерных материалов» (направление подготовки «Ядерные физика и технологии»). Данные учебные программы были реализованы в рамках Российско-американского образовательного проекта.

В подготовке учебного пособия участвовали преподаватели факультета «Информационная безопасность» МИФИ и специалисты ФГУП «СНПО «ЭЛЕРОН»».

В настоящее время подготовка специалистов по физической защите, учету и контролю ядерных материалов ведется не только в МИФИ, но при этом существенно ограничена поддержка обучения узкопрофильной учебной литературой. Представляемое учебное пособие поможет в решении данной проблемы.

Основная задача данной книги – предоставить обучающимся систематизированный подход к решению проблемы обеспечения физической защиты ядерных объектов.

Учебное пособие состоит из введения, двенадцати глав, библиографии и списка сокращений.

Первая глава (подготовил Толстой А.И.) посвящена основам методологии проектирования систем физической защиты и обеспечения физической безопасности любого объекта.

Во второй главе (Бондарев П.В.) представлены данные о составе подсистемы обнаружения. Приведены классификации датчиков обнаружения по физическому принципу функционирования и по способу применения.

В третьей главе (Толстой А.И.) рассмотрены особенности подсистемы контроля доступа, ее структура и функциональный состав. Описаны основные методы и средства аутентификации субъектов, в том числе биометрические технологии.

В четвертой главе (Бондарев П.В.) представлена информация о подсистеме телевизионного наблюдения. Определены основные цели ее использования. Рассмотрены характеристики элементов подсистемы и каналов передачи видеоизображения.

В пятой главе (Бондарев П.В.) описаны особенности подсистемы сбора и обработки информации. Определено назначение станций сбора и обработки информации, рассмотрены технологии передачи данных и методы контроля линий связи, описаны особенности оборудования для станций сбора и обработки информации.

В шестой главе (Бондарев П.В.) основное внимание уделено особенностям подсистемы задержки, включающей различные заграждения и элементы конструкций зданий.

В седьмой главе (Бондарев П.В.) кратко сформулированы требования к подсистеме ответного реагирования и связи, рассмотрены их задачи и функции.

В восьмой главе (Толстой А.И.) рассмотрены особенности системы физической защиты ядерных объектов.

В девятой главе (Измайлов А.В.) рассмотрены вопросы создания и совершенствования систем физической защиты ядерных объектов.

В десятой (Измайлов А.В.) рассмотрены вопросы физической защиты ядерных материалов при их перевозке.

В одиннадцатой главе (Измайлов А.В.) рассмотрены вопросы, связанные с оценкой эффективности систем физической защиты ядерных объектов.

В двенадцатой главе (Толстой А.И.) представлены материалы, относящиеся к методам обеспечения информационной безопасности систем физической защиты ядерных объектов.

В написании отдельных глав учебника также принимали участие Давыдов Ю.Л. (десятая глава) и Скворцов Д.А. (одиннадцатая глава).

В конце учебника представлен общий список литературы как использованной, так и рекомендуемой.

В качестве методической основы подготовки данного учебного пособия была использована методическая разработка «Методика проектирования систем физической защиты» [П.1], подготовленная и переданная МИФИ Сандийской национальной лабораторией США, и учебные пособия «Системы физической защиты ядерно-опасных объектов» [П.2], «Информационная безопасность систем физической защиты, учета и контроля ядерных материалов» [П.3] и «Методы проектирования и анализа эффективности систем физической защиты ядерных материалов и установок» [П.4], подготовленные в МИФИ.

Авторы признательны коллегам по факультетам «Информационная безопасность» и «Физико-технический» МИФИ, а также представителям Национальных лабораторий США – участникам Российско-американского образовательного проекта – за поддержку в подготовке данного учебного пособия.

Авторы не претендуют на исчерпывающее изложение всех названных аспектов проблемы обеспечения физической защиты ядерно-опасных объектов, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей в дальнейшей своей работе.

Н.С. Погожин

Введение

В настоящее время ключевой задачей безопасного использования современных ядерных технологий является обеспечение режима нераспространения ядерных материалов. Составляющая этой проблемы – создание и эксплуатация эффективных систем физической защиты ядерных объектов (ЯО).

Под системой физической защиты объекта будет пониматься комплекс мер, включающих нормативные документы, организационные и технические меры, направленные на обеспечение безопасности ЯО и ядерных материалов. Необходимо отметить, что понятие «физическая защита объекта» все более часто используется в современной практике создания и эксплуатации подобных систем, постепенно вытесняя использование более традиционных понятий таких, как «инженерно-техническая защита объекта», «инженерная защита и техническая охрана объекта», которые имеют тот же смысл. В дальнейшем мы будем использовать первый вариант, как наиболее приемлемый в случае рассмотрения ядерных объектов.

Тенденция развития современных систем физической защиты любых объектов вообще и ЯО в частности связана с использованием новейших разработок технических средств с переходом к интегрированным системам безопасности, представляющим собой сложные территориально распределенные автоматизированные системы сбора и обработки информации о состоянии охраняемого объекта в совокупности с необходимыми организационными мероприятиями по охране и реагированию.

На ядерном объекте система физической защиты имеет свои особенности. Создание такой системы и ее эксплуатация требуют определенных подходов, знание которых необходимо специалистам по физической защите, учету и контролю ядерных материалов.

Систематизации методов и средств с учетом комплексного характера функционирования систем физической защиты посвящено данное учебное пособие. Материал, помещенный в основных главах учебного пособия, выстроен таким образом, чтобы его изучение шло от общих методов построения подобных систем к описанию средств, используемых в отдельных подсистемах. При этом ставится задача учета особенностей, которыми отличаются системы физической защиты ЯО от подобных на других объектах.

1. МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

Методологические основы построения систем физической защиты объектов, рассмотренные в данной главе, целесообразно использовать при проектировании, разработке и сертификации СФЗ, а также при оценке ее уязвимости и эффективности. Знания методологических основ полезны также для специалистов по физической защите, которые эксплуатируют конкретные системы физической защиты.

При создании СФЗ любого объекта, независимо от его характера, должны быть пройдены этапы, которые отрабатывались на основе достаточно обширного опыта разработки, создания и эксплуатации СФЗ. Обобщенная совокупность используемых при этом подходов составляет методологическую основу построения СФЗ [П.1, П.2, 1.1-1.3]. Данные подходы относятся к решению следующих задач:

- определение характеристик и особенностей объекта, которые необходимо учитывать при создании его СФЗ;
- определение задач, которые должна решать СФЗ;
- определение функций, которые должна выполнять СФЗ;
- формулировка принципов построения СФЗ;
- определение перечня угроз безопасности объекта;
- определение модели нарушителя;
- определение структуры СФЗ;
- определение этапов проектирования СФЗ.

Рассмотрим более подробно выделенные задачи.

1.1. Определение характеристик и особенностей объекта

Определение характеристик и особенностей объекта предполагает описание самого объекта и всех процессов, имеющих место на данном объекте.

При описании объекта в целом необходимо подробно определить границы территории объекта, описать расположение зданий, планировку зданий и определить все точки доступа на территорию объекта.

Определение природы ведущихся на объекте работ, характеристик операций, выполняемых на объекте, и условий их выполнения позволяет сформировать понимание ограничений, связанных с характером выполняемых на объекте операций, и связать их с ограничениями, накладываемыми требованиями по обеспечению безопасности объекта.

Характеристики объекта определяются посредством идентификации всех операций, условий и физических характеристик, которые каким-либо образом могут повлиять на систему физической защиты. Подробное, исчерпывающее описание объекта позволяет сформулировать требования к его системе физической защиты объекта.

1.2. Определение задач, которые должна решать СФЗ

При создании системы физической защиты объекта решаются следующие задачи, которые формулируются в виде целей:

1. Предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения материальных ценностей.

2. Защита объекта от воздействия стихийных сил и прежде всего, пожара и воды.

Решение этих задач направлено на сведение к минимуму возможностей несанкционированного проникновения на объект и к его жизненно важным центрам, вероятности осуществления актов промышленного шпионажа и последствий от воздействия стихии.

При решении указанных выше задач необходимо учитывать большое число различных факторов, что не удается, как правило, выполнить на основе здравого смысла. Поэтому основы физической защиты должны содержать как теоретические знания, так и методические рекомендации.

1.3. Определение функций, которые должна выполнять СФЗ

Хищение и саботаж на территории объекта могут быть предотвращены двумя способами: путем удержания нарушителей от совершения нежелательных действий или путем успешного противодействия нарушителям.

Удержание обеспечивается внедрением системы физической защиты, которую потенциальные нарушители рассматривают как непреодолимое препятствие, что делает данный объект непривлекательной для них целью. Связанная с методом удержания проблема состоит в том, что измерить эффективность удержания невозможно. Было бы ошибкой предполагать, что система защиты успешно удерживает нарушителей от попыток проникновения на территорию объекта только потому, что таких попыток не наблюдалось.

Противодействие нарушителям предусматривает определенные меры охраны объекта или сил ответного действия, предотвращающие достижение нарушителями их цели уже после начала фактических действий, направленных на совершение диверсии на объекте. Существуют несколько функций, которые должна выполнять система физической защиты. Важно рассмотреть эти функции системы достаточно подробно, так как для оценки всей системы в це-

лом необходимы исчерпывающее понимание определений этих функций и способность к измерению эффективности выполнения каждой из этих функций. Ниже перечислены основные функции СФЗ (рис. 1.1).

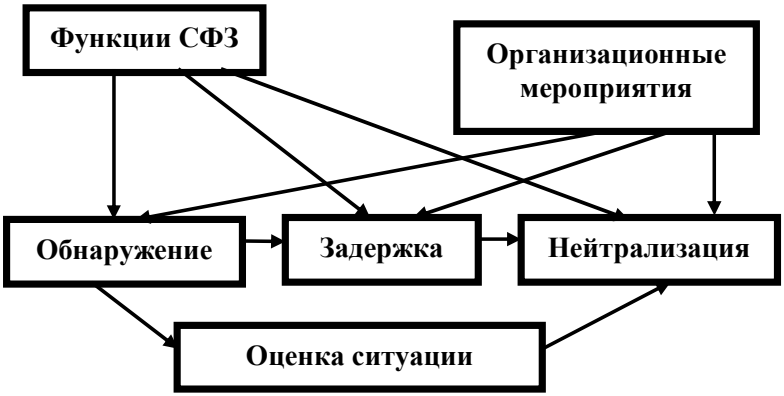


Рис. 1.1. Функции СФЗ

Обнаружение. Обнаружение определяется как раскрытие действий, совершаемых нарушителями. К функции обнаружения относится оповещение о тайных или открытых действиях нарушителей с помощью датчиков (извещателей), систем контроля доступа или систем телевизионного наблюдения.

Датчики или извещатели могут быть внешними (контролирует внешнюю границу объектов) и внутренними (устанавливаются внутри объекта).

Система контроля доступа осуществляет пропускной контроль: допуск на территорию объекта или отдельного участка объекта лиц, имеющих соответствующие полномочия, и обнаружение попыток проникновения на такую территорию неуполномоченных лиц или попыток вноса на территорию неразрешенных материалов.

Задачей системы телевизионного наблюдения является наглядное представление видеоинформации об оперативной обстановке на объекте. Поэтому данная система может использоваться и для обнаружения нарушителей.

Для того чтобы действия нарушителей были раскрыты, необходимо, чтобы произошли следующие события в указанной последовательности (рис. 1.2).

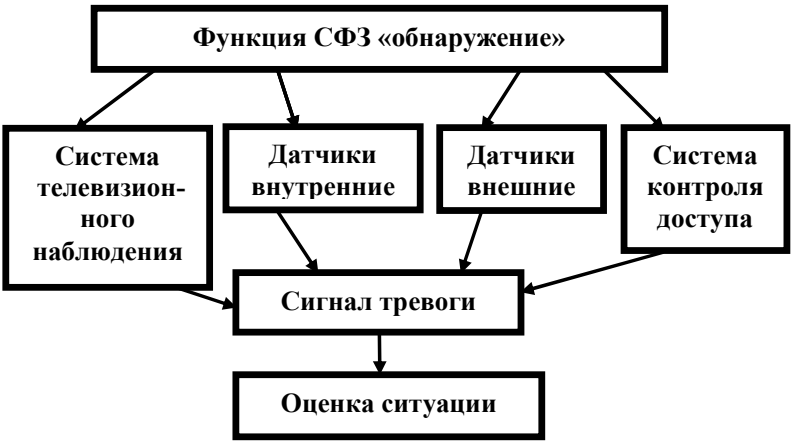


Рис. 1.2. Порядок обнаружения

•Датчики (внешние, внутренние), система контроля доступа или система телевизионного наблюдения регистрирует необычное явление и передает сигнал тревоги.

•Информация, переданная датчиком, элементами системы контроля доступа или системы телевизионного наблюдения подсистеме оценки аварийной ситуации, регистрируется и выводится на устройства отображения (например, дисплей).

•Ответственное лицо оценивает полученную информацию и решает, является ли переданный сигнал тревоги действительным или ложным. Если выносится решение, что полученный сигнал тревоги недействителен (т.е. передан в результате воздействия помех), обнаружение не имеет места. В случае, если сигнал действителен, имеет место обнаружение действий нарушителей.

Эффективность выполнения функции обнаружения определяется следующими характеристиками:

•вероятность обнаружения;

•продолжительность времени, затрачиваемого на передачу информации и оценку аварийной ситуации;

•частота передачи ложных сигналов тревоги.

Эффективность выполнения функции обнаружения измеряется с помощью таких характеристик, как вероятность обнаружения действий нарушителей датчиками (*Ps*) и суммарное время, необходимое для передачи сигнала тревоги, оповещения и оценки действительности сигнала тревоги (*T*), что отображает график на рис. 1.3.

Датчик срабатывает в момент времени *T*0. Через некоторое время, например в момент времени *T*1, *T*2 или *T*3, ответственное лицо получает информацию, переданную датчиком и подсистемами оценки аварийной ситуации. Если время, прошедшее с момента срабатывания датчика до момента определения действительности сигнала тревоги (*T*), невелико, вероятность обнаружения (*Ps*) будет близка к вероятности срабатывания датчика при совершении неразрешенных действий. Вероятность обнаружения понижается по мере увеличения продолжительности времени оценки аварийной ситуации.

Количественными характеристиками, позволяющими измерять эффективность пропускного контроля, являются нагрузка пропускного пункта, коэффициент ошибочных пропусков и коэффициент

ошибочных задержаний. Нагрузкой пропускного пункта называется количество уполномоченных лиц, проходящих через данный пропускной пункт за единицу времени; при определении этой характеристики допускается, что все пытающиеся пройти через пропускной пункт лица имеют соответствующие полномочия или разрешения. Коэффициент ошибочных пропусков определяется как количество неуполномоченных лиц, проходящих через данный пропускной пункт по подложным пропускам или удостоверениям за единицу времени. Как коэффициент ошибочных пропусков, так и коэффициент ошибочных задержаний снижаются, если снижается общая нагрузка пропускного пункта. Снижение нагрузки пропускного пункта может, однако, неблагоприятно повлиять на эксплуатационные характеристики объекта.

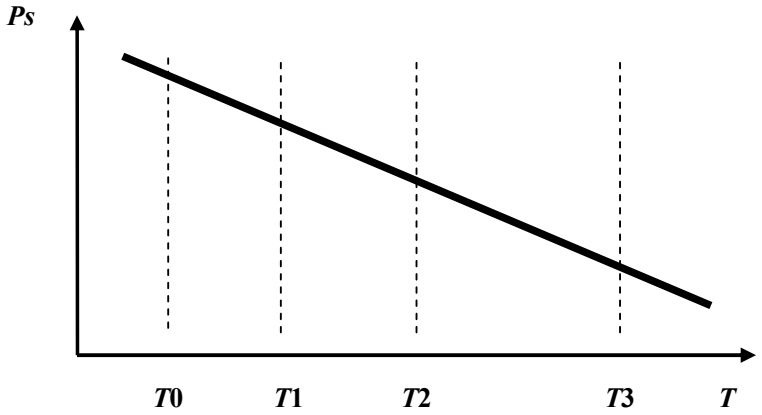


Рис. 1.3. Зависимость вероятности обнаружения (*Ps*) от суммарного времени, необходимого для передачи сигнала тревоги, оповещения и оценки действительности сигнала тревоги

Количественными характеристиками, позволяющими измерять эффективность пропускного контроля, являются нагрузка пропускного пункта, коэффициент ошибочных пропусков и коэффициент ошибочных задержаний. Нагрузкой пропускного пункта называется количество уполномоченных лиц, проходящих через данный пропускной пункт за единицу времени; при определении этой характеристики допускается, что все пытающиеся пройти через пропускной пункт лица имеют соответствующие полномочия или разрешения. Коэффициент ошибочных пропусков определяется как количество неуполномоченных лиц, проходящих через данный пропускной пункт по подложным пропускам или удостоверениям за единицу времени. Как коэффициент ошибочных пропусков, так и коэффициент ошибочных задержаний снижаются, если снижается общая нагрузка пропускного пункта. Снижение нагрузки пропускного пункта может, однако, неблагоприятно повлиять на эксплуатационные характеристики объекта.

Функция обнаружения может быть выполнена также силами охраны или персоналом объекта. Охранники, находящиеся на стационарных постах или патрулирующие объект, могут сыграть критическую роль в процессе обнаружения нарушителей.

Эффективная система оценки аварийной ситуации предоставляет два вида информации: информацию о том, является ли переданный сигнал тревоги действительным, и информацию о том, чем или кем был вызван сигнал тревоги, где это произошло, и сколько человек участвуют в диверсии.

Задержка — вторая функция системы физической защиты. Выполнение этой функции состоит в замедлении продвижения нарушителей. Задержка может быть обеспечена заграждениями, замками и механическими (активируемыми) средствами задержки. Отряды охраны объекта могут рассматриваться в качестве элементов задержки, если они занимают стационарные и хорошо защищенные позиции.

Эффективность выполнения функции задержки измеряется продолжительностью времени, необходимого нарушителям (после их обнаружения) для преодоления каждого элемента задержки. Несмотря на то, что задержка нарушителей может иметь место до их обнаружения, такая задержка не повышает эффективности системы физической защиты, так как она не предоставляет охране или силам ответного действия никакого дополнительного времени на развертывание и перехват.

Ответные действия. Функция ответного действия определяется как действия, предпринимаемые охраной или специальным защищающим объект подразделением для предотвращения успешного выполнения нарушителями своей задачи. Эффективность выполнения функции ответного действия измеряется продолжительностью времени, проходящего с момента получения сообщения о действиях нарушителей до момента их нейтрализации.

Ответные действия состоят в перехвате и нейтрализации нарушителей. Перехват определяется как прибытие сил ответного действия на тот участок территории объекта, где они могут остановить продвижение нарушителей. Перехват предусматривает поддержание связи с передачей охране объекта точной информации о действиях нарушителей и развертывании сил ответного действия.

Эффективность поддержания связи с силами ответного действия измеряется вероятностью поддержания бесперебойной связи и продолжительностью времени, необходимого для передачи сообщений. Вероятность поддержания бесперебойной связи и время передачи сообщений взаимозависимы. Количество времени, проходящего с момента передачи первоначального сообщения, может значительно изменяться в зависимости от метода поддержания связи. По прошествии этого первоначального периода вероятность поддержания бесперебойной связи начинает быстро возрастать. С каждым повторением сообщения вероятность передачи точной текущей информации возрастает.

Таким образом, СФЗ должна выполнять функции обнаружения, задержки и ответного действия. Эти функции должны быть выполнены на протяжении периода времени, продолжительность которого меньше, чем продолжительность времени, требуемого для выполнения нарушителями их задачи. На рис. 1.4 показано соотношение времени, необходимого для выполнения задачи нарушителями, и времени, необходимого для выполнения своих функций системой физической защиты.

Все время в совокупности, необходимое нарушителям для выполнения их задачи, обозначается как «время выполнения задачи». Продолжительность этого времени зависит от эффективности задержки, обеспечиваемой системой физической защиты. Нарушители могут начать выполнение своей задачи несколько ранее подачи первого сигнала тревоги, в момент, обозначенный на диаграмме *T*0. Время выполнения задачи нарушителями изображается прерывистой линией до момента *T*0, так как перед обнаружением функция задержки не играет роли. После передачи первого сигнала тревоги полученная информация должна быть зарегистрирована и оценена с определением действительности сигнала тревоги. Время окончания оценки действительности сигнала тревоги обозначено на диаграмме как момент *Ta*: в этот момент информация о местонахождении нарушителей должна быть передана персоналу сил ответного действия. Затем определенное время необходимо для развертывания надлежащего количества сил ответного действия, располагающих соответствующим оборудованием, необходимым для перехвата и нейтрализации нарушителей.

Рис. 1.4. Зависимость времени выполнения задачи нарушителей от требований к системе защиты

Все время в совокупности, необходимое нарушителям для выполнения их задачи, обозначается как «время выполнения задачи». Продолжительность этого времени зависит от эффективности задержки, обеспечиваемой системой физической защиты. Нарушители могут начать выполнение своей задачи несколько ранее подачи первого сигнала тревоги, в момент, обозначенный на диаграмме *T*0. Время выполнения задачи нарушителями изображается прерывистой линией до момента *T*0, так как перед обнаружением функция задержки не играет роли. После передачи первого сигнала тревоги полученная информация должна быть зарегистрирована и оценена с определением действительности сигнала тревоги. Время окончания оценки действительности сигнала тревоги обозначено на диаграмме как момент *Ta*: в этот момент информация о местонахождении нарушителей должна быть передана персоналу сил ответно-

го действия. Затем определенное время необходимо для развертывания надлежащего количества сил ответного действия, располагающих соответствующим оборудованием, необходимым для перехвата и нейтрализации нарушителей.

Момент, в который силы ответного действия перехватывают и нейтрализуют нарушителей, обозначен *Ti*, а момент выполнения нарушителями их задачи *Tc*. Очевидно, что для того чтобы система физической защиты могла выполнить свою функцию, момент *Ti* должен наступить раньше момента *Tc*. Очевидно также, что обнаружение (т.е. передача первого сигнала тревоги) должно произойти как можно раньше, и момент *T*0 (а также моменты *Ta* и *Ti*) должен находиться в точке, расположенной как можно ближе к началу оси отсчета времени.

1.4. Принципы построения систем физической защиты

Так как службе безопасности объекта, обеспечивающей его физическую защиту, могут противодействовать нарушители, оснащенные средствами, находящимися на острие научно-технического процесса, то возможности системы физической защиты не должны, по крайней мере, уступать возможностям потенциальных нарушителей. Исходя из этого в основу физической защиты должны быть положены следующие *общие* принципы [1.1]:

- непрерывность защиты, характеризующая постоянную готовность СФЗ к отражению угроз безопасности объекта;
- активность, предусматривающая прогнозирование действий нарушителей, разработку и реализацию опережающих мер по защите;
- скрытность, исключающая ознакомление посторонних лиц со средствами и процедурами защиты;

•целеустремленность, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценным составляющим объекта;

•комплексное использование различных способов и средств защиты.

Общие принципы не содержат конкретных рекомендаций. Они определяют общие требования, которые необходимо учитывать при проектировании, создании и эксплуатации СФЗ конкретного объекта.

Следующая группа принципов характеризует основные профессиональные подходы к организации физической защиты, обеспечивает рациональный уровень защищенности объекта и позволяет сократить затраты на создание и эксплуатацию СФЗ:

•многозональность систем физической защиты, предусматривающая разбиение объекта на зоны с контролируемым уровнем защиты;

•многорубежность защиты на пути движения нарушителя;

•равнопрочность (сбалансированность) защиты.

Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к различным составляющим объекта путем разделения его пространства на контролируемые зоны. Такими зонами могут являться, например:

•территория, занимаемая объектом и имеющая внешнюю границу;

•здание на территории объекта;

•коридор или его часть в здании;

•помещение в здании.

Пример расположения зон показан на рис. 1.5. Зоны могут быть независимыми (например, отдельные здания на территории объекта) или вложенными, как это показано на рис. 1.5.

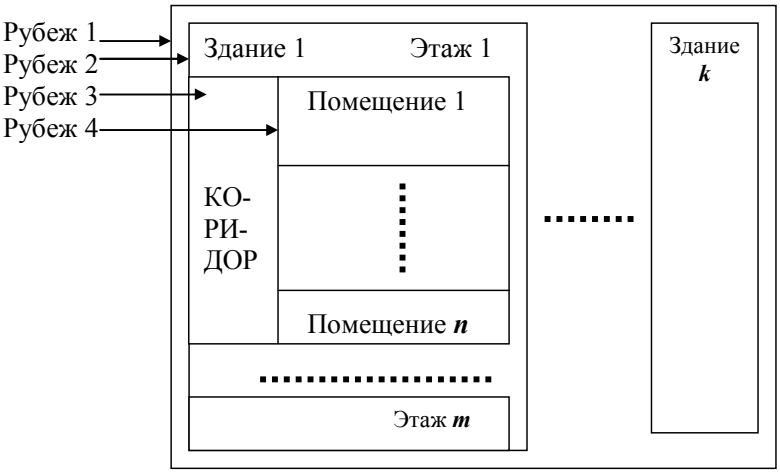


Рис. 1.5. Принцип многозональности и многорубежности

С целью воспрепятствования проникновения нарушителя в конкретную зону на ее границе создаются один или несколько рубежей защиты. Разбиение объекта на рубежи защиты соответствует принципу **многорубежности**.

Совокупность многозональности и многорубежности обеспечивает эшелонированную защиту объекта.

Эшелонированная защита означает, что для достижения своей цели нарушители должны обойти или преодолеть определенное количество последовательных защитных элементов (рубежей защиты). Например, предположим, что нарушители должны проникнуть через три различных заграждения перед тем, как они смогут войти в некоторое помещение. Время, необходимое для преодоле-

ния каждого из трех заграждений, может быть различным, и эффективность каждого заграждения также может быть неодинаковой, но каждое из заграждений потребует от нарушителей приложения усилий в различных точках по мере их продвижения по маршруту. Таким образом, эшелонированная защита оказывает следующее воздействие на нарушителей:

- увеличивает у нарушителей неопределенность представления о возможностях СФЗ (их неуверенность);
- требует от нарушителей более тщательной подготовки к преодолению рубежей защиты;
- создает дополнительные преграды, которые могут заставить нарушителей отказаться от своих намерений или прервать свои действия.

Эшелонированная защита сводит к минимуму последствия отказов компонентов СФЗ. Маловероятно, что когда-либо будет разработана такая система, ни один из компонентов которой не откажет на протяжении всего срока ее эксплуатации. Причинами отказа компонентов системы физической защиты могут служить самые различные явления (например, факторы воздействия окружающей среды, проявление дефектов самих компонентов, целенаправленные действия нарушителей). Несмотря на то, что важно знать причину отказа компонента для восстановления нормального режима эксплуатации системы, еще более важно разработать планы действия в непредвиденных обстоятельствах, гарантирующие функционирование системы при возникновении неожиданных явлений. Предъявление требований, предусматривающих автоматическое выполнение части таких планов (например, требование об автоматическом включении оборудования, дублирующего функции отказавших компонентов) в некоторых случаях весьма желательно.

Равнопрочность (сбалансированность) защиты означает, что независимо от того, каким способом нарушители попытаются дос-

тичь своей цели, им придется встретиться с эффективными элементами системы физической защиты. Рассмотрим для примера защитную поверхность, окружающую некоторое помещение. Эта поверхность может включать:

•стены, полы и потолки нескольких типов;

•двери нескольких типов; люки для оборудования в полах и потолках;

•отверстия систем обогрева, вентиляции и кондиционирования воздуха с решетками различных типов.

В полностью сбалансированной системе защиты минимальное время, необходимое для преодоления каждого из этих заграждений, будет одинаковым, и минимальная вероятность обнаружения проникновения через каждое из этих заграждении будет одинаковой. Тем не менее, полностью сбалансированная система, скорее всего, невозможна или даже нежелательна. Некоторые элементы, такие, как стены, могут быть чрезвычайно труднопреодолимыми не потому, что таковы требования, предъявляемые к системе физической защиты, а потому, что таковы конструкционные требования. Двери, люки и решетки могут обеспечивать значительно менее продолжительную задержку, нежели стены, и все же могут считаться адекватными элементами задержки.

Введение излишних элементов защиты, например, установка дорогостоящих бронированных дверей, проникновение через которые может занять несколько минут, не дает никаких преимуществ, если стены построены из гофрированного асбеста, через которые можно проникнуть в течение нескольких секунд, пользуясь ручным переносным инструментом.

Наконец, элементы, рассчитанные на защиту от какого-либо одного вида угрозы, не следует удалять лишь потому, что они дублируют элемент, защищающий от другого вида угрозы. Задача состоит в том, чтобы обеспечить адекватную защиту от всех видов

угроз на всех возможных маршрутах продвижения нарушителей и учитывать при этом другие соображения, относящиеся, например, к стоимости работ, безопасности персонала и конструкционной целостности объекта.

1.5. Определение перечня угроз безопасности объекта

Под угрозой безопасности объекта будем понимать потенциальную возможность нанесения объекту определенного вида ущерба. В общем случае эти угрозы могут проявиться в результате:

- действий нарушителей;
- воздействия стихийных сил;
- сбоев в работе средств СФЗ;
- воздействия субъективного фактора, связанного с непреднамеренными ошибками персонала объекта, недостаточного уровня его квалификации.

Угрозы разделяют на внешние и внутренние исходя из направления их проявления по отношению к границам объекта. При рассмотрении различных угроз необходимо учитывать также способы их осуществления. Данные факторы определяют уязвимые места объекта и его СФЗ, что очень важно при анализе их уязвимости.

Для составления перечня угроз необходимо:

- определить исходные данные;
- собрать информацию о возможных видах угрозы;
- привести эту информацию в пригодный для дальнейшего использования вид.

Каждый из этих этапов имеет большое значение для разработки окончательного определения угрозы определенному объекту.

К исходным данным относится информация о потенциальных нарушителях, о стихийных бедствиях, которые могут проявиться в

местности, где располагается защищаемый объект, а также о специфике объекта и характеристиках его персонала.

Обобщение информации о потенциальных нарушителях обычно представляется в виде его модели. В связи с важностью этого вопроса модель нарушителя будет описана в отдельном параграфе.

Сбор информации о возможных видах угроз связан с использованием различных источников информации. Разведывательные организации могут предоставить подробную информацию о группах, которые могут представлять угрозу для объектов. Изучение истории преступности и преступности в настоящем позволяет иногда получить информацию, полезную для определения характеристик возможной угрозы. Неправительственные структуры обмена информацией, такие как конференции и встречи различных профессиональных организаций, время от времени дают доступ к информации, помогающей произвести оценку существующей угрозы. Электронные базы данных, текущие периодические издания и литература содержат обширную информацию, относящуюся к различным видам угроз.

Собранная таким образом информация может быть представлена в табличной форме и обобщена с тем, чтобы различные угрозы можно было перечислить в порядке, соответствующем степени потенциальной опасности, которую они представляют для определенного объекта. Результатом такого процесса является информация, имеющая большую ценность для проектировщика системы физической защиты.

Необходимо отметить принципиальную сложность составления приоритетного перечня угроз для конкретного объекта. Она связана с тем, что проявление определенной угрозы связано со многими неопределенностями. Некоторые из них носят случайный характер (например, стихийные бедствия или неисправности оборудования). Поэтому количественные оценки величины угрозы связаны с ее вероятностными характеристиками.

1.6. Определение модели нарушителя

Для определения модели нарушителя необходимо получить информацию о:

- категории нарушителя и его возможных тактических методах;
- возможных действиях нарушителя;
- причинах и мотивах действий нарушителя;
- возможностях нарушителя.

Нарушители подразделяются на три категории: внешние, внутренние и внешние нарушители в сговоре с внутренними (рис. 1.6).

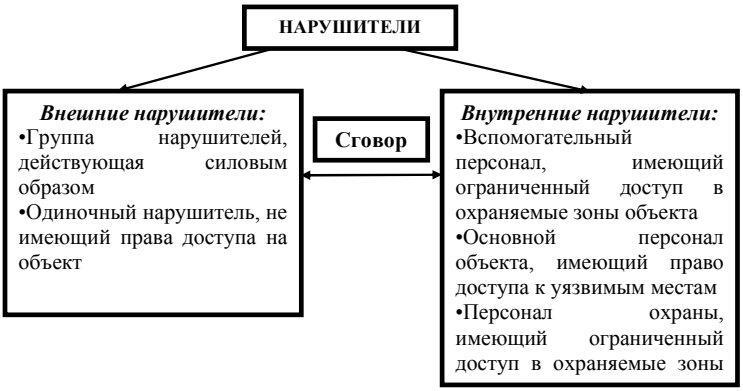


Рис. 1.6. Категории нарушителей

Рассмотрим особенности этих нарушителей исходя из влияния на безопасность объекта.

Внешний нарушитель имеет намного больше сложностей в проникновении на объект, плохо ориентируется на объекте и легко заметен. Это способствует его обнаружению. Усложняют проблему обеспечения безопасности объекта те факты, что внешний наруши-

тель проявляется внезапно, зачастую неизвестен заранее и может быть вооружен.

В противоположность внешнему нарушителю внутренний нарушитель хорошо ориентируется на объекте и может иметь необходимые права доступа в защищаемые зоны. Это существенно затрудняет противодействие его замыслам. Положительным моментом является то, что он известен как сотрудник объекта.

Решение проблемы нейтрализации угрозы, появляющейся от действий внутреннего нарушителя в сговоре с внешним, усложняется из-за совокупности тех отрицательных качеств, которые присущи внутреннему и внешнему нарушителю.

К внешним нарушителям могут относиться движимые различными мотивами преступные элементы. К внутренним нарушителям могут относиться враждебно настроенные служащие, преследующие вполне определенные цели. Третья категория объединяет усилия внутренних и внешних нарушителей, причем сотрудники вступают в сговор с внешними нарушителями вследствие корыстных мотивов или из-за насильственного принуждения к сотрудничеству с преступниками посредством шантажа или угрозы насильственной расправы над ними или над их близкими.

От нарушителей можно ожидать использования любых тактических методов, повышающих вероятность достижения ими цели. К ним, например, можно отнести применение силы (насильственные действия), хищение (кражи) или дезинформацию (обман), т.е. любую тактику, дающую им определенные преимущества.

При рассмотрении возможных действий нарушителя следует учитывать, в каких видах преступной активности он заинтересован, и какие из этих видов преступной активности могут иметь отношение к данному объекту. Большую ценность может иметь понимание мотивов и причин действий противника.

Огромное значение для модели нарушителя имеет определение его потенциальных возможностей. Первостепенную роль во всех

случаях играет количество нарушителей, которым должна успешно противостоять система физической защиты. Большую ценность также имеет информация об оснащенности нарушителей (от инструмента и оборудования до оружия). К другим факторам, которые могут характеризовать возможности нарушителей, относятся описание транспортных средств (следует учитывать возможности передвижения нарушителей на грузовике и на вертолете, а также применения ими сверхлегких радиоуправляемых движущихся устройств), уровень технических навыков и опыта нарушителей, а также вероятность содействия нарушителям со стороны служащих объекта.

С учетом особенностей нарушителей, рассмотренных выше, можно сформулировать модель нарушителя. При этом различают «макромодели» и «микромодели» нарушителей.

Макромодель содержит следующие сведения:

· категория нарушителя;

· ожидаемая акция;

· цель акции;

· количественный состав (в случае группы нарушителей);

· осведомленность;

· подготовленность;

· техническая оснащенность;

· вооружение.

Микромодель содержит следующие сведения:

· способы преодоления физических барьеров и средств обнаружения (СО);

· скорость перемещения в зоне обнаружения СО;

· наличие подручных средств;

· наличие специальных технических средств, например, предназначенных для деблокирования СО.

Макромодели используются, в основном, при разработке концепции построения объекта в целом, тогда как микромодели позво-

ляют выработать требования к отдельным элементам СФЗ, например, к средствам обнаружения и физическим барьерам на периметре, локальных зонах, в зданиях, помещениях и т.п.

Модель нарушителя следует регулярно пересматривать. Поводом для этого могут послужить изменение обстановки вокруг объекта и изменения на самом объекте.

В заключение следует отметить, что на практике модель нарушителя для конкретного объекта формируется после анализа его уязвимости путем заполнения соответствующих анкет.

Все это дает представление о СФЗ, как о сложных человекомашинных системах, в которых присутствует конфликт интересов сторон (нарушитель - система защиты). Кроме того, следует отметить, что задача физической защиты решается в условиях неопределенности, так как имеется лишь общее представление о целях вероятного нарушителя, стратегии и тактике их реализации.

1.7. Определение структуры СФЗ

В соответствии с принципами многозональности и многорубежности построения системы физической защиты рубежи защиты создаются на границах контролируемых зон. В общем случае структура СФЗ объектов может быть представлена в виде следующих подсистем (рис. 1.7):

Подсистема обнаружения должна оповещать сотрудников службы безопасности и возможно других служб (например, органы вневедомственной охраны, пожарную охрану, милицию и т.д.) о проникновении нарушителя на охраняемую территорию объекта, о пожаре и других стихийных бедствиях, защита от которых предусмотрена задачами системы.

Подсистема телевизионного наблюдения обеспечивает визуальный дистанционный контроль за охраняемой территорией и действиями нарушителей. В нее также входят средства дежурного

освещения, обеспечивающие необходимый уровень освещенности охраняемой территории.

Подсистема управления доступом представляет собой совокупность технических и программных средств, инженерно-технических сооружений и организационных мер, обеспечивающих контролируемый доступ на объект и на отдельные его составляющие, а также запрещает такой доступ всем, кто не имеет соответствующих полномочий.

Подсистема сбора и обработки данных обеспечивает передачу сигналов тревоги, вырабатываемых датчиками обнаружения и элементами системы контроля доступа. В современных СФЗ данная подсистема представляет собой автоматизированную интегрированную систему управления, что повышает эффективность функционирования всей системы физической защиты.

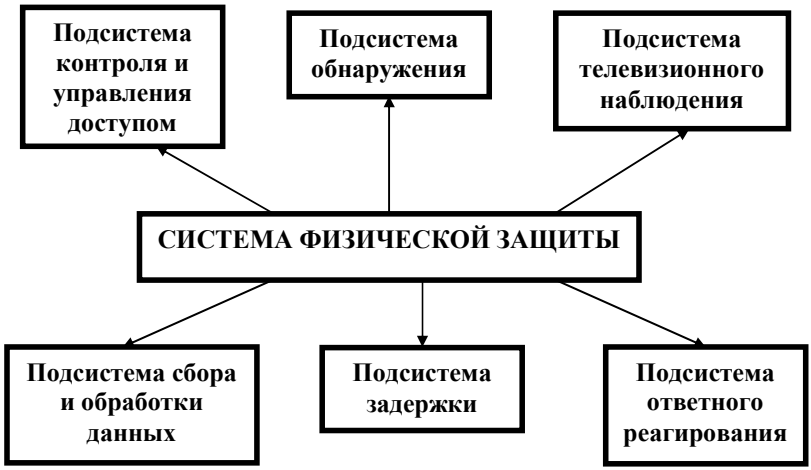


Рис. 1.7. Структура системы физической защиты

Подсистема задержки образуется совокупностью инженерных сооружений, представляющих собой естественные преграды и механические барьеры на пути нарушителя. К ним относятся неровности поверхности земли (рвы, овраги, скалы и т.д.) труднопроходимые элементы ландшафта (река, лес, кустарник) и искусственные преграды (заборы, решетки, стены, ворота и двери с замками, окна и т.д.).

Подсистема ответного реагирования предназначена для нейтрализации угроз безопасности объекта. Это обеспечивается силами ответного реагирования службы безопасности, системой связи, службой и средствами пожаротушения, наличием резервных систем жизнеобеспечения и сопровождается действием тревожной звуковой и световой сигнализациями.

Таким образом, основу СФЗ составляют механические средства и инженерные сооружения, препятствующие физическому движению нарушителей к месту нахождения объектов защиты, технические средства, информирующих сотрудников службы безопасности о проникновении нарушителя в контролируемую зону и позволяющие наблюдать обстановку в них, а также средства и люди, устраняющие угрозы.

Использование при создании СФЗ современных технических средств охраны и средств обработки и представления информации привело к тому, что СФЗ превратились в автоматизированные интегрированные системы безопасности, комплексно выполняющие функций обеспечения безопасности объекта.

1.8. Определение этапов проектирования СФЗ

Процесс создания СФЗ будем называть проектированием (в широком смысле слова), так как объектами проектирования являются не только технические системы, строительные конструкции, но и организационные структуры и алгоритмы их функционирования.

В процессе проектирования необходимо решать задачи анализа и синтеза СФЗ.

Под анализом понимается определение свойств системы (характеристик и т.п.) при заданных ее структуре и составе.

Под синтезом понимается определение структуры и состава при заданных требованиях, предъявляемых к системе (по характеристикам, функциям и т.п.). В процессе синтеза необходимо решать, как правило, многократно, задачу анализа.

Кроме умения достоверно с заданной точностью, определять характеристики СФЗ необходимо иметь критерии, в соответствии с которыми производится синтез системы. В общем случае задача синтеза решается с помощью методов многокритериальной (векторной) оптимизации. Наиболее распространенным является двумерный случай: синтез сложной системы по критерию «эффективность-стоимость». Как будет показано ниже, эффективность СФЗ можно характеризовать вероятностью защиты объекта при заданной модели потенциального нарушителя. В качестве стоимостного показателя могут выступать капитальные затраты на создание СФЗ и отдельных ее элементов, эксплуатационные затраты, в том числе трудозатраты сил реагирования и технического персонала.

Таким образом, проектирование эффективной системы физической защиты объекта требует методического подхода, позволяющего проектировщику сопоставлять цели СФЗ с имеющимися ресурсами и затем производить оценку предлагаемого объект. Разработка СФЗ без такой тщательной оценки может привести к неоправданному расходованию ценных ресурсов на средства защиты, в которых нет необходимости, или, что еще хуже, к неспособности системы обеспечить адекватную защиту тех участков объекта, которые имеют критическое значение. В данном случае целесообразен определенный порядок разработки системы физической защиты (рис. 1.8).

Рис. 1.8. Процесс разработки СФЗ

На первом этапе разработки СФЗ определяются цели системы защиты. Для этого необходимо (рис. 1.9) определить характеристики и особенности объекта, на котором будет создаваться СФЗ, составить перечень угроз безопасности объекта и определить модель нарушителя с выявлением его целей.

Располагая информацией о характеристиках объекта и установив существующие виды угроз и цели нарушителей, проектировщик может определить задачи и цели СФЗ. Например, целью СФЗ может являться «перехват хорошо оснащенного нарушителя перед тем, как они смогут получить определенные материальные ценности.

Следующим этапом разработки СФЗ является ее проектирование. На этом этапе определяется наилучшее сочетание таких элементов, как ограждения, датчики, процедуры, средства связи и обязанности службы безопасности, наиболее соответствующего целям физической защиты. Разработка проекта СФЗ должна производиться в соответствии с поставленными целями физической защиты, и в

то же время с учетом ограничений, накладываемых необходимостью ведения работ на конкретном объекте, а также соображениями безопасности и экономическими факторами.

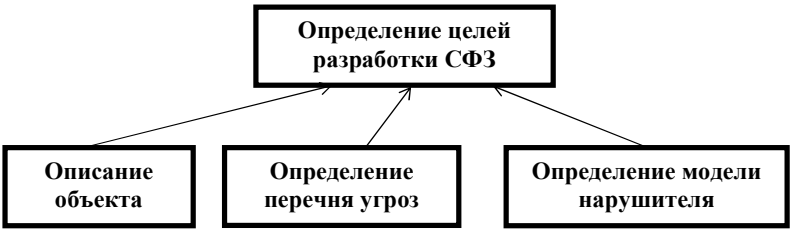


Рис. 1.9. Задачи, решаемые при определении целей разработки СФЗ

Основные функции СФЗ (обнаружение нарушителя, его задержка, ответные действия) реализуют различные подсистемы (рис. 1.10). Определение состав средств, которые входят в конкретные подсистемы также является необходимым этапом проектирования.

При разработке СФЗ необходимо учитывать некоторые требования, при выполнение которых СФЗ функционирует более эффективно. Например, датчики обнаружения проникновения нарушителей на территорию объекта целесообразно устанавливать как можно дальше от цели, к которым стремятся нарушители, а средства задержки – как можно ближе к цели. Кроме того, существует тесная связь между обнаружением нарушителя и оценкой ситуации. Проектировщик должен учитывать, что обнаружение проникновения без оценки ситуации не является «настоящим обнаружением». Тесная связь существует также между развертыванием сил ответного действия и системой связи, которой пользуется служба безопасности (рис. 1.10). Развертывание сил ответного действия не может быть достаточно эффективным, если не обеспечена надежная связь между подразделениями безопасности.

Рис. 1.10. Составляющие проектирования СФЗ

Учет этих и многих других характеристик компонентов СФЗ помогает проектировщику в полной мере использовать преимущества отдельных единиц оборудования и планировать такое сочетание элементов системы, при котором одни средства защиты дополняют другие и устраняют возможность возникновения «слабых мест» в системе защиты.

Анализ и оценка проекта СФЗ начинается с пересмотра и тщательного изучения целей, которым должна соответствовать проектируемая система. При этом производится проверка выполнения системой физической защиты требуемых функций. Следует иметь в виду, что, если даже СФЗ и выполняет все необходимые функции

защиты, вся система может и не отличаться высокой эффективностью, когда сочетание всех элементов системы не позволяет обеспечить надлежащий уровень защиты. В целях дальнейшей оценки минимального уровня эффективности СФЗ могут быть применены более сложные методы анализа и оценки.

Система физической защиты, уже установленная на действующем объекте, как правило, не может подвергнута исчерпывающим испытаниям. В данном случае методика оценки системы в целом основывается на испытаниях эффективности входящих в СФЗ отдельных подсистем. Оценка эффективности функционирования всей системы в целом производится с применением методов моделирования с использованием результатов оценки эффективности отдельных подсистем.

Конечным результатом этого этапа разработки СФЗ является оценка уязвимости системы. Анализ проекта СФЗ позволяет сделать вывод о том, что система или соответствует поставленным целям, или она имеет «слабые места». Если поставленные цели защиты объекта достигаются, то процесс проектирования и анализа системы завершается утверждением проекта (рис. 1.7). Если анализ показывает, что СФЗ неэффективна, то производится повторное проектирование и анализ эффективности (рис.1.7). Может понадобиться также и переоценка поставленных целей СФЗ. Цикл повторного проектирования и анализа повторяется до тех пор, пока результаты анализа не будут указывать на полное соответствие СФЗ целям и задачам защиты объекта.

Вопросы для самоконтроля

1. Какие факторы образуют методологическую основу построения СФЗ?
2. Какие характеристики и особенности объекта, необходимы для создания его СФЗ?
3. Каковы цели создания СФЗ?
4. Какие функции выполняет СФЗ?
5. Каков порядок реализации функции «обнаружение» в СФЗ?
6. Как реализуется функция «задержка» в СФЗ?
7. Как реализуется функция «ответные действия» в СФЗ?
8. Как классифицируются принципы построения СФЗ?
9. Объясните сущность принципа многозональности СФЗ.
10. Объясните сущность принципа многорубежности СФЗ.
11. Объясните сущность эшелонированной защиты объекта.
12. Что такое «равнопрочность» защиты?
13. Какие существуют источники угроз безопасности объекта?
14. Какие необходимы исходные данные для составления перечня угроз безопасности объекта?
15. Как классифицируются составляющие модели нарушителя?
16. Опишите структуру СФЗ (подсистемы).
17. Назовите этапы разработки СФЗ.
18. Назовите этапы проектирования СФЗ.

2. ПОДСИСТЕМА ОБНАРУЖЕНИЯ

Подсистема, или далее – система обнаружения, устанавливает факт несанкционированного действия, направленного на объект, и в рамках системы физической защиты выполняет функцию обнаружения проникновения на объект постороннего лица (нарушителя) или транспортного средства, пытающихся получить несанкционированный доступ на защищаемый участок объекта [2.1].

2.1. Основные принципы построения системы обнаружения

К основным принципам построения системы обнаружения относятся:

- непрерывность (равномерность) линии обнаружения;
- одинаковый уровень защиты (равнопрочность);
- комплексное применение технических средств обнаружения, использующих различные физические принципы;
- учет климатических условий (температура воздуха, высота снежного покрова, осадки);
- учет помеховой обстановки. Помехи разделяют на природные (растительность, животные, климат) и индустриальные (транспорт, летающий мусор, линии электропередач, промышленные установки);
- учет уровня подготовки обслуживающего персонала;
- учет особенностей функционирования объекта. Система обнаружения не должна мешать работе объекта и оказывать влияние на технические процессы на объекте.

Все перечисленные выше принципы являются следствием общих принципов построения СФЗ.

2.2. Тактико-технические характеристики системы обнаружения

Тактико-технические характеристики системы обнаружения определяются характеристиками технических средств обнаружения (СО), которые формируют подсистемы обнаружения. Технические СО – устройства, предназначенные для автоматической выдачи сигнала тревоги в случае несанкционированного действия. Сигналом тревоги обычно является замыкание или размыкание контактов реле (сухой контакт). Другими названиями СО являются: «датчик», «извещатель», «детектор».

Основными тактико-техническими характеристиками всех систем обнаружения являются:

- вероятность обнаружения, т.е. вероятность выдачи сигнала тревоги при пересечении человеком зоны обнаружения. Она определяет «тактическую надежность» рубежа охраны и должна составлять не менее 0,9–0,95 (для ядерно-опасных объектов – не менее 0,95);
- наработка на ложное срабатывание – среднее время между двумя выдачами ложного сигнала тревоги средством обнаружения;
- универсальность средства обнаружения – возможность работы в широком диапазоне условий эксплуатации в различных климатических условиях;
- уязвимость системы, т.е. возможность преодоления рубежа охраны без выдачи средством обнаружения сигнала тревоги;
- маскировка (визуальная и техническая) средств обнаружения. Маскировка позволяет увеличить надежность и эффективность системы обнаружения, поскольку нарушитель не знает о наличии охранной сигнализации, и это не искажает архитектурного облика охраняемого объекта;

- надежность, долговечность, простота монтажа и эксплуатации.

На вероятность обнаружения СО влияют следующие факторы:

- характеристики цели (например, размеры и скорость движения);
- грамотное размещение и установка СО;
- настройка чувствительности и зоны обнаружения СО;
- условия функционирования. Со временем могут меняться погода, помехи и другие факторы, влияющие на чувствительность СО.

Ложные срабатывания СО вызываются:

- помехами;
- несовершенством и неисправностями аппаратуры;
- неверным или неправильным монтажом.

Для каждого СО можно изобразить рабочую характеристику – зависимость вероятности обнаружения ($P_{\text{обн}}$) от наработки на ложное срабатывание ($T_{\text{л.с.}}$) (рис. 2.1). Перемещение по данной кривой вызывается регулировкой чувствительности.

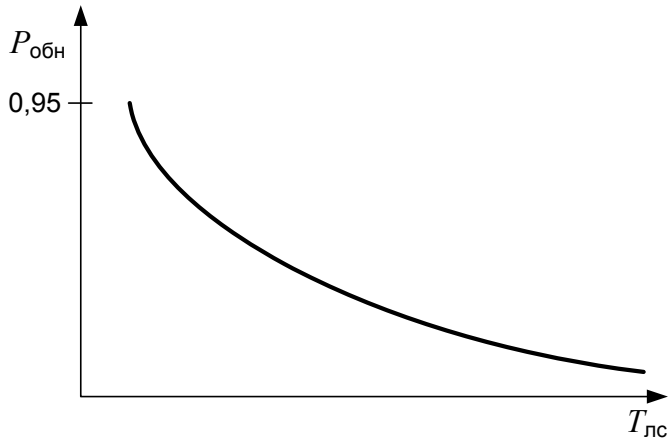


Рис. 2.1. Рабочая характеристика СО

2.3. Классификация средств обнаружения

Средства обнаружения можно разделить на периметровые и объектовые [П.1, П.2, 2.1 – 2.3]. Периметровые СО используются на открытой местности для блокировки участков периметра объекта, а объектовые средства обнаружения устанавливаются внутри зданий и помещений.

Специфика отечественных условий проектирования и эксплуатации периметровых систем физической защиты заключается прежде всего в широком разнообразии климатических и почвенно-геологических условий. Большие сезонные колебания температуры, сильные снегопады, метели, мокрый снег, частые плотные туманы, ураганные ветры, сильные дожди, гололед, иней вызывают большие трудности при выборе соответствующих средств обнаружения и делают практически невозможным использование какой-либо единой системы для любой климатической зоны России.

Другим типом классификации является разделение СО по используемым ими физическим принципам функционирования:

- емкостные;
- радиотехнические;
- вибрационные;
- акустические;
- оптические;
- контактные;
- комбинированные;
- другие.

Подробнее эти типы извещателей будут рассмотрены ниже.

Среди других классификаций выделяют следующие:

- активные и пассивные СО;
- потайные и видимые СО;

- волюмометрические (измеряющие характеристики ограниченного объема) и линейные;
- устанавливаемые на открытом пространстве и в соответствии с рельефом местности.

2.4. Уязвимость средств обнаружения и способы ее снижения

Существуют следующие способы нейтрализации СО:

- обход зоны обнаружения (например, по «мертвой зоне» СО);
- обман СО – преодоление зоны обнаружения без вызова сигнала тревоги. Обман может достигаться путем изменения зоны обнаружения, изменения положения или экранирования СО.

Все существующие СО можно нейтрализовать тем или иным способом.

Основными способами снижения уязвимости СО являются следующие:

- защита от НСД (например, с помощью другого СО);
- контроль вскрытия корпуса СО;
- контроль работоспособности СО:
  - прямой (ежедневные реальные испытания);
  - дистанционный (нужна отдельная линия сигнализации для каждого СО);
  - автоматический (самодиагностика устройства через определенные интервалы времени);
- отключение сигнальных ламп СО. Сигнальные лампы на СО помогают при его установке, регулировке и проверке функционирования, однако они же могут помочь злоумышленнику установить зону обнаружения СО.

2.5. Емкостные средства обнаружения

Принцип действия емкостного СО основан на измерении емкости антенного устройства относительно земли. При этом блок обработки сигнала (БОС) производит измерение только емкостной составляющей импеданса антенны и не реагирует на изменение сопротивления (квадратурная обработка сигнала с помощью синхронного детектора). Емкость антенной системы изменяется при приближении и прикосновении к ней нарушителя.

Емкостные СО могут использоваться как для охраны периметра, так и в помещениях.

Периметровые емкостные средства обнаружения

Одним из примеров использования емкостных средств обнаружения для охраны периметра является конструкция антенного устройства, представляющая собой металлический козырек, изготавливаемый в виде сварной или даже кованой решетки. На рис. 2.2 представлен вариант монтажа такого козырька по верху железобетонного ограждения. Она допускает изгибы в вертикальной и горизонтальной плоскостях, позволяет отслеживать рельеф местности и другие топографические особенности объекта. При соответствующем дизайне козырек не ухудшает внешний архитектурный облик здания.

К преимуществам емкостных СО относится то, что они не имеют мертвых зон и обладают стабильной высокой чувствительностью, при этом зона обнаружения регулируется и может быть очень узкой.

При использовании емкостных СО большая часть стоимости приходится на изготовление и монтаж металлоконструкций антенной части.

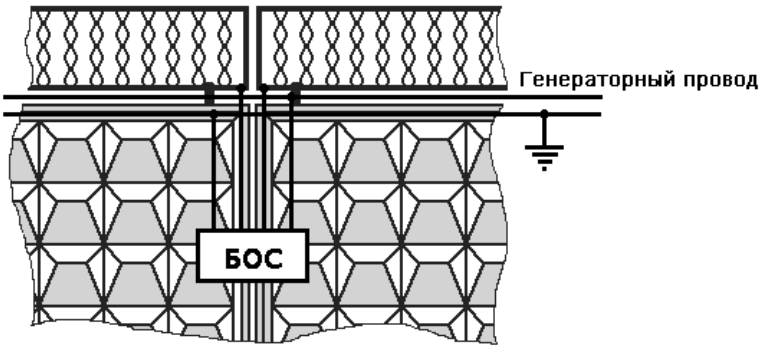


Рис. 2.2. Вариант применения емкостного СО

Поскольку антенная система должна быть изолирована от земли, для крепления металлоконструкций используют специальные изоляторы (рис. 2.3).

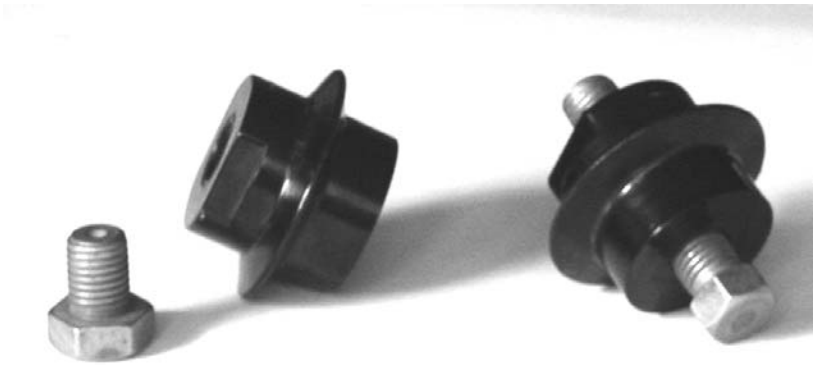


Рис. 2.3. Стандартные изоляторы для емкостных СО и крепеж

К настоящему времени разработано целое семейство емкостных сигнализаторов серии «Радиан» («Радиан-М», «Радиан-13», «Радиан-14», «Радиан-15»).

«Радиан-14». Емкостное периметровое средство обнаружения «Радиан-14» производства ФГУП «СНПО «Элерон»» – одна из последних модификаций семейства емкостных сигнализаторов для охраны периметра. Оно разработано на основе изучения опыта длительной эксплуатации аналогичных приборов «Радиан-М» и «Радиан-13» и воплотило в себе достижения схемотехники, современных алгоритмов обработки сигналов и новой элементной базы.

Принципиальное отличие прибора «Радиан-14», позволившее значительно повысить его помехоустойчивость, заключается в применении двухканальной схемы обработки сигнала и алгоритма «компенсации». Суть ее в том, что помеховый сигнал в резистивном канале вычитается из сигнала в емкостном канале и препятствует ложному срабатыванию. Схема настроена таким образом, что пороговое устройство реагирует только на одну полярность, соответствующую сигналу в емкостном канале. Поэтому помеховый сигнал в резистивном канале, какой бы большой величины он ни был, может только компенсировать емкостную составляющую, но не вызовет срабатывания порогового устройства.

Частая причина ложных срабатываний – воздействие импульсных электрических помех, особенно радиопомех, характерных для городских условий. В приборе «Радиан-14» импульсные радиопомехи возникают строго одновременно в обоих каналах и тем самым компенсируются (вычитаются), что препятствует ложному срабатыванию.

Таким образом, «Радиан-14» обладает следующими преимуществами:

- высокая помехоустойчивость к дождю, мокрому снегу, загрязненным изоляторам и т.п.;
- высокая защищенность от индустриальных электро- и радиопомех.

Это позволило добиться почти на порядок большего времени наработки на ложное срабатывание – 2000 ч (вместо 250 ч в приборе «Радиан-М»).

Кроме того, введение компенсирующего канала позволило отказаться от обязательного использования специальных изоляторов-переходников. Для монтажа прибора «Радиан-14» можно применять обычные изоляторы, используемые в электрических установках. Это резко удешевляет всю систему, дает большие возможности для конструкторских и дизайнерских решений по улучшению внешнего вида и маскировки антенной системы. Разработан вариант антенной козырьковой системы, включающий в себя элементы установки (пластмассовые кронштейны, стальной провод и крепеж) и поставляемый вместе с электронным блоком (СО «Ярус»).

«Радиан-14» выполнен в том же корпусе, что и «Радиан-13», имеет те же конструктивные и стыковочные параметры. Это позволяет легко провести замену старого прибора на новый, причем не требуется реконструкция антенной системы, питающих и сигнальных линий.

Существует также СО «Радиан-15», разработанное специально для функционирования в условиях высоких электромагнитных помех (например, вблизи ЛЭП).

Использование емкостных средств обнаружения в помещениях

Емкостные датчики приближения — датчики активного типа. Датчики такого типа требуют установления резонансной электрической связи между защищаемым металлическим объектом и контрольным компонентом датчика. Электрическая емкость, образуемая заземленным защищаемым металлическим объектом, становится частью откалиброванной емкости схемы, установленной в генераторе частоты электрического тока. Частота электрического

тока, вырабатываемого откалиброванной схемой, может быть постоянной или изменяющейся.

Генераторы с постоянной частотой вырабатываемого тока оснащены устройством, позволяющим регулировать емкость в целях компенсации различных емкостных нагрузок. Проволочный проводящий контур, называемый защитным контуром, подсоединяется к проводящему защищаемому объекту или к нескольким таким объектам и к контрольному устройству, в котором установлена откалиброванная электронная схема. После того, как контур подсоединен ко всем защищаемым объектам, производится регулировка электронной схемы с использованием калибровочного измерительного прибора, позволяющего найти емкостный резонанс. Если впоследствии произойдет любое изменение емкости в электрической цепи, соединяющей защитный контур (который включает подсоединенные к нему защищаемые объекты и заземление), емкостный резонанс будет нарушен, и контрольное устройство подаст сигнал тревоги.

На рис. 2.4 представлен вариант использования емкостного СО для защиты двух металлических предметов (сейфа и шкафа). Неметаллические предметы могут защищаться с использованием металлической сетки.

Другой вариант использования емкостного СО в помещении – использование под ковром помещения специального «бутерброда» из двух тонких проводящих сеток, между которыми располагается мягкая резина. При нажатии на такой «бутерброд» (или даже приближении к нему) его емкость изменяется.

Если использовать шторы из металлизированной ткани, то можно защитить помещение от проникновения через окно. При этом окна должны быть плотно закрыты, так как любой сквозняк будет вызывать ложные срабатывания.

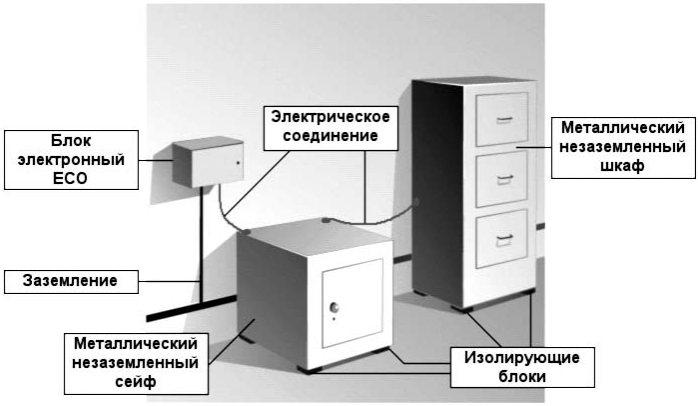


Рис. 2.4. Пример использования емкостного СО в помещении

Емкостные датчики также применяются для регистрации проникновения в помещение через существующие отверстия и проходы, такие как решетки вентиляционных и других трубопроводов и металлические рамы окон и дверей.

2.6. Радиотехнические средства обнаружения

Радиотехнические средства обнаружения – это активные СО, в том или ином виде использующие электромагнитное излучение в радиодиапазоне. Среди них выделяют следующие подтипы:

- радиолучевые СО;
- микроволновые СО;
- проводно-волновые СО;
- СО на основе «линии вытекающей волны» (ЛВВ).

Эти типы средства обнаружения будут описаны ниже.

Радиолучевые средства обнаружения

Принцип работы радиолучевого СО основан на создании между передатчиком и приемником протяженного электромагнитного поля и регистрации изменения суммарной амплитуды принимаемого сигнала при пересечении злоумышленником зоны обнаружения (ЗО).

Используется излучение с частотой от 14 до 37 ГГц. Зона обнаружения представляет собой вытянутый эллипсоид. Длина ЗО может составлять до 500 м (например, СО «Барьер-500» производства ЗАО «Охранные системы», внешний вид которого показан на рис. 2.5). Использование более мощных источников для создания более протяженной ЗО не эффективно с той точки зрения, что невозможно будет точно установить место нарушения. Диаметр ЗО в ее середине может составлять от 80 до 600 см в зависимости от размеров антенны и частоты излучения. Объемная зона обнаружения является достоинством датчика, ее труднее преодолеть без сигнала тревоги.

На работоспособность радиолучевых средств обнаружения практически не влияют дождь, туман, ветер. Однако они требуют при эксплуатации наличия геометрически свободного пространства между излучателем и приемником и перестают работать при образовании сугробов, «затеняющих» луч. Необходимо убирать снег, либо использовать телескопические стойки для поднятия передатчика и приемника на периметре объекта. Источником ложных срабатываний являются животные, летающий мусор, вибрация стоек с СО, метель.

При использовании радиолучевых СО необходимо учитывать наличие «мертвых зон» около передатчика и приемника. Длина «мертвых зон» зависит от характеристик антенны. Среднее значение таких зон составляет примерно 14 м для СО с длиной ЗО 200 м и 17 м для СО с длиной ЗО 300 м. Кроме этого, при установке при-

емников и передатчиков непосредственно на металлической поверхности сплошных оград (полотна забора), внешних стен ангаров, «мертвые зоны» образуются в середине ЗО. В самых современных СО длины «мертвых зон» значительно уменьшены.

Рис. 2.5. Радиолучевое СО «Барьер-500»

С учетом вышесказанного радиолучевые СО необходимо устанавливать с перекрытием 7 – 15 м. Если необходимо защитить угол территории, можно использовать металлический экран, «преломляющий» ЗО (рис. 2.6).

Можно использовать радиолучевые СО совместно со спиралью «Егоза» (см. главу 6). При этом зона обнаружения не будет выходить за пределы спирали. Средства обнаружения будут реагировать на любые изменения формы спирали.

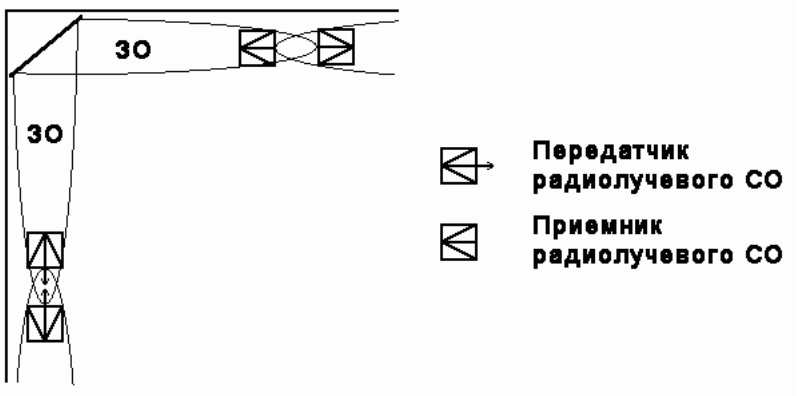


Рис. 2.6. Использование металлического экрана для «преломления» ЗО и перекрытие «мертвых зон» радиолучевого СО

«Радий-2/1» фирмы «Юмирс» – пример радиолучевого СО. Длина ЗО данного средства может составлять от 10 до 200 м, высота в центре – 1,8 м. Извещатель выдает сигнал тревоги при пересечении ЗО нарушителем со скоростью от 0,1 до 10 м/с в полный рост или пригнувшись. При этом данное средство обнаружения сохраняет свою работоспособность при дожде и снеге, травяном покрове высотой до 30 см и высоте снежного покрова до 50 см без дополнительных регулировок.

Микроволновые средства обнаружения

Микроволновые средства обнаружения используют излучение с частотой около 10 ГГц. В основном они используются для охраны помещений и иногда для коротких участков периметра. Микроволновые СО могут быть как однопозиционными, так и двухпозиционными.

Принцип действия двухпозиционных микроволновых СО не отличается от принципа действия радиолучевых СО. Единственное

отличие состоит в том, что зона обнаружения микроволновых СО обычно значительно шире.

Принцип действия однопозиционных микроволновых СО состоит в создании в ЗО объемного электромагнитного поля и регистрации сдвига частоты между передаваемым и принимаемым сигналами, возникающего при движении нарушителя вследствие эффекта Доплера.

Зона обнаружения однопозиционных микроволновых СО имеет удлиненную каплеобразную форму, параметры которой определяются конструкцией антенны. Антенна, как правило, представляет собой микроволновый рупорный облучатель, хотя в некоторых случаях используются также планарные (плоские) антенны (печатные платы) или фазированные антенные решетки.

Однопозиционные микроволновые извещатели могут быть выбраны с учетом дальности обнаружения. Такой выбор связан с электронной калибровкой извещателя, позволяющей принимать только те отраженные сигналы, которые поступают в течение определенного заданного периода времени. Отраженные сигналы, поступающие до или после заданного периода времени, игнорируются. Время поступления отраженного сигнала определяется расстоянием от датчика до диверсанта, проникнувшего в помещение (или до другой цели). Отбор извещателей по дальности, как правило, применяется для того, чтобы предотвращать их срабатывание при перемещении объектов за пределами максимального желаемого радиуса действия.

Отбор извещателей по дальности необходим, когда СО используется там, где микроволновое излучение может проникнуть через стены защищаемого помещения. Микроволновое излучение легко проникает через оконное стекло, штукатурку, гипс, фанеру и другие материалы, обычно используемые при возведении стен и перегородок. Металлические объекты, такие, как большие книжные стеллажи, столы, перегородки и экраны, установленные в защи-

щаемой зоне, вызывают затенение сигнала, т.е. создают участки, перемещение в которых не поддается обнаружению с помощью микроволнового извещателя.

Тот факт, что микроволновое излучение может проникать через стены, дает определенные преимущества, но может оказаться и отрицательным фактором. Преимущество состоит в том, что микроволновый датчик может регистрировать перемещение диверсанта в помещении, разделенном перегородками на небольшие отделения. Вместе с тем, возможность регистрации тем же датчиком перемещения объектов за пределами защищаемой зоны и даже за пределами здания приведет к подаче ложного сигнала тревоги и, следовательно, является отрицательным фактором. Так как ограничение распространения микроволнового излучения за пределы определенного объема связано с техническими трудностями, следует с особой тщательностью планировать расположение и направление микроволновых антенн в помещениях, требующих защиты.

Однопозиционные микроволновые устройства могут быть также использованы в качестве датчиков, регистрирующих проникновение в какой-либо определенной точке или на небольшом участке в тех случаях, когда датчики другого типа не могут обеспечить достаточной защиты или могут быть выведены из строя нарушителями. Однопозиционные микроволновые СО часто используются коммерческими организациями в качестве устройств для автоматически открывающихся дверей в больших универсальных магазинах и аэропортах.

Микроволновые датчики следует устанавливать высоко, под потолком защищаемого помещения. Антенна датчика должна быть направлена в сторону зоны обнаружения, но не в сторону металлических предметов, которые могут отражать микроволновые сигналы и вызывать подачу ложных сигналов тревоги. Источниками ложных срабатываний также являются люминесцентное освеще-

ние, вибрация СО или предметов в ЗО, перемещающиеся животные.

Извещатель «Волна-5» фирмы «Аргус-Спектр» используется для обнаружения проникновения в охраняемое помещение и имеет ЗО каплевидной формы длиной до 15 м и шириной до 5 м, но при необходимости может быть уменьшена до 2…5 м в длину. Данные СО могут иметь 4 различные частоты излучения, что позволяет использовать в одном помещении несколько извещателей.

Проводно-волновые средства обнаружения

Принцип действия проводно-волновых средств обнаружения – создание вокруг протяженной системы проводников объемного электромагнитного поля и регистрация его изменения при появлении в ЗО нарушителя.

Проводно-волновые СО могут быть использованы для создания как «козырьковой», так и «приземной» ЗО. Данные СО могут применяться для любых, даже самых сложных, форм периметра. Они надежно отслеживают все повороты, подъемы, спуски на периметре. С их помощью также можно блокировать стены и крыши зданий, являющихся частью периметра объекта. Достоинством проводно-волновых СО является также то, что в антенных системах могут использоваться недорогие провода широкого применения.

Антенная система состоит из двух изолированных проводов. К одному из них подключается УКВ-генератор, к другому – приемник.

Источником ложных срабатываний для проводно-волновых СО служат животные и колебания проводников.

«Уран-М1» производства НИКИРЭТ – пример проводно-волнового средства «козырькового» типа. В комплект поставки входят блок генератора, блок приемника, кронштейны для крепле-

ния проводов, сами провода и комплекты муфт. Муфты поставляются как неразъемные (для сращивания порвавшихся проводов), так и разъемные – для использования, например, над редко открывающимися воротами.

Максимальная длина ЗО для средства обнаружения «Уран-М1» составляет 200 м. Проводники крепятся на расстоянии 40 см друг от друга и образуют протяженную зону обнаружения, имеющую в сечении форму эллипса длиной 70 см и шириной 40 см. Необходимо, чтобы в пределах ЗО не было металлических предметов.

Извещатель «Газон» – пример средства обнаружения «приземного» типа. Оно используется для блокирования временных рубежей охраны и локальных участков периметра на неподготовленной местности со сложным рельефом и конфигурацией. Проводник, подключенный к блоку приемника, развертывается на высоте 1,5 – 1,8 м от земли с использованием диэлектрических стоек, располагаемых вдоль периметра через каждые 7 – 9 м. Второй провод прокладывается по поверхности земли под верхним проводом (рис. 2.7).

Существуют также многофункциональные СО, например, ***«Импульс-12»***, которые на одном охраняемом участке могут использоваться и как «приземные», и как средства «козырькового» типа.

Средства обнаружения на основе «линии вытекающей волны»

Принцип действия средств обнаружения на основе «линии вытекающей волны» (ЛВВ) тот же, что и у проводно-волновых СО: создание между излучающим и приемным кабелями электромагнитного поля и регистрация его изменения при появлении в ЗО нарушителя. Разница состоит в типах используемых кабелей и месте их прокладки.

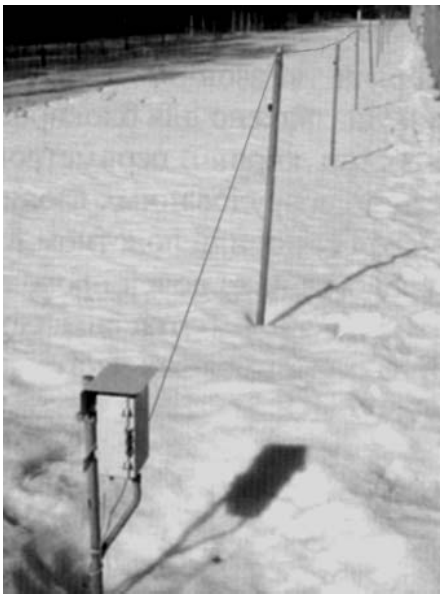


Рис. 2.7. Проводно-волновое СО «Газон»

В качестве чувствительного элемента используется коаксиальный кабель, металлическая оплетка которого по всей длине имеет перфорацию (отверстия) или специально прорежена (так называемый «сочащийся кабель») (рис. 2.8).

Система состоит из двух параллельных кабелей, размещаемых в грунте на глубине 0,1–0,3 м вдоль охраняемого периметра при расстоянии между кабелями 2–3 м. К одному из них подключается генератор УКВ-диапазона, к другому — приемник. За счет отверстий часть энергии из генераторного кабеля поступает на приемный, формируя зону обнаружения шириной 3–5 м и высотой 0,7–1 м. Система такого типа полностью маскируется и может быть обнаружена только с помощью специальной аппаратуры.

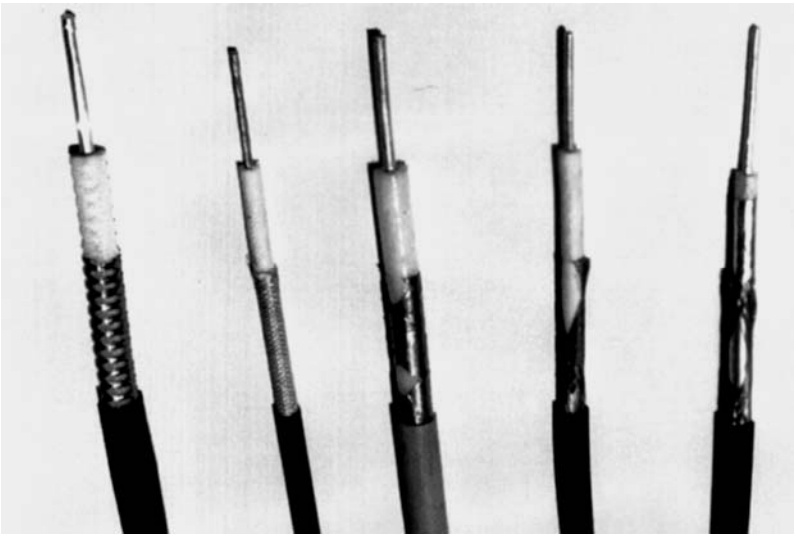


Рис. 2.8. Различные типы перфорированного коаксиального кабеля

Средства обнаружения на основе ЛВВ могут использоваться на периметрах, не имеющих заграждений, и защищать периметр с заграждениями от подкопа. Эти средства подходят для блокирования участков периметра сложной формы.

Недостатком данного типа СО является то, что при резко отличающихся по своему составу грунтах в пределах зоны прокладки кабелей одного изделия, при сильных дождях может сильно измениться чувствительность по длине участка. Кроме того, ввиду малой глубины закладки кабелей, в зоне их размещения запрещается производить какие-либо земляные работы (посадку растений, проводку подземных коммуникаций, устройство фундаментов и т.п.).

Извещатель «Бином-М» производства ФГУП «СНПО «Элерон»» – пример СО на основе ЛВВ. Оно позволяет организовать зону обнаружения шириной 6 м, высотой над грунтом 0,7 м и длиной двух участков по 60–125 м.

2.7. Вибрационные средства обнаружения

Вибрационные средства обнаружения можно разделить на два подтипа:

- СО с кабельным чувствительным элементом (ЧЭ);
- вибросесмические СО.

Средства обнаружения с кабельным ЧЭ, в свою очередь, также делятся на несколько подтипов:

- трибоэлектрические СО;
- СО на основе протяженного микрофона;
- вибромагнитометрические СО;
- волоконно-оптические СО;
- манометрические СО.

Трибоэлектрические средства обнаружения

Принцип действия трибоэлектрических СО состоит в контроле появления в протяженном чувствительном элементе электрических зарядов, возникающих при воздействии на заграждение или ЧЭ. Данный тип СО используется для охраны заграждений и их козырьков. Также он может использоваться для охраны коробов (кабель-каналов).

В качестве ЧЭ может использоваться обычный телефонный кабель, содержащий 10 пар проводов, или специальный кабель. Такое средство обнаружения может использоваться для заграждений из сварной сетки (сетка-рабица обычно не используется, так как провисает и плохо натягивается), деревянных, бетонных заграждений, металлических решеток. На сетке ЧЭ обычно закрепляется с помощью пластмассовых хомутов или мягкой проволоки; на бетонном или деревянном заборе ЧЭ закрепляется с помощью пластмассовых или металлических «лапок».

Блок обработки сигнала (БОС) обычно реагирует на возникновение зарядов с двумя частотами:

- низкой (2–6 Гц), что соответствует преодолению (перелазу) заграждения или загибу сетки;
- высокой (70–1200 Гц), что соответствует разрушению полотна заграждения.

Ложные тревоги могут вызываться растениями, раскачиваемыми ветром, или животными. Для того чтобы мелкие животные не пытались пролезть через решетку или сетку, вызывая сигналы тревоги, обычно через каждые несколько десятков метров делают для них небольшие дырки (лазы).

Вибрационное кабельное средство обнаружения ***«Дельфин-М»*** производства ГУП «Дедал» состоит из протяженного чувствительного элемента в виде специального трибоэлектрического кабеля и электронного блока усиления и обработки сигнала. Кабель крепится к пассивному ограждению из металлической сетки и преобразует ее вибрацию, создаваемую нарушителем, в электрический сигнал, который после обработки в электронном блоке формирует сигнал тревоги. Внешний вид данного СО и способ его размещения показаны на рис. 2.9.

«Дельфин-М» способен надежно функционировать в условиях воздействия сильного ветра, снега, гололеда, дождя и т.д. и индустриальных помех (близкого проезда транспорта, ЛЭП, работы радиостанции). Он выдает сигнал тревоги при попытках человека перелезть через ограждения, повредить сетку, перекусить проволоку, перерезать кабель и т.д. Длина ЗО может составлять до 250 м.

Средство обнаружения «Дельфин-М» широко используется для охраны АЭС и других ЯО.

Рис. 2.9. Пример использования СО «Дельфин-М»

Средства обнаружения на основе протяженного микрофона

В качестве чувствительного элемента для таких систем выступает специальный кабель, внутри которого имеется пара протяженных магнитов, в зазорах между которыми расположены подвижные проводники (рис. 2.10). При вибрациях кабеля подвижные проводники в кабеле перемещаются в магнитном поле полимерных магнитов; в них наводится электрическое напряжение, регистрируемое анализатором. Микрофонный кабель уникален также тем, что в нем генерируются высококачественные звуковые сигналы, которые дополнительно позволяют распознать вторжение на слух, что снижает вероятность ложной тревоги.

Средства обнаружения «Гардвайр» и «Дефенсор» английской фирмы Geoquip получили наибольшее распространение. В данных СО производится двухканальная обработка сигналов в ЧЭ, необходимая для регистрации двух характерных типов вторжений – перелезание

через ограду (продолжительное воздействие) и разрушение ограды (импульсное ударное воздействие или перекусывание). Чувствительность системы устанавливается независимо в каждом канале. Максимальная протяженность зон охраны для этих систем составляет 400 м.

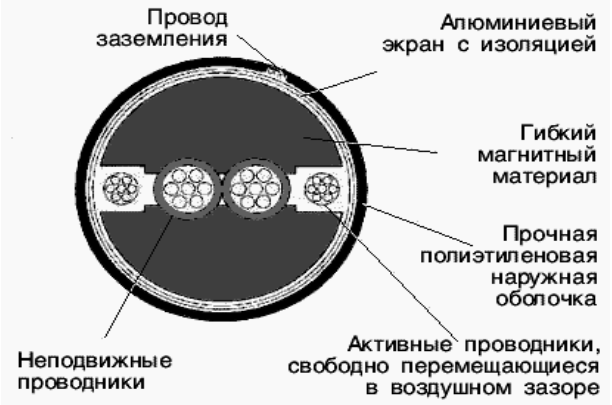


Рис. 2.10. Структура микрофонного кабеля GW400K

Вибромагнитометрические средства обнаружения

В качестве чувствительного элемента вибромагнитометрических СО используется система изолированных проводов, закрепляемых на пассивном ограждении на всем протяжении участка периметра. При преодолении ограждения нарушитель вызывает его вибрацию (избыточные шумы), которые, в свою очередь, приводят к колебанию проводов ЧЭ в постоянном магнитном поле Земли и генерацию электрических сигналов. Они поступают на схему обработки электронного блока прибора и при выполнении определенных заданных критериев обнаружения вызывают срабатывание выходного реле тревоги.

Средство обнаружения «Дрозд» ГУП «Дедал» может устанавливаться на следующих типах ограждений (заборов): бетонных, кирпичных, деревянных, металлических сетчатых, а также ограде из штампованных, сварных или кованых металлических элементов. Кроме того, можно сделать заграждение целиком из ЧЭ СО «Дрозд». Пример использования СО «Дрозд» представлен на рис. 2.11.

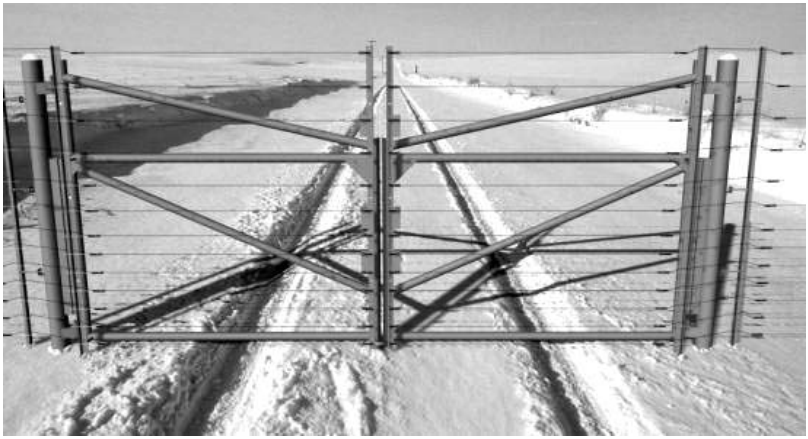


Рис. 2.11. Пример использования магнитометрического средства обнаружения «Дрозд» на воротах ограждения периметра

Средство обнаружения «Дрозд» имеет следующие преимущества.

- Не требуется обязательного использования металлического сетчатого ограждения, что снижает его стоимость. Кроме того, использование дешевого провода П274 («полевка») вместо специального трибоэлектрического кабеля также удешевляет систему.
- Его можно использовать практически на всех типах заборов, а также для защиты эстакад, стен и крыш зданий.

- Высокая помехоустойчивость: на работу прибора практически не оказывают влияние дождь, снег, туман, высокая трава или ветви деревьев в непосредственной близости от чувствительного элемента (допускается переплетение проводов ЧЭ вьюном, плющом и т.п.).
- СО устойчиво к электромагнитным помехам промышленного происхождения.

Волоконно-оптические средства обнаружения

В волоконно-оптических средствах обнаружения в качестве чувствительного элемента используется обычный волоконно-оптический кабель. При его вибрации или деформации изменяются фазовые характеристики лазерного излучения, распространяющегося в световедущей жиле.

Средство обнаружения «Ворон» производства ЗАО «НПО Прикладная радиофизика - ОС» — одна из немногих систем данного типа. В базовой комплектации данное СО позволяет контролировать рубеж длиной до 30 км (56 зон, каждая от 0 до 550 м). При этом на всем протяжении периметра полностью отсутствуют электрические элементы и кабели электропитания.

Изменения фазовых характеристик излучения в ЧЭ с помощью пассивных фазово-амплитудных преобразователей, устанавливаемых на границах зон обнаружения, трансформируются в амплитудную модуляцию излучения в волоконно-оптическом кабеле связи, поступают на пульт охраны, демодулируются в фотоприемном устройстве, затем анализируются в нейрокомпьютерном блоке обработки и при соответствующей идентификации воспринимаются как сигнал тревоги, отображаемый на плане объекта на экране монитора (рис. 2.12).

В системах «Ворон» анализ сигналов производится при использовании процессора с элементами искусственного интеллекта

на основе нейронных сетей «Ворон-Нейро - 1», обучаемого на объекте после полного монтажа системы «Ворон».

Рис. 2.12. Аппаратная стойка СО «Ворон»

Процесс обучения состоит в накоплении в памяти обучающей ЭВМ сигналов, соответствующих реальным попыткам обучающего персонала пересечь охраняемое ограждение, и сигналов различной природы, вызывающих ложные срабатывания системы. После этого обучающая программа автоматически вырабатывает алгоритм распознавания сигналов на данном конкретном типе и варианте ограждения и создает соответствующую распознающую структуру в нейрокомпьютере «Ворон-Нейро - 1» для многопараметрического анализа всех приходящих с ограждения сигналов.

Применение нейропроцессорных методов обработки и анализа сигналов позволяет адаптировать системы «Ворон» практически к любым типам подвижных ограждений при вероятностях обнаружения нарушителя не менее 0,98.

Манометрические средства обнаружения

В качестве чувствительного элемента манометрического СО выступает протяженный шланг, заполненный незамерзающей жидкостью и подключенный к мембранному датчику давления. При появлении человека непосредственно над шлангом за счет изменения давления возникает сигнал тревоги.

Средство обнаружения «GPS» итальянской фирмы «GPS Standard» имеет две модификации, отличающихся числом подключаемых труб. Ширина ЗО обнаружения данного СО составляет около 3 м для двухтрубного варианта и 6…7 м для четырехтрубного варианта при длине до 200 м (два участка по 100 м).

Данное СО не теряет чувствительности и зимой, в мерзлом грунте. При проведении испытаний оно четко фиксировало переползание, перекатывание и прохождение по доске человека при высоте снежного покрова около 1 м. Даже весной, когда образовался слой наста, способный удержать вес человека, обнаружение оставалось на достаточном уровне [2.2].

Вибросейсмические средства обнаружения

Принцип действия вибросейсмических СО – регистрация колебаний грунта или вибрации заграждений с помощью специальных датчиков при попытках нарушителя преодолеть контролируемую зону. Чувствительными элементами извещателей являются пьезо- или индуктивные преобразователи.

Данные СО могут использоваться как на улице, установленные на заграждение, так и в помещении, на стенах, дверях, окнах. Зона обнаружения таких извещателей сильно зависит от поверхности, на которой они установлены.

Вибросейсмические извещатели любого типа рассчитаны на регистрацию вибраций определенной частоты, характерных для взлома дверей и окон или пробивания стен (как правило, частота характерной вибрации составляет более 4 кГц), но не срабатывают под воздействием обычных для зданий и помещений вибраций, вызываемых работой систем кондиционирования воздуха или отопительного оборудования.

Вибросейсмические извещатели, устанавливаемые на стеклах, специально рассчитаны подавать сигнал тревоги при возникновении вибрации, частота которой соответствует характеристикам процесса разрушения стекла. Эта частота превышает 20 кГц.

Основное преимущество вибросейсмических извещателей состоит в том, что они обеспечивают заблаговременную подачу предупреждающего сигнала при попытке насильственного проникновения. Планируя применение вибрационных извещателей, проектировщик должен учитывать, что извещатели такого типа, установленные на стенах или конструкционных элементах, подверженных внешним вибрациям, могут генерировать ложные сигналы тревоги. Если конструкционный элемент подвергается сильным вибрациям, вызываемым такими внешними источниками, как вращающиеся механизмы, на поверхности этого элемента не следует устанавливать вибрационные извещатели. Тем не менее, если конструкционный элемент подвергается сильным вибрациям лишь время от времени, может оказаться эффективным использование вибрационных извещателей, оборудованных устройствами или схемами для аккумуляции или подсчета импульсов.

Извещатель «Грань-2» (рис. 2.13) предназначен для обнаружения преднамеренного разрушения монолитных бетонных стен и

перекрытий толщиной не менее 12 см, кирпичных стен толщиной не менее 15 см, деревянных конструкций из досок толщиной от 20 до 40 см, фанеры толщиной не менее 4 мм и типовых металлических сейфов.

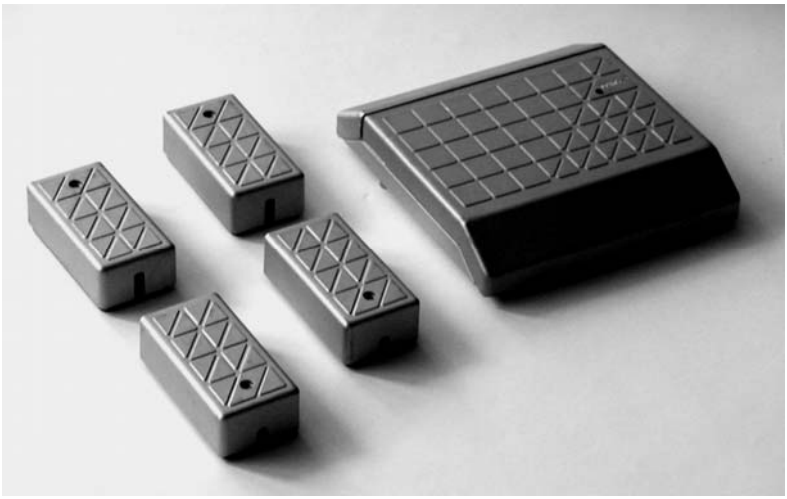


Рис. 2.13. Вибросейсмическое СО «Грань-2»: БОС и датчики

Комплект поставки СО «Грань-2» состоит из блока приема и обработки сигналов (БОС) и нескольких датчиков сигналов вибрации (ДСВ) двух типов, в сумме не более 10. ДВС первого типа (ДСВ1) предназначен для установки на монолитные конструкции. Он имеет ЗО радиусом не менее 2,2 м для монолитной бетонной или кирпичной конструкции и не менее 1,5 м для цельной деревянной конструкции. Он же служит для защиты металлических сейфов с площадью внешней поверхности не менее 8 м^2.

Датчик второго типа (ДСВ2) служит для защиты немонолитных конструкций. К нему подключается специальный звуковод

длиной до 5 м. ЗО одного ДСВ2 составляет 1,5 м в каждую сторону от звуковода.

Все датчики ДСВ1 и ДСВ2 объединяются в одну цепь и подключаются к БОС.

2.8. Акустические средства обнаружения

Среди акустических СО выделяют несколько подтипов:

- инфразвуковые извещатели;
- пассивные акустические извещатели;
- активные акустические (или ультразвуковые) извещатели.

Все они тем или иным способом используют распространение в воздухе колебаний давления. Каждый из перечисленных подтипов будет рассмотрен далее.

Инфразвуковые извещатели

Инфразвуковыми называются датчики проникновения, регистрирующие изменение давления (возникновение низкочастотной звуковой волны) в помещении, в котором они установлены. Например, небольшое изменение давления имеет место каждый раз, когда дверь, ведущая в закрытое помещение, открывается или закрывается. Звуковые волны, возникающие в таких ситуациях, имеют частоту ниже 2 Гц. Инфразвуковые извещатели — пассивные датчики, которые могут быть установлены на некотором расстоянии от входных дверей помещения. Поступление наружного воздуха в закрытый объем помещения может вызвать подачу инфразвуковыми извещателями ложного сигнала тревоги.

Сейчас извещатели такого типа применяются довольно редко из-за жестких условий их применения и высокой частоты ложных срабатываний.

Пассивные акустические извещатели

Принцип действия пассивных акустических СО – пассивная регистрация акустических колебаний, возникающих при разбиении стекла.

Типичный акустический датчик состоит из микрофона, усилителя и блока обработки сигналов. Обработка сигналов может заключаться в фильтрации, подсчете импульсов или в интеграции импульсов и шумов. Извещатель выдает сигнал тревоги только при наличии звуков двух частот, разнесенных по времени. Сначала должен появиться звук низкой частоты, соответствующий удару по стеклу, и только после него звук высокой частоты, соответствующий падению осколков стекла.

Пассивные акустические извещатели отличаются ограниченной эффективностью и используются только для обнаружения неопытных диверсантов, производящих много шума при проникновении в защищаемую зону или при перемещении в ее пределах.

Извещатель FG-1525F американской фирмы Intellisense встраивается в стену напротив защищаемого окна и имеет несколько настроек чувствительности: расстояние от датчика до окна может составлять от 1,5 до 7,6 м.

Активные ультразвуковые средства обнаружения

В основном используются однопозиционные извещатели. Вокруг ультразвуковых извещателей, испускающих акустические волны с частотой в диапазоне от 19 до 40 кГц, образуется поле обнаружения. Обнаружение проникновения основано на регистрации сдвига частоты между передаваемым и принимаемым сигналом, вызываемого эффектом Доплера, возникающим при перемещении объекта (нарушителя) в зоне обнаружения. Амплитуда и диапазон сдвига частот зависят от размера движущегося объекта, скорости

его перемещения и направления перемещения. Форма зоны обнаружения с помощью ультразвуковых датчиков сходна с формой зоны обнаружения, характерной для однопозиционных микроволновых датчиков.

Большинство широко употребляемых твердых материалов, таких как строительные материалы, из которых изготовлены стены, картон, оконные стекла и т.д., способны останавливать или отражать ультразвуковые волны. Зоны затенения ультразвукового сигнала (уменьшения чувствительности датчика) будут создаваться объектами большого размера, расположенными в защищаемом объеме, такими, как книжные полки, столы и перегородки, разделяющие помещение на отделения. Как правило, эти трудности могут быть преодолены путем установки нескольких ультразвуковых датчиков.

Ультразвуковые волны не проникают через физические преграды типа стен и перегородок; следовательно, область их распространения может быть без труда ограничена объемом защищаемого помещения. Так как физические преграды непроницаемы для акустических волн, стены защищаемого помещения будут поглощать или отражать передаваемые сигналы. Ввиду того, что стены, не покрытые специальным мягким материалом типа звукоизоляционных тканей, поглощают очень небольшое количество ультразвуковых волн, большинство ультразвуковых волн ими отражается. Отраженные ультразвуковые волны обеспечивают заполнение защищаемого объема, вследствие чего нарушителю труднее проникнуть в помещение незамеченным.

Явления механического характера, такие, как вихревые возмущения в воздухе или различные источники акустических волн, расположенные в пределах защищаемой зоны, могут вызвать подачу ложного сигнала тревоги. Перемещения воздуха, вызываемые отопительными системами, системами кондиционирования воздуха, сквозняками и тому подобное, могут снизить эффективность обна-

ружения, ограничивая радиус действия ультразвукового датчика и в то же время вызывая подачу ложного сигнала тревоги. Акустические волны, испускаемые звонками, и свистящий шум, который обычно производят разгерметизированные отопительные радиаторы или приборы, содержащие сжатый воздух, обладают частотными характеристиками, способными вызвать срабатывание ультразвукового датчика. Полезным «побочным действием» ультразвуковых извещателей является способность регистрировать открытое пламя.

Другая характеристика окружающей среды, оказывающая воздействие на эффективность ультразвуковых датчиков — климатические условия в защищаемом помещении. Значительные изменения относительной влажности могут повлиять на характеристики приемника ультразвуковых волн таким образом, что чувствительность датчика повысится, и он будет регистрировать обычные для окружающей среды изменения, подавая ложные сигналы тревоги.

Ультразвуковые извещатели могут иметь также двухпозиционную конфигурацию; в этом случае регистрация перемещения в защищаемом объеме вызывается сочетанием доплеровского эффекта и изменения амплитуды принимаемого сигнала. Передатчик и приемник двухпозиционного ультразвукового извещателя устанавливаются, как правило, на потолке помещения таким образом, чтобы защищаемая зона находилась между ними. Дальность действия индивидуальных приемников может быть отрегулирована. Другие характеристики двухпозиционных извещателей сходны с характеристиками однопозиционных ультразвуковых извещателей.

Извещатель «Эхо-А» (рис. 2.14), выпускаемый по заказу ГУ ВО МВД РФ, является примером однопозиционного ультразвукового извещателя.

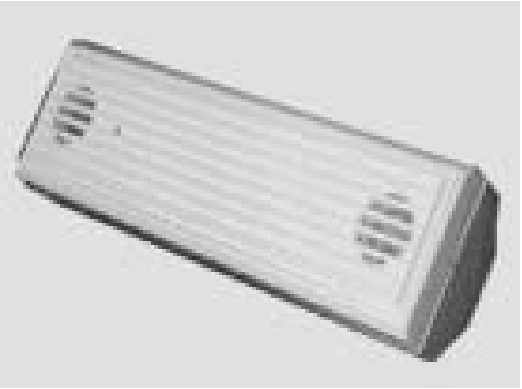


Рис. 2.14. Ультразвуковой извещатель «Эхо-А»

Данный извещатель имеет зону обнаружения каплевидной формы с регулируемой длиной от 2 до 8,5 м с максимальной шириной 4 м. Кроме нарушителей, двигающихся со скоростью от 0,3 до 2 м/с, он реагирует на открытые очаги пламени площадью от 0,1 м^2.

Также извещатель «Эхо-А» может быть установлен на потолке, что позволяет контролировать отдельные объекты (например, витрины, выставочные экспонаты), размещенные в больших помещениях.

2.9. Оптические средства обнаружения

Другим названием оптических извещателей является «инфракрасные извещатели». Их делят на активные и пассивные.

Активные оптические средства обнаружения

Принцип действия активных оптических извещателей состоит в формировании между излучателем и приемником луча инфра-

красного (ИК) излучения (с длиной волны 0,8…0,9 мкм) и регистрация его пересечения нарушителем.

Как правило, используются несколько передатчиков и приемников, позволяющих сформировать систему с множественными лучами инфракрасного света, причем лучи расположены обычно так, чтобы образовывалась вертикальная инфракрасная решетка (рис. 2.15). Может быть использована также технология генерации синхронизированных импульсов в целях снижения уровня интерференции и возможности нейтрализации датчика с помощью посторонних источников инфракрасного света. Это также позволяет извещателю функционировать при высокой фоновой засветке (например, при всходящем или заходящем солнце, свете фар и т.п.).

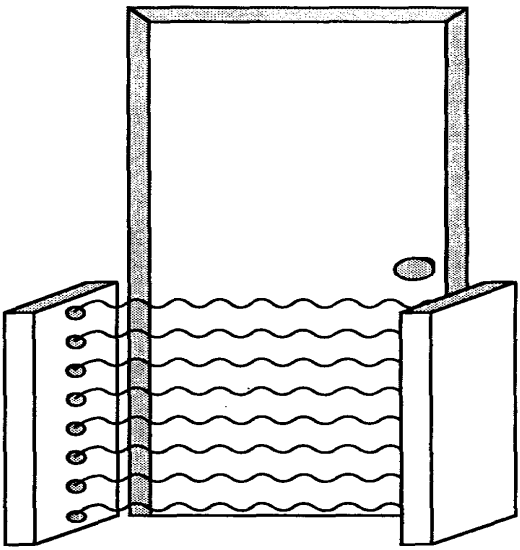


Рис. 2.15. Активная инфракрасная система обнаружения с решеткой из множества лучей

Узкая вертикальная зона действия извещателя не позволяет регистрировать перемещение в значительном объеме, вследствие чего при разработке СФЗ необходимо тщательно продумать расположение таких извещателей, существенно затрудняющее нейтрализацию датчиков посредством обхода или обмана. Эти извещатели могут применяться также в таких требующих дополнительной защиты небольших пространствах, как ворота для транспортных средств, дверные проемы и проходные. Инфракрасные извещатели могут действовать и на больших расстояниях (до 300 м). Инфракрасный свет невидим для человеческого глаза.

В целях снижения вероятности нейтрализации активного инфракрасного датчика путем обхода, извещатели такого типа следует устанавливать как минимум попарно, чтобы образовывать надежное инфракрасное заграждение, перекрывающее вход.

Инфракрасные извещатели могут подавать ложные сигналы тревоги при различных сочетаниях условий. Определенная концентрация дыма или взвешенной в воздухе пыли может приводить к рассеянию инфракрасного луча, достаточному для понижения регистрируемой приемником энергии до уровня, вызывающего подачу сигнала тревоги. Падающие предметы, небольшие животные и любые другие объекты, способные достаточно долго прерывать инфракрасное излучение, могут послужить причиной срабатывания инфракрасного датчика.

Извещатель «Вектор-СПЭК» (рис. 2.16) фирмы «СПЭК» выпускается в двух вариантах: с максимальной дальностью 75 и 150 м. Практически данное СО может использоваться и для защиты более длинных участков периметра, поскольку имеет запас по мощности 100 %, однако тогда во время сильного дождя или снега его работа будет нестабильной.

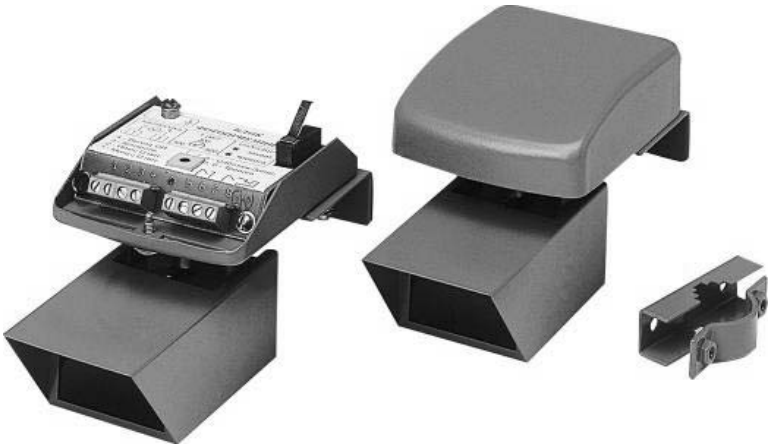


Рис. 2.16. Активный инфракрасный извещатель «Вектор-СПЭК»: приемник и излучатель

Данные извещатели имеют контакты синхронизации, что позволяет объединять несколько извещателей в многолучевые конфигурации. Можно, например, объединить два извещателя в двухлучевой барьер, который будет выдавать сигнал тревоги при пересечении любого луча. Более интересной является схема соединения, при которой сигнал тревоги выдается только при пересечении всех лучей одновременно. Это позволит исключить ложные срабатывания от падающих листьев, пролетающих птиц и других мелких объектов.

Пассивные оптические средства обнаружения

Принцип действия пассивных инфракрасных СО состоит в регистрации изменения теплового фона, вызванного движением нарушителя в зоне обнаружения. Тепловое излучение, исходящее от тела человека, имеет частоту, соответствующую длине волны 8…14 мкм, что примерно соответствует тепловому излучению, исходящему от горящей 50-ваттной электрической лампочки.

Пассивный инфракрасный извещатель представляет собой термочувствительный элемент или пироэлектрический приемник, регистрирующий тепловое излучение, исходящее от тела нарушителя, и преобразующий это излучение в электрический сигнал. Полученный сигнал затем усиливается и обрабатывается логическими схемами, которые срабатывают, как правило, при том условии, что источник излучения перемещается в зоне обнаружения датчика. Если полученный сигнал достаточно силен и имеет место требуемое перемещение излучающего объекта, генерируется сигнал тревоги. В целом, вероятность регистрации перемещения человеческого тела на фоне, для которого характерна изменяющаяся интенсивность теплового излучения, выше, чем вероятность регистрации перемещения объекта на единообразном тепловом фоне.

Выпускаются инфракрасные извещатели с однолучевой удлиненной конической формой зоны обнаружения и с многолучевой формой ЗО. Датчики с однолучевой удлиненной конической формой зоны обнаружения используются для защиты коридоров, тогда как датчики с многолучевой формой ЗО устанавливаются на больших открытых участках. Дальность действия извещателей с многолучевой формой зоны обнаружения составляет примерно от 6 до 9 м при угловой величине охвата от 70 до 120°. Дальность действия извещателей с однолучевой удлиненной формой поля обнаружения может составлять до 50 м. Часто один и тот же извещатель может иметь как протяженную, так и объемную зону обнаружения в зависимости от установленной в него линзы (зеркала) Френеля.

Птицы и небольшие летающие насекомые могут вызывать подачу инфракрасными извещателями ложных сигналов тревоги. Птица, пролетающая близко к датчику, может затенить фоновое тепловое излучение. Вместе с тем, перемещение птицы соответствует критериям, установленным для извещателей данного типа, в результате чего подается ложный сигнал тревоги. Так как инфракрасные извещатели оснащены линзами небольшого диаметра, на-

секомое, ползущее по поверхности линзы, может заблокировать зону обнаружения. Если насекомое будет находиться на поверхности линзы достаточно долго, может последовать ложный сигнал тревоги.

Инфракрасное излучение не проникает через большинство строительных материалов, в том числе через стекло. Следовательно, источники теплового излучения, расположенные за пределами зданий, как правило, не вызывают подачу ложных сигналов тревоги. Тем не менее, подача ложных сигналов тревоги может быть вызвана источниками, находящимися вне зданий и помещений, косвенным путем, а именно посредством нагревания отдельных участков. Например, в то время как стекло и плексиглас для окон являются эффективными фильтрами для инфракрасного излучения с интересующей нас длиной волны (от 8 до 14 мкм), солнечный свет, проникающий через окна, может нагревать отдельные участки поверхностей таким образом, что они начинают испускать инфракрасные волны с этой длиной волны.

Инфракрасные извещатели следует устанавливать поодаль от любых источников тепла, способных вызывать изменения температурных характеристик в радиусе действия линзы инфракрасного приемника. Извещатели такого типа следует удалять от перемежающихся нагретых участков в поле обнаружения или направлять в сторону от таких участков. Например, инфракрасные извещатели нельзя устанавливать поблизости от обогревательных приборов, радиаторов системы отопления, горячих труб и т.д. Тепловая энергия, излучаемая этими источниками, может вызвать тепловые возмущения в радиусе действия линзы инфракрасного детектора, которые приведут к изменению характеристик фонового излучения. Если тепловое излучение источника достаточно интенсивно, тепловые возмущения могут вызвать подачу ложного сигнала тревоги. Неэкранированная лампа накаливания, расположенная на расстоянии менее 3…5 м от извещателя, также может вызвать подачу лож-

ного сигнала тревоги, если она перегорит или погаснет в случае неисправности в системе электропитания.

Диаграмма направленности поля обнаружения типичного пассивного инфракрасного извещателя показана на рис. 2.17. Причем разделение зоны обнаружения на отдельные сегменты, которое достигается посредством применения оптических устройств (линз Френеля или зеркал), позволяет регистрировать перемещение объекта от одного сегмента к другому.

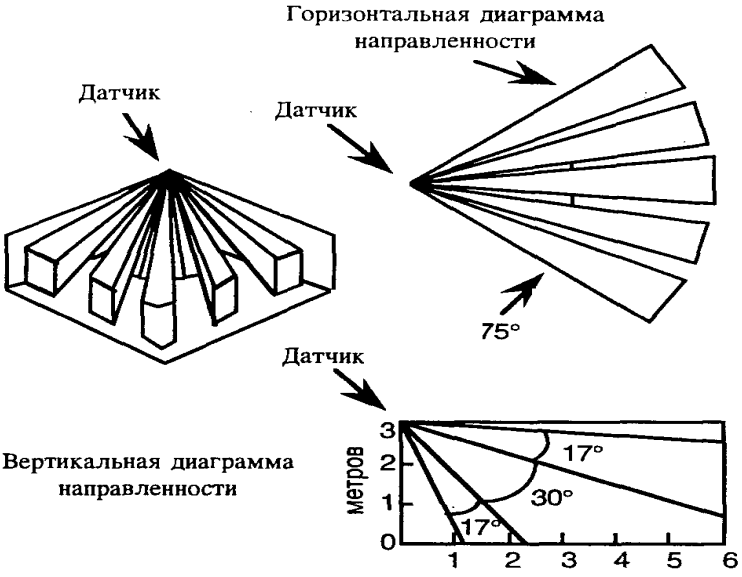


Рис. 2.17. Зона обнаружения пассивного инфракрасного датчика

Из-за сравнительно низкой стоимости, на рынке имеется огромное количество пассивных инфракрасных СО как российского, так и зарубежного производства со сходными характеристиками.

2.10. Контактные средства обнаружения

Принцип действия контактных СО состоит в отслеживании контакта (электрического или через магнитное поле) между двумя частями извещателя. Соответственно, контактные СО разделяют на магнитоконтактные и электроконтактные.

Магнитоконтактные средства обнаружения

Принцип действия магнитоконтактных СО состоит в пассивном контроле положения подвижного магнита, закрепленного на створке окна, ворот, на люке, двери и тому подобное. Данный тип СО может использоваться как на улице, так и в помещении.

Большинство таких извещателей относятся к категории электромагнитных реле, состоящих из двух компонентов: собственно реле и магнитного компонента. На рис. 2.18 изображена схема конструкции электромагнитного контактного реле (другие названия: «магнитоуправляемый контакт» или «геркон»).

Блок реле, содержащий электромагнитное контактное устройство, монтируется на неподвижной части двери или окна. Магнитный компонент, содержащий постоянный магнит, устанавливается на движущейся части двери или окна непосредственно напротив блока реле. Максимальное расстояние между реле и магнитом различно для разных моделей извещателей. Для извещателей, используемых на улице для защиты ворот, это расстояние может достигать 10 см. Пока дверь или окно закрыты, магнитное поле, исходящее от постоянного магнита, заставляет контакт электромагнитного реле оставаться в замкнутом (безопасном) положении. Последующее открывание двери или окна (удаление постоянного магнита от блока реле) вызывает резкое ослабление магнитного поля и перемещение контакта в разомкнутое (или тревожное) положение.

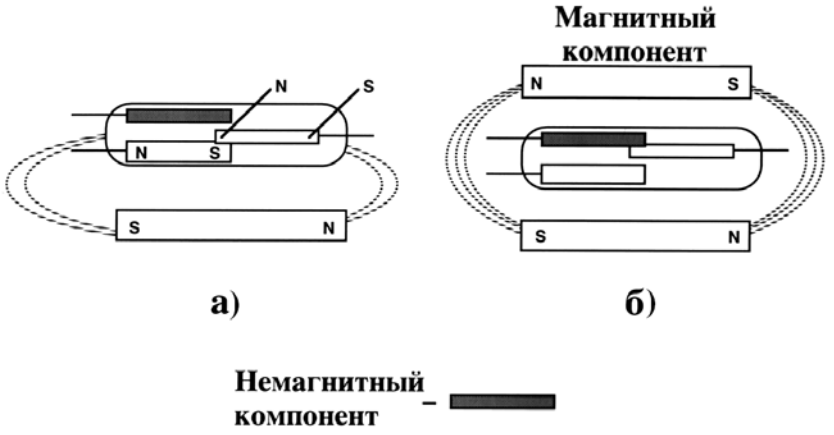


Рис. 2.18. Конструкция и принцип действия электромагнитного контактного реле: а) несбалансированного; б) сбалансированного

В некоторых устройствах такого типа устанавливается дополнительный подмагничивающий элемент, предотвращающий нейтрализацию датчика с использованием сильного магнита. Такие герконы называются сбалансированными. Выпускаются также электромагнитные извещатели с множественными контактными реле и множественными магнитами, устройства с перегорающими или плавящимися предохранителями и извещатели, регистрирующие прерывание напряжения, а также извещатели с экранированными корпусами. Некоторые модели оснащены электронными устройствами самопроверки.

Сбалансированные электромагнитные реле обеспечивают более эффективную защиту дверей и окон по сравнению с магнитными или механическими контактными или шариковыми реле. Тем не менее, защитные функции таких извещателей ограничиваются исключительно теми случаями, когда нарушитель проникает в помещение, открывая дверь или окно.

Преимуществами магнитоконтактных СО являются их простота, низкая стоимость, а также то, что для их функционирования не требуется электропитание.

Электроконтактные средства обнаружения

Принцип действия электроконтактных СО – это пассивный контроль целостности разрывных проволочных контактов, закрепленных на контролируемой поверхности или протянутых вдоль охраняемого периметра. Также их называют «датчики проводимости» или «датчики с разрывными проволочными контактами».

Обычно электроконтактные СО устанавливаются на поверхности или внутри стен, потолков и полов и позволяют регистрировать проникновение через конструкционные элементы различных типов. Извещатель состоит из проводящих проволочных элементов небольшого диаметра и БОС, генерирующего сигнал тревоги при прерывании контакта. Проволочные проводящие элементы могут быть установлены в любом расположении, соответствующем форме конструкционных элементов самой необычной конфигурации. При необходимости извещатели такого типа могут быть изготовлены с применением технологии производства печатных плат.

Решетки и экраны с проводящими проволочными элементами могут быть использованы для регистрации проникновения через вентиляционные отверстия, полы, стены, потолки, закрытые на длительное время отделения и отсеки хранилищ, а также через световые колодцы. Для извещателей такого типа характерна очень низкая частота ложных срабатываний, так как сигнал тревоги подается таким датчиком только в случае прерывания проволочного контакта. Нужно осуществлять постоянную периодическую проверку состояния извещателей с проводящими проволочными элементами в целях предотвращения попыток их блокирования или шунтирования.

Недостатком электроконтактных СО является необходимость восстановления проволоки после срабатывания. Часто при этом необходимо заменять всю проволоку.

К типу электроконтактных СО относятся как автономные быстроразворачиваемые системы обнаружения (например, «Краб-М1»), так и простые средства, не имеющие своих собственных БОС и подключаемые напрямую к аппаратуре сбора и обработки информации. Ко второму типу относятся различные проволочные конструкции и кнопки (например, кнопка, удерживаемая закрытой дверью в нажатом состоянии).

Средство обнаружения «Краб-1М» фирмы НИКИРЭТ используется для оперативного блокирования временных рубежей охраны (транспортных средств, грузовых площадок и т.п.), охраны отдельных участков (в лесу, на пересеченной местности), охраны отдельных стен, различных проемов и так далее. В качестве чувствительного элемента служит одножильный микропровод длиной от 10 до 500 м, при обрыве которого выдается сигнал тревоги.

Достоинствами данного СО являются простота установки (требуется не более 10 мин для оборудования рубежа длиной 500 м), отличная маскируемость (микропровод практически не виден на местности), а также то, что прибор способен определять расстояние до места обрыва провода с точностью не более 5 м.

2.11. Комбинированные средства обнаружения

Для особых объектов, где требуется исключительно высокая наработка на ложное срабатывание и вероятность обнаружения, разработаны комбинированные системы, сочетающие в себе несколько датчиков различного физического принципа действия. Расположение чувствительных элементов выбирается таким образом, чтобы сигнал от проникновения человека возникал одновременно в нескольких датчиках, тогда как помехи, оказывающие раз-

ное воздействие на каждый их них, разнесены во времени. Надо отметить, что комбинирование СО не может повысить и вероятность обнаружения, и наработку на ложное срабатывание одновременно, а только улучшает одну из этих характеристик за счет ухудшения другой.

Средство обнаружения «Протва-4» производства ГУП «СНПО «Элерон»» – пример системы, сочетающей в себе приборы трех принципов действия — сетчатое ограждение с трибоэлектрическим кабелем, реагирующим на вибрации, радиолучевое СО, зону обнаружения которого необходимо направить параллельно сетке, и датчик на основе «линии вытекающей волны», размещаемый в грунте в непосредственной близости от сетчатого заграждения. Электронный блок обрабатывает сигналы от каждого датчика в соответствии с логической схемой «2 из 3», т.е. сигнал тревоги формируется только при одновременном срабатывании любых двух датчиков, входящих в систему. Это обеспечивает резкое (на порядок) снижение частоты ложных срабатываний, сохраняя высокую вероятность обнаружения.

Средство обнаружения «Протва-4» позволяет контролировать периметр длиной до 7,5 км (60 участков от 50 до 125 м каждый) и имеет общую зону обнаружения шириной до 6 м. Система дает возможность определять направление пересечения ЗО, обеспечивает документирование событий.

Для помещений наиболее частый вид комбинирования – использование извещателей, содержащих в себе пассивный инфракрасный и однопозиционный микроволновый датчики. Реже вместо микроволнового используется активный ультразвуковой датчик. Подобное сочетание позволяет логически комбинировать сигналы тревоги, поступающие от ультразвукового или микроволнового датчика и от инфракрасного датчика с использованием логической операции «И», т.е. для подачи окончательного сигнала тревоги не-

обходима предварительная одновременная подача сигналов тревоги активным и пассивным датчиками.

Важно учитывать, что при логическом сочетании датчиков двух типов вероятность обнаружения проникновения с помощью сдвоенного датчика ниже вероятности обнаружения проникновения с помощью индивидуальных датчиков. Кроме того, для ультразвуковых и микроволновых датчиков характерна высокая вероятность обнаружения перемещения по направлению к датчику или от него, тогда как для инфракрасных датчиков характерна высокая вероятность обнаружения перемещения поперек поля обнаружения. Следовательно, вероятность обнаружения проникновения с помощью сдвоенного датчика, установленного в одной точке, будет меньше вероятности обнаружения с помощью двух индивидуальных датчиков, установленных в двух различных точках перпендикулярно друг к другу таким образом, чтобы их диаграммы направленности и поля обнаружения взаимно перекрывались. Поэтому в тех случаях, когда необходимо обеспечить повышенную вероятность обнаружения проникновения, рекомендуется устанавливать логически соединенные друг с другом индивидуальные датчики. Самая высокая вероятность обнаружения обеспечивается установкой индивидуальных датчиков с независимыми системами оповещения.

Детекторы движения серии 8100S (рис. 2.19) компании C&K используются тогда, когда требуется обеспечить надежную охрану в неблагоприятных условиях окружающей среды. Максимальная дальность действия детектора 8120S достигает 61 м.

Детекторы движения серии 8100S используют пассивную ИК и микроволновую технологии, которые обеспечивают необходимую помехоустойчивость, чувствительность и стабильность работы приборов в целом. Детекторы 8110S и 8120S имеют узкую диаграмму направленности, а 8140S – широкую. Детектор 8140S имеет 19 сегментов (лучей), образующих дальнюю (11 лучей), промежу-

точную (5 лучей) и ближнюю (3 луча) зоны обнаружения. Детектор 8120S – 9 сегментов, образующих дальнюю (1 луч), промежуточную (5 лучей) и ближнюю (3 луча) зоны обнаружения соответственно.

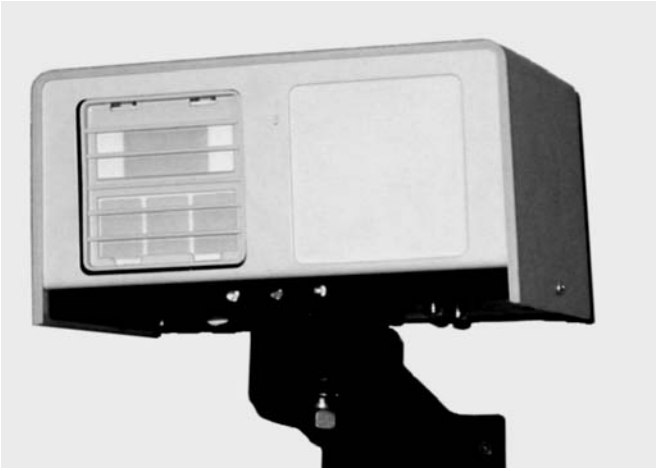


Рис. 2.19. Внешний вид детектора 8110S

Основные технические характеристики приборов серии 8100S.

- Размер зоны обнаружения, м – 27х21 (для 8140S); 37х3 (для 8110S); 61х5 (для 8120S).
- Рабочая частота микроволнового источника – 9–10,687 ГГц.
- Напряжение питания – 5,5–16,0 В.
- Потребляемый ток (при напряжении питания +12 В) – 35 мА.
- Выходные реле: тревоги (трехполюсное); вмешательства (двухполюсное); неисправности (трехполюсное).
- Габаритные размеры – 210х110х142 мм.
- Масса – 2,75 кг.

Извещатели имеют запатентованную цепь «Информер», которая используется для контроля работоспособности прибора. При

сопоставлении сигналов от обоих извещателей неоднозначность в их показаниях может означать, что один из них блокирован или неисправен. Сравнивая количество несоответствий (четыре возможных варианта), цепь «Информер» фиксирует неисправность извещателя и выдает соответствующее сообщение (выходное реле неисправности).

Неисправность извещателя может быть определена пользователем на месте (мигание красного светодиода) или по информации, передаваемой на контрольную панель при помощи специального, не входящего в комплект поставки, реле.

2.12. Средства обнаружения, использующие другие физические принципы

В классификации, приведенной в разделе 2.1, не были указаны устаревшие и редко используемые средства обнаружения. Некоторые из них описаны ниже.

Резистивные средства обнаружения

Первыми средствами обнаружения, применяемыми с 20-х гг. XX в., были системы в виде вертикального ограждения из колючей поволоки. Ограждение выполняло роль шлейфа, сопротивление которого измерялось резистивным датчиком. Датчик выдавал сигнал тревоги при обрыве или замыкании проводов. Такие системы сохранились и до наших дней, сегодня их использование вряд ли целесообразно как из-за устрашающего вида, так и из-за низкой эффективности: проволока через несколько месяцев покрывается слоем окисла и датчик не срабатывает при замыкании соседних проводов. Вероятность обнаружения в этом случае падает до 20 – 30 %.

Средства обнаружения натяжного типа

Средства обнаружения данного типа представляют из себя несколько нитей проволоки, натянутых параллельно друг другу. Извещатель реагирует на резкое изменение натяжения одной или нескольких нитей. Данный тип СО также выполняет роль физического барьера.

Самый простой способ регистрации изменения натяжения нитей проволоки – подключение каждой из них к тензометрическому датчику.

Магнитометрические средства обнаружения

В ряде случаев может представлять интерес магнитометрическая система обнаружения с чувствительным элементом в виде многопроводного кабеля, размещаемого в грунте на глубине 0,1…0,2 м вдоль охраняемого участка. Все жилы кабеля соединены последовательно, образуя распределенную индуктивную «катушку». Электронный блок измеряет индуктивность и выдает сигнал тревоги при ее изменении, связанном с пересечением зоны человеком, имеющим при себе какие-нибудь металлические предметы (огнестрельное или холодное оружие, предметы экипировки и т.д.). Чувствительность системы достаточна для обнаружения магнитной массы, характерной для обычного пистолета и тем более для автомата или карабина. В то же время система не реагирует на пересечение зоны такими животными, как кабаны, зайцы, собаки и кошки. Она перспективна для охраны участков периметров и границ в условиях, где неизбежны миграции диких животных, в комбинации с другими СО.

В заключение следует отметить, что существуют и другие варианты классификации средств обнаружения. После изучения

представленного материала можно, например, классифицировать СО по методам применения для охраны периметров.

В этой главе не рассмотрены особенности применения СО, позволяющие улучшить тактико-технические характеристики системы обнаружения в целом.

Вопросы для самоконтроля

1. Назовите основные принципы построения подсистемы обнаружения.
2. Какие существуют классификации средств обнаружения (СО)?
3. Назовите тактико-технические характеристики СО.
4. Объясните принцип действия СО:
    а) емкостных;
    б) радиотехнических;
    в) вибрационных;
    г) акустических;
    д) оптических;
    е) контактных.
5. Какие другие типы СО существуют?
6. Объясните необходимость существования комбинированных СО: цели комбинирования СО, принципы комбинирования СО, примеры комбинированных СО.
7. Какие СО применяются для охраны протяженных периметров?
8. Какие СО применяются для охраны помещений?
9. Назовите основные методы применения СО для охраны протяженных периметров.
10. Напишите расширенную классификацию СО по физическому принципу функционирования.

3. ПОДСИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Подсистема (далее – система) контроля и управления доступом – важнейшая составляющая системы физической защиты безопасности объекта. Она выполняет функции обнаружения и задержки и имеет свою структуру. В состав системы входят различные средства, реализующие различные технологии и процедуры, обеспечивающие доступ на объект или на отдельные части объекта субъектов, имеющих необходимые права, и препятствует доступу, если таких прав нет. Данный раздел посвящен рассмотрению классификации средств и систем контроля и управления доступом, общих технических требований к ним, структуры и принципов построения и функционирования. Нормативной основой данного рассмотрения является ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний» [3.1]. Стандарт введен в действие с 1 января 2000 года. Кроме этого в разделе будут описаны различные технологии аутентификации, и будет дан обзор наиболее часто используемых систем и оборудования [П.1, П.2, 3.2, 3.3].

3.1. Определения и назначение подсистемы контроля и управления доступом

Под *контролем и управлением доступом* (КУД) понимается комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, предметов, транспорта и других объектов в (из) помещения, здания, зоны и территории.

Подсистема контроля и управления доступом как составная часть системы физической защиты объекта представляет собой (*определение № 1*) совокупность организационных мер, оборудования и приборов, инженерно-технических сооружений, алгоритмов

и программ, которая автоматически выполняет в определенных точках объекта в заданные моменты времени следующие основные задачи:

•разрешает проход уполномоченным субъектам (сотрудникам, посетителям, транспорту);

•запрещает проход всем остальным.

Современные системы контроля и управления доступом могут решать и другие задачи в зависимости от специфики объекта. С учетом этого возможны еще два определения, относящиеся к системам КУД.

Определение № 2. Совокупность программно-технических и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением объекта в целом и отдельных его частей, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта.

Определение № 3. Совокупность оборудования и процедур, используемых для подтверждения права уполномоченных лиц проходить на территорию объекта, а также для обнаружения и задержания неуполномоченных лиц и неразрешенных материалов при перемещении персонала и материалов по установленным маршрутам.

С учетом задач, которые должна решать подсистема контроля и управления доступом, и которые отражены в определениях, приведенных выше, можно определить назначение систем КУД, которое формулируется в виде перечня основных и дополнительных возможностей.

Основные возможности системы контроля и управления доступом:

1) обеспечение входа и выхода в зоны объекта только уполномоченным субъектам;

2) обеспечение управления перемещением персонала и материальных ценностей в пределах объекта;

3) обнаружение и предотвращение попадания на объект неуполномоченных субъектов и транспорта;

4) обнаружение и предотвращение выноса с территории объекта материальных ценностей неуполномоченными субъектами;

5) обнаружение и предотвращение попадания на территорию объекта контрабандных материалов;

6) обеспечение задержки нарушителей при их попытках проникновения на объект;

7) предоставление службе безопасности (охраны) информации, предназначенной для быстрой оценки ситуации и развертывания сил ответного реагирования.

Дополнительные возможности системы контроля и управления доступом:

- организация и учет рабочего времени;
- управление освещением, лифтами, вентиляцией и другой сервисной автоматикой;
- управление автоматикой автостоянок;
- поддержка различных функций охранной и пожарной сигнализации;
- управление приборами подсистемы телевизионного наблюдения.

3.2. Базовые структуры, компоненты и принципы функционирования подсистемы контроля и управления доступом

Базовые структуры подсистемы контроля и управления доступом определяются концептуальной моделью управления доступом на объекте (рис. 3.1).

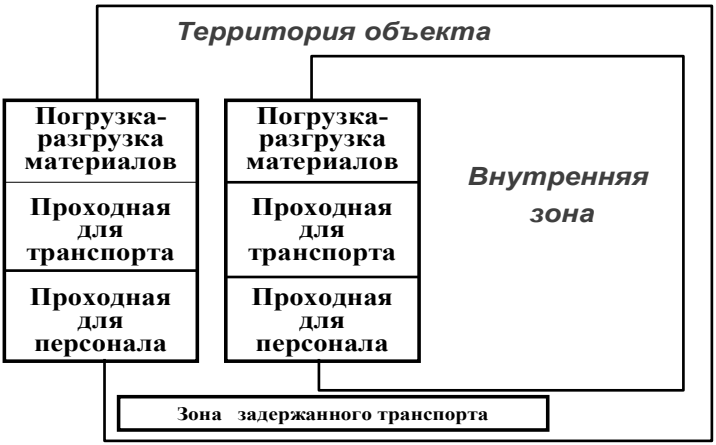


Рис. 3.1. Модель управления доступом на объекте

Объект разбит на зоны доступа, в каждую из которых имеют право проходить строго определенные лица (субъекты). Для доступа в зоны субъекту необходимо пройти набор точек доступа (ТД).

Точка доступа – полностью или частично контролируемая преграда (барьер) на границе контролируемой зоны. В точке доступа находится *проходная* (*пропускной пункт)*, которая наделяется особыми функциями, относящимися к решению основных задач системы КУД.

В каждой точке доступа установлены считыватели и исполнительные устройства.

Считыватель – устройство, предназначенное для считывания информации с идентификатора передачи ее в контроллер системы КУД.

Идентификатор – устройство или признак, по которому определяется субъект доступа.

Контроллер системы КУД – управляющее устройство, предназначенное для обработки информации со считывателя, принятия решения и управления исполнительными устройствами.

К исполнительным устройствам относятся шлагбаумы, турникеты, двери с замками и тому подобное.

Проходная (пропускной пункт), идентификаторы, считыватели, контроллеры и исполнительные устройства являются основными *компонентами системы КУД*. К ним также относят иногда размещаемые на проходных средства обнаружения неразрешенных (контрабандных) материалов (например, оружия, взрывчатых веществ) и материальных ценностей, запрещенных к перемещению (например, ядерных материалов, цветных металлов и т.д.). В совокупности такие компоненты иногда называют *средствами контроля и управления доступом* – это механические, электромеханические, электрические, электронные устройства, конструкции и программные средства, обеспечивающие реализацию контроля и управления доступом.

Управляющее устройство (контроллер) получает со считывателей информацию «свой/чужой». После того как характеристики субъекта определены и подтверждены, система принимает решение, имеет ли он право на проход через данную точку доступа. Для этого система проводит *авторизацию* субъекта доступа, проверяя его *уровень полномочий* (иногда говорят *уровень доступа* или *уровень привилегий*).

В системах контроля и управления физическим доступом применяется так называемая *дискреционная модель* доступа. Для каждого пользователя системы подразумевается существование *таблицы полномочий*, в которой каждой точке доступа объекта ставится в соответствие набор операций, которые субъект в данной точке имеет право выполнять. Возможно, на объекте будет целесообразнее иметь таблицы для каждой точки доступа, в которых каждому

уполномоченному субъекту будут поставлены в соответствие разрешенные ему действия.

В управляющем устройстве (контроллере) может вестись также документирование работы системы КУД, т.е. сбор, хранение и обработка информации о действиях субъектов и состояниях самой системы во времени.

Идентификация и аутентификация. Для выполнения основной задачи системе управления доступом необходимо определить, имеет ли право субъект выполнить запрашиваемое действие или нет. Для этого, прежде всего, надо ответить на два вопроса: «Кто этот субъект?» и «Тот ли он, за кого себя выдает?». Точность, с которой можно ответить на эти вопросы, определяет надежность системы КУД. Существует мнение, что если нет возможности точно определить характеристики субъекта, то все другие средства безопасности не имеют смысла.

Идентификацией (identification) называется процесс отождествления объекта с одним из известных системе объектов. Другими словами, идентификация – выяснение того, кто есть, например, человек (субъект), предъявивший системе некоторые данные (идентификатор).

Аутентификация (authentication) – проверка соответствия субъекта предъявляемому им идентификатору. Иначе говоря, аутентификация (употребляют термины верификация, отождествление) – это ответ на вопрос: «Является ли человек тем, кем представился?». Предположим, что человек с предъявленным идентификатором зарегистрирован в системе КУД. Аутентификация заключается в сравнении дополнительно вводимых признаков этого человека с хранящимися в базе данных (БД) эталонами (полученными во время контрольного заполнения БД).

Различие между идентификацией и аутентификацией на практике не всегда наблюдается – процедуры могут выполняться одновременно одним и тем же способом. Так, предъявляя пропуск ох-

ране, человек «представляется» и одновременно подтверждает личность (по фотографии). Применительно к аппаратно-программным средствам системы КУД, разница между процедурами идентификации и аутентификации заключается в следующем: при идентификации система просматривает всю БД зарегистрированных пользователей, сравнивая имеющиеся записи с введенным идентификатором, и если подобная запись найдена, система определяет уровень привилегий и другую информацию о субъекте. При аутентификации уже известно имя (идентификатор) субъекта, и для подтверждения его личности системе достаточно выполнить единственное сравнение – сопоставить дополнительно вводимые данные с данными о пользователе в базе данных.

Часто в литературе смешивают понятия аутентификации и идентификации. В дальнейшем, если в контексте нет смысла различать эти термины, мы будем говорить об аутентификации субъекта.

Анализ литературы по системам контроля и управления доступом показывает, что можно выделить три парадигмы подтверждения личности человека.

Первая парадигма называется *«Что Ты Имеешь»*. Человек может подтвердить личность, предъявив «уникальные» предметы (идентификаторы). Известно много типов идентификаторов, которые мы рассмотрим позже.

Основные проблемы, связанные с применением идентификаторов в системах КУД – вероятность их потери или кражи. Идентификаторы также можно забыть где-нибудь. Не исключена возможность изготовления нарушителями копии идентификатора.

Вторая парадигма аутентификации называется *«Что Ты Знаешь»*. Для подтверждения своей личности человек может назвать «секретные» сведения. Широко распространены системы с использованием, например, паролей и персональных идентификационных номеров (ПИН – кодов).

Парольные системы также имеют ряд недостатков. Пароль можно забыть, злоумышленник может подсмотреть пароль при вводе. Кроме того, пароли содержат относительно небольшое количество бит информации, что делает их неустойчивыми к подбору. Пароли часто выбирают, чтобы они легко запоминались, и злоумышленник в ряде случаев может угадать их.

Третья парадигма аутентификации человека – *«Что Ты Есть»* – подразумевает применение биометрических методов (будут рассмотрены позже). Системы управления доступом, построенные с использованием биометрической аутентификации, имеют ряд преимуществ перед системами на основе паролей или идентификаторов и встречаются в последнее время все чаще.

На практике почти всегда для увеличения безопасности систем применяют одновременно несколько способов аутентификации. Например, для повышения уровня безопасности на практике биометрическая аутентификация часто дополняется вводом ПИН (пароля) и/или предъявлением идентификаторов.

С учетом рассмотренных выше модели и принципов функционирования системы КУД базовую структуру системы КУД можно представить в виде, показанном на рис. 3.2.

Отличительной чертой базовой структуры системы КУД является использование или неиспользование ЭВМ для управления системой. Все определяется сложностью объекта и системы физической защиты. Поэтому реализацией базовой структуры системы КУД могут быть следующие схемы:

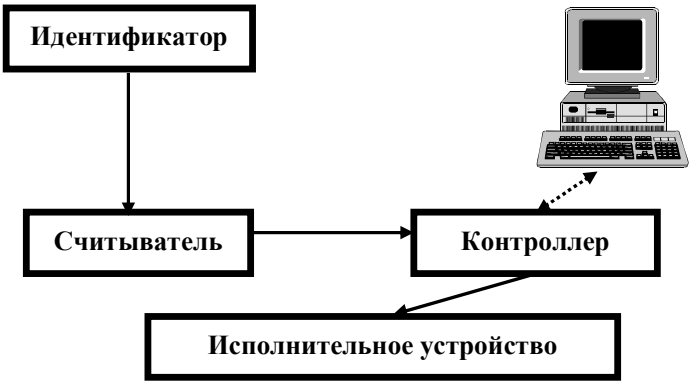


Рис. 3.2. Базовая структура системы КУД

1. Однодверная схема — реализует наиболее простую систему КУД малой емкости (до 16 точек доступа), имеющую автономный контроллер (без ЭВМ). Например, контроль и управление доступом в помещение, имеющее одну точку доступа (дверь с замком).

2. Многодверная схема — реализует систему КУД средней емкости (от 16 до 64 точек доступа), имеющую автономный или сетевой контроллер (с ЭВМ). Пример такой системы показан на рис. 3.3.

3. Комбинированная схема – реализует систему КУД большой емкости (более 64 точек доступа), имеющей сетевой комбинированный контроллер, позволяющий управлять не только компонентами подсистемы КУД, но и компонентами других подсистем (например, подсистемы телевизионного наблюдения). Примеры таких систем показаны на рис. 3.4 и 3.5 для комбинированной одноконтроллерной и комбинированной многоконтроллерной схем соответственно.

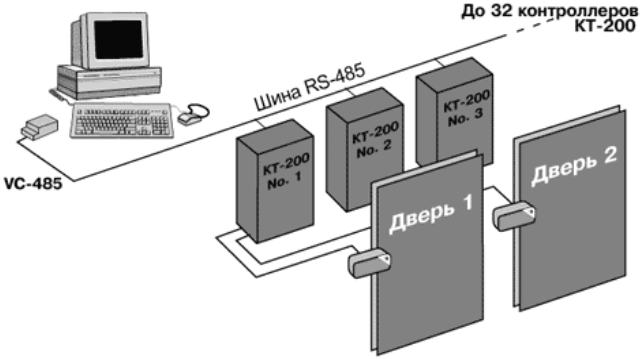


Рис. 3.3. Многодверная схема реализации системы КУД

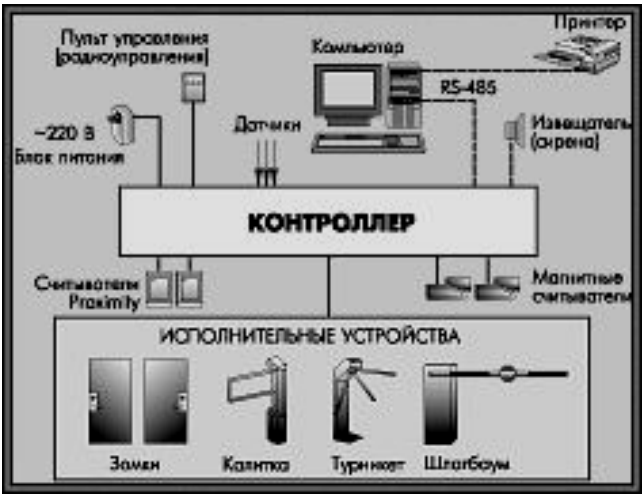


Рис. 3.4. Комбинированная одноконтроллерная схема реализации системы КУД

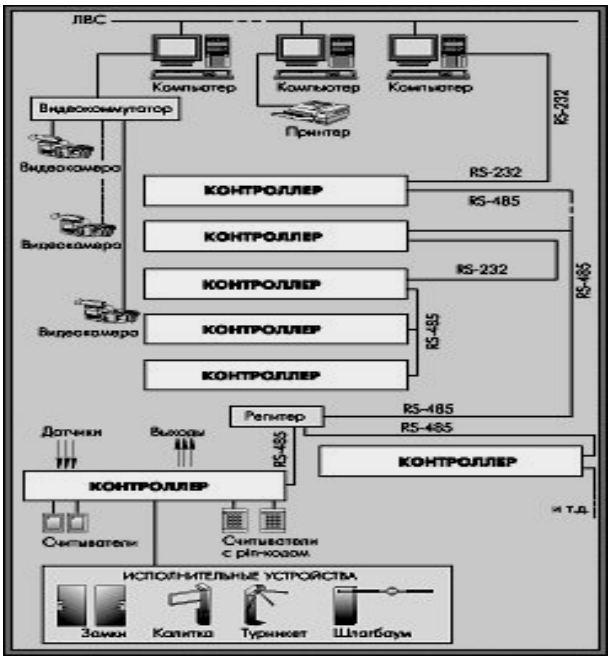


Рис. 3.5. Комбинированная многоконтроллерная схема реализации системы КУД

3.3. Идентификаторы и считыватели

Компоненты системы КУД (идентификаторы) как предметы, в которые (на которые) с помощью специальной технологии занесены идентификационные признаки, и считыватели как электронные устройства ввода этих признаков в систему должны рассматриваться вместе, так как в их основе лежит использование конкретного уникального признака субъекта доступа. Совокупность такого идентификатора и соответствующего ему считывателя будем называть устройством ввода идентификационного признака (УВИП).

По виду используемых идентификационных признаков УВИП могут быть:

•механические – идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);

•магнитные – идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);

•оптические – идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т.д.);

•электронные – идентификационные признаки представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);

•акустические – идентификационные признаки представляют собой кодированный акустический сигнал;

•биометрические – идентификационные признаки представляют собой индивидуальные физические признаки человека (рисунок радужной оболочки и сетчатки глаза, геометрия ладони, отпечатки пальцев, голос, динамика подписи, стиль нажатия клавиш при вводе информации и т.д.);

•комбинированные – для идентификации используются одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков УВИП могут быть:

•с ручным вводом – ввод производится с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;

•контактные – ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;

•дистанционные (бесконтактные) – считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;

•комбинированные.

В качестве идентификатора может использоваться запоминаемый код, вещественный код (предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации – карты, электронные ключи, брелоки и т.д.) или биометрический признак.

Запоминаемый код

Идентификатор на основе запоминаемого кода обеспечивает парольную аутентификацию. Субъект доступа, используя такой идентификатор, предъявляет системе КУД некоторую «секретную» (которую может знать только он) информацию. Пример идентификатора – комбинация цифр и/или букв. Также идентификатор может задаваться положениями различного рода переключателей.

Комбинацию, состоящую только из цифр, обычно называют персональным идентификационным номером (ПИН-кодом).

ПИН может выбираться самим субъектом или присваиваться соответствующими службами. Достоинство этого подхода – наименьшая вероятность, что субъект (человек) забудет ПИН. Недостаток – обычно люди выбирают в качестве ПИН цифры, связанные с датой рождения, номером телефона и тому подобное; следовательно, нарушителю легче подобрать такие коды.

По классификации ГОСТ Р 51241-89 [3.1] коды нормальной устойчивости должны состоять не менее, чем из 5 цифр, повы-

шенной устойчивости – не менее, чем из 7 цифр, высокой устойчивости – не менее, чем из 9 цифр.

Для ввода ПИН применяются цифровые клавиатуры (кодонаборники). Кодонаборники должны быть защищены от перебора кода. При вводе неразрешенного кода ввод должен быть заблокирован на некоторое время. Время должно быть выбрано таким образом, чтобы обеспечить заданную пропускную способность при ограничении числа попыток подбора за 1 ч (100 – нормальной, 30 – повышенной, 10 – высокой устойчивости к манипулированию по ГОСТ).

Чтобы затруднить злоумышленнику подсматривание паролей, применяют несколько методов.

Основной путь – ограничение углов обзора клавиатуры. Этого можно добиться с помощью как установленных сбоку и сверху «козырьков», так и путем применения в клавиатурах специальных дисплеев (например, на жидких кристаллах, имеющих угол бокового обзора всего несколько градусов).

Для защиты от подсматривания разработаны кодонаборники с переменным расположением цифр. Каждый раз, когда очередной субъект доступа подходит к считывателю, расположение цифр на клавишах меняется случайным образом. Даже если нарушитель узнает порядок нажатия клавиш, он не сможет узнать порядок цифр в пароле.

У парольной технологии аутентификации есть недостатки: субъект доступа может сообщить свой пароль неуполномоченному лицу, забыть свой пароль. Нарушитель может узнать ПИН угадыванием или перебором.

Достоинства парольной технологии аутентификации – низкая стоимость и удобство для пользователей.

На рис. 3.6 представлены различные варианты реализации кодонаборников: клавишный (рис. 3.6,а), сенсорный (рис. 3.6,б) и

комбинированный – сочетания кодонаборника и считывателя магнитных карт (рис. 3.6,в).

С целью повышения уровня безопасности почти всегда пароли применяются совместно с другими средствами аутентификации.

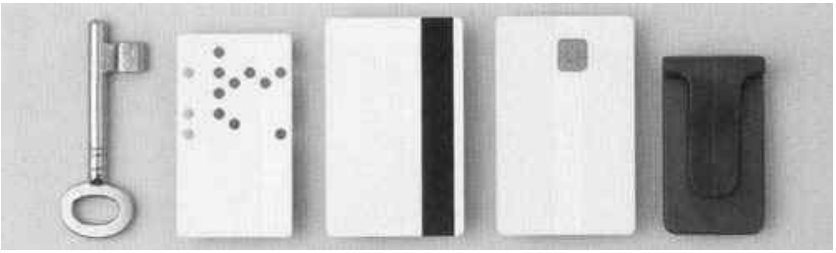
а) **б)** **в)**

Рис. 3.6. Примеры реализации кодонаборников

Вещественный код

Примеры некоторых идентификаторов, использующих вещественный код, показаны на рис. 3.7.

Они могут иметь различное исполнение: удостоверения, документы с штриховым кодом, обычные ключи от механических замков (рис. 3.7,а), карты перфорированные (рис. 3.7,б), с магнитной полосой (рис. 3.7,в), полупроводниковой электронной схемой (рис. 3.7,г) или изготовленные по проксимити-технологиям (рис. 3.7,д), электронные ключи – «таблетки», брелоки (рис. 3.7,а) и т.д.



а) б) в) г) д)

Рис. 3.7. Примеры идентификаторов, использующих вещественный код

Основные проблемы, связанные с применением таких идентификаторов – вероятность их потери или кражи. Их можно забыть где-нибудь. Не исключена возможность изготовления нарушителем копии идентификатора.

Рассмотрим более подробно некоторые из них.

Удостоверения. Для аутентификации субъекта (человека) часто используются удостоверения личности с фотографией или закодированные удостоверения.

Удостоверение с фотографией относительно несложно подделать. Возможно также изменить внешность субъекта таким образом, чтобы она соответствовала фотографии на удостоверении.

При использовании закодированных удостоверений охранник сравнивает хранящееся в памяти защищенной системы изображение служащего с изображением, закодированным на удостоверении. Преимущество такой системы – трудность подделки хранящейся в памяти системы изображения.

Считывание информации с идентификатора – удостоверения, как правило, осуществляет сотрудник охраны или службы безопасности объекта.

Штриховой код. Штриховой (линейный или bar) код представляет собой группу параллельных линий различной ширины, наносимых на поверхность карты. На сегодняшний день штрих-

код – самая дешевая технология изготовления карточек, что является ее достоинством в случае массового применения. Карточки можно печатать на обычном офисном принтере.

Считыватель является фоточувствительным элементом, мимо которого на некотором расстоянии проносится карта.

Главный недостаток технологии – простота подделки. Незащищенный штрих-код можно скопировать на ксероксе. В более сложных модификациях штриховой код заклеивают особой пленкой, непрозрачной для человеческого глаза и прозрачной для инфракрасного света. В настоящее время такой метод маскировки кода получил широкое распространение, но стоимость таких карт со штрих-кодом заметно возросла.

Современная разновидность технологии – двумерный штрих-код. Штрих-код представляет собой покрытый черными точками или другими фигурами светлый прямоугольник на карточке. Пример одного из видов двумерного штрих-кода показан на рис. 3.8.

Рис. 3.8. Двумерный штрих-код

Используя помехоустойчивое кодирование, на небольшой площади можно разместить до 2000 байт информации, что может быть более выгодным, нежели использование для этих целей более дорогих смарт-карт.

Чаще всего в системах контроля и управления доступом штрих-коды используются при оформлении пропусков на объект. Пример такого пропуска показан на рис. 3.9.

Рис. 3.9. Пример оформления пропуска с использованием одномерного штрих-кода

Код считывается при помощи специального лазерного или ПЗС-сканера. Для печати кода используются принтеры с хорошим разрешением (термо-трансферные или лазерные). Образцы считывателей показаны на рис. 3.10,а и 3.10,б для считывания штрих-кода, нанесенного на объект, и с удостоверений, предъявляемых на автостоянках, соответственно.

а)

б)

Рис. 3.10. Пример считывателей штрих-кода

Карты с магнитной полосой. Цифровые магнитные коды широко применяются в системах контроля доступа. Двоичный код записан на полоске магнитного материала, нанесенной на пластиковую карту (структура пластиковой карты показана на рис. 3.11).

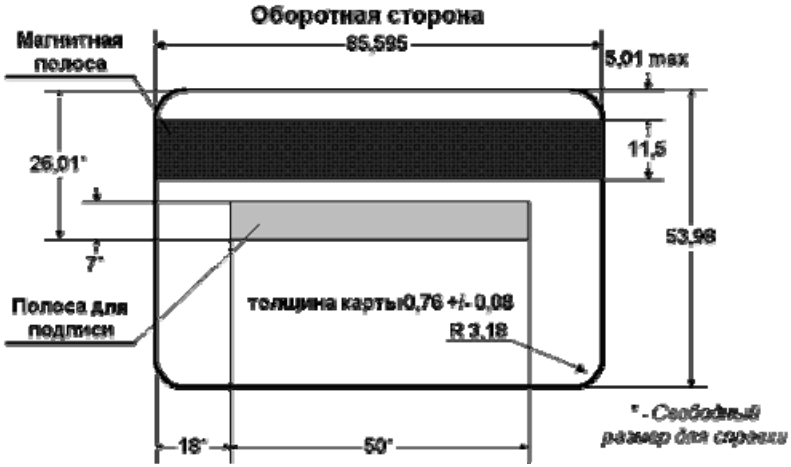


Рис. 3.11. Структура пластиковой карты с магнитной полосой

Данные считываются при перемещении карточки вдоль считывающей головки, аналогичной магнитофонной. Примеры считывателей показаны на рис. 3.12.

Согласно международному стандарту ISO на магнитной полосе может находиться от одной до трех дорожек записи объемом 78, 39, 106 символов соответственно, причем положение и ширина дорожек, способ и глубина записи регламентированы стандартом. Не все карточки и считыватели совместимы.

Магнитные полосы, наносимые на пластиковые карты, бывают двух типов: LoCo (Low Coercitive) и HiCo (High Coercitive). Различие между магнитными полосами LoCo и HiCo заключается в напряженности магнитного поля, используемого при намагничива-

нии. Для того чтобы записать информацию на магнитную полосу LoCo, используется поле напряженностью 300 эрстед. Для полосы HiCo применяется поле напряженностью от 2700 до 4000 эрстед. Пластиковые карты с магнитной полосой HiCo более надежны и долговечны, так как информация на магнитных полосах HiCo менее подвержена размагничиванию внешними магнитными полями, чем на полосах LoCo. Магнитная полоса HiCo используется в тех случаях, когда требуется защитить информацию на магнитной карте от возможного размагничивания, а также повысить защищенность карт от возможной подделки. Карты с магнитной полосой HiCo стоят дороже, чем карты с LoCo.

Рис. 3.12. Примеры считывателей пластиковых карт с магнитной полосой

Существует комбинированный случай – магнитная полоса с двумя слоями покрытия напряженностью 300 и 4000 эрстед. Данные, записанные на магнитном слое напряженностью 4000 эрстед, изменить практически невозможно. А данные, записанные на слое напряженностью 300 эрстед, могут перезаписываться.

Достоинства технологии:

- невысокая стоимость считывателей и магнитных карт;

•есть возможность с помощью специальных устройств менять код на карте.

Недостатки:

•простота подделки – данные, записанные на магнитной полоске, могут быть прочитаны и скопированы с помощью широкодоступного оборудования. Тем не менее, эта проблема может быть частично решена путем использования особых, нестандартных методов шифровки информации и считывания кодов;

•незащищенность от электромагнитного воздействия. Всю информацию можно стереть, оставив карту близ источника электромагнитного излучения;

•незащищенность от механического воздействия. Карту можно поцарапать ключом, находящимся в одном кармане с картой;

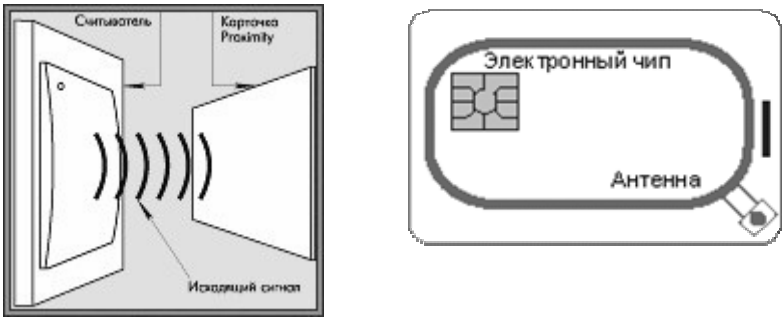
•быстрый износ карты от частых контактов со считывающей головкой;

•ограниченный срок службы считывающей головки (в среднем порядка 150 – 200 тысяч считываний).

Проксимити-технология. Проксимити-карты (иногда называемые радиокартами) и проксимити-брелоки предназначены для дистанционного считывания кодовой информации (рис. 3.13,а). Расстояние между считывателем и картой зависит от мощности считывателя и типа карты и варьируется от 5 см до нескольких метров. Структура проксимити карты показана на рис. 3.13,б.

Проксимити-считыватель, постоянно посылающий радиосигнал, представляет собой одну из обмоток воздушного трансформатора. Другая обмотка находится в карте или брелоке. Когда карта приближается к считывателю на определенное расстояние, энергии излучения считывателя оказывается достаточно, чтобы запитать кристалл, находящийся в карте. Получив питание, кристалл модулирует электромагнитное поле кодом, «зашитым» в него при про-

изводстве. Этот код демодулируется электроникой считывателя, приводится к требуемому типу интерфейса и поступает в виде ключа на контроллер.



а) **б)**

Рис. 3.13. Проксимити технология

Проксимити-карты делятся на активные и пассивные. В отличие от пассивных карт, излучающих за счет энергии поля считывателя, активные карты имеют встроенный передатчик на батарейке. Естественно, что расстояние срабатывания активной карты больше, чем пассивной. Кроме того, активные карты можно перепрограммировать, в то время как на пассивные карты информация записывается только один раз. Недостатки активных проксимити-карт – меньший, чем у пассивных карт, срок службы, более узкий рабочий диапазон температур, более высокая цена. Вообще, стоимость проксимити-систем сильно возрастает с увеличением дальности считывания.

В зависимости от используемого передатчиком диапазона частот проксимити-системы можно условно разделить на низкочастотные (от 33 кГц до 500 кГц) и высокочастотные (от 2,5 МГц до 10 ГГц). Наиболее распространены проксимити-системы, пере-

дающие на частоте 125 кГц. Высокочастотные карты имеют недостаток – повышенная возможность дистанционного снятия кода.

Для кодирования информации чаще всего используются Манчестер-код и бифазный код, обладающие свойствами самосинхронизации. В код всегда включаются контрольные данные (чаще всего, контрольные суммы по модулю 2 для битов, байтов и полубайтов) на случай нечеткого считывания кода. Так называемые «плавающие» коды, широко применяемые в автомобильных сигнализациях, в управлении доступом широкого распространения не получили, так как заметно удорожают систему.

Проксимити-карты могут существенно различаться и по используемой технологии записи идентификационного кода. Вот некоторые технологии записи и считывания:

•использование эффекта поверхностной акустической волны. Радиочастотный сигнал индуцируется поверхностью кристалла ниобата лития, расположенного в карте, и создает акустическую волну на поверхности другого кристалла, находящегося в считывающем устройстве. Эта волна затем модифицируется металлическими преобразователями;

•использование интегральных схем. Устройства этого типа передают закодированную информацию двумя способами. В первом случае код записывается при изготовлении устройства и не может быть изменен; во втором случае код загружается в интегральную схему и может быть изменен по желанию пользователя;

•использование схем с электрической настройкой. В таких устройствах код записывается в виде запрессованных в пластиковую карточку электрических схем, имеющих определенную резонансную частоту. Считывающее устройство постоянно сканирует весь диапазон рабочих частот и принимает сигналы, поступающие от резонирующих электросхем, встроенных в проксимити-карты.

Проксимити-идентификаторы можно изготавливать в виде карт (стандартный размер карты 85,7*54 мм, толщина от 0,9 до 3,1 мм), брелоков, жетонов на ремешке от часов и т.д.

Защищенность от простого перебора кода определяется числом разрядов кода. Широко распространены идентификаторы с длиной кода 24, 32, 40, 64, 128 бит.

Главное достоинство проксимити-систем – бесконтактное считывание. Отсюда следуют:

- возможность контроля за перемещением не только людей, но и предметов, автотранспорта и т.д.;
- благодаря отсутствию контакта между картой и считывателем, срок службы пассивных карт не ограничен (многие изготовители дают пожизненную гарантию). Активные карты через 5 лет требуют замены батарейки;
- удобство использования (не требуется ориентация в пространстве);
- высокая пропускная способность.

Основной недостаток технологии – высокая по сравнению с устройствами других типов стоимость. Первоначальная стоимость систем на проксимити-картах высока, но, благодаря отсутствию дополнительных эксплуатационных расходов, при длительных сроках эксплуатации оказывается не выше, чем стоимость систем, использующих другие технологии считывания.

Смарт-карты. Смарт-карта представляет собой пластиковую карточку, по размерам соответствующую обычной кредитной карточке, в которую заключены микропроцессор и запоминающее устройство. Внешний вид смарт-карт и считывателей показан на рис. 3.14,а и 3.14,б соответственно.

Внутренняя архитектура смарт-карты включает микропроцессор, позволяющий использовать сложные способы кодирования информации, постоянную память, в которую зашиты команды для процессора, оперативную память, используемую в качестве рабо-

чей, и перезаписываемую память для чтения и записи информации извне.

а) **б)**

Рис. 3.14. Смарт-карты (а) и считыватель смарт-карт (б)

Объем памяти наиболее распространенных типов смарт-карт варьируется от 1 до 256 Кбайт. В настоящее время появляются карты с памятью объемом до 1 Мбайта.

Основным преимуществом смарт-карт является большой объем памяти и высокая защищенность информации от попыток модификации и дублирования. Смарт-карты могут содержать значительное количество информации, причем многократно перезаписываемой.

Основные недостатки технологии: наличие электрического контакта со считывателем, очень низкая защищенность от физических воздействий, высокая стоимость.

Электронные ключи «TOUCH MEMORY». Термин «Touch Memory» можно перевести (дословно «касание памяти») как «моментальное считывание информации, записанной в памяти идентификатора».

Touch Memory представляют собой микросхему, размещенную в прочном корпусе из нержавеющей стали (16,3 мм в диаметре и высотой 3,2 или 5,8 мм). Внешний вид идентификатора Touch Memory показан на рис. 3.15

Рис. 3.15. Внешний вид идентификаторов Touch Memory

Для идентификации необходимо прислонить таблетку к считывателю, который имеет два считывающих контакта — один для передачи данных, второй «земля». Скорость считывания составляет порядка 0.1 секунды. Микросхема может иметь постоянное запоминающее устройство (ПЗУ) и оперативное запоминающее устройство (ОЗУ) либо иметь только ПЗУ. В ПЗУ записан уникальный неперепрограммируемый код длиной 8+48+8 бит, формируемый производителем методом лазерной записи на кремниевом кристалле. Ряд моделей, кроме индивидуального кода, позволяет заносить в ОЗУ дополнительную информацию о пользователе. В табл. 3.1 приведены данные по некоторым микросхемам Touch Memory.

Наиболее распространенная в России микросхема DS1990A имеет только ПЗУ. Иногда используют ряд микросхем серий DS19xx и DS18xx, отличающихся друг от друга объемом и структурой памяти. Идентификаторы с перепрограммируемой памятью (например, DS1991/92/96 и т.д.) питаются от литиевой батареи, которой хватает на 10 лет.

Таблица 3.1. Микросхемы Touch Memory

Тип		Память	Примечание
DS1990A	Serial Number iButton	ПЗУ	Серийный номер в ПЗУ
DS1991	MiltiKey iButton	1344 Bits NVRAM	3 области памяти по 384 байта
DS1992	Memory iButton	1024 Bits NVRAM	4 страницы по 256 бит
DS1993	Memory iButton	4096 Bits NVRAM	16 страниц по 256 бит
DS1994	Memory + Time iButton	4096 Bits NVRAM	16 страниц по 256 бит
DS1995	Memory iButton	16384 Bits NVRAM	64 страницы по 256 бит
DS1996	Memory iButton	65536 Bits NVRAM	128 страниц по 256 бит
DS 1954	Crypo iButton	Secure Coprocessor	Криптографический сопроцессор
DS1985	AddOnly iButton	16384 Bits EPROM	Однократно программируемая память
DS1986	AddOnly iButton	65536 Bits EPROM	Однократно программируемая память

Среди достоинств систем Touch Memory можно выделить: компактность; высокую стойкость к механическим повреждениям (выдерживают статическую нагрузку до 11 кг), коррозии, перепадам температур (от -40 до +70 или +85 °С); достаточно высокую скорость считывания и сравнительно небольшую стоимость системы. Различные модификации Touch Memory могут содержать встроенные часы или термометр. В настоящее время появилась новая модель DS1954 со встроенным криптографическим ключом длиной 1054 бит, что в принципе должно повысить защищенность системы.

Главный недостаток технологии – наличие контакта с гальванической связью с микроконтроллером. Отсюда низкая стойкость к вандализму и влиянию статического электричества (известны случаи выхода системы из рабочего состояния при помощи электрошока).

В системах с повышенными требованиями к безопасности Touch Memory либо не применяются вовсе, либо используются в комбинации с другими средствами (в простейшем случае дополнительно ставятся клавиатуры с ПИН-кодом).

Оптический код. Оптический код представляет собой определенную конфигурацию точек, расположенных на вкладыше, запрессованном в карточку-удостоверение, или светопроницаемом материале. Фотоэлементы считывающего устройства регистрируют изменения освещенности при просвечивании оптического кода и определяют взаимное расположение точек, образующих код. Для того чтобы оптический код было трудно скопировать, расположение точек может быть замаскировано пленкой, непрозрачной для обычного света и прозрачной для инфракрасных лучей.

Кроме того, точки можно наносить с помощью особой краски, непрозрачной для инфракрасных лучей, на поверхности, прозрачной для инфракрасных лучей. Этот метод позволяет хорошо предохранять удостоверения с оптическими кодами от попыток видоизменить или скопировать их. Удостоверение с оптическим кодом можно изготовлять из полностью немагнитных и неметаллических материалов, что позволяет избежать взаимодействия карточек с чувствительными металлоискателями.

На практике используется редко.

Магнитный точечный код. В настоящее время также используются несколько систем с магнитными точечными кодами. Магнитный код представляет собой конфигурацию намагниченных участков или точек. Код определяется по расположению и полярности намагниченных участков. Считывающее устройство оснаще-

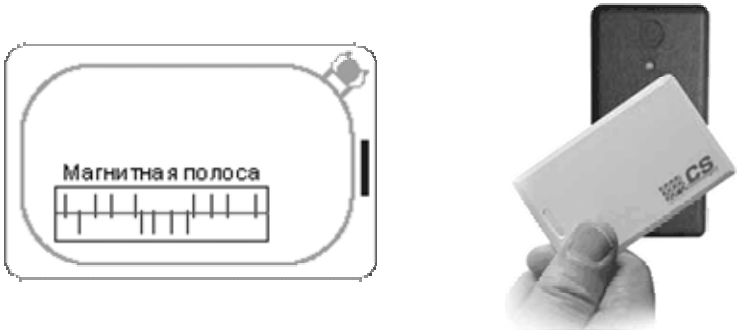
но либо магнитными датчиками, передающими электрические сигналы, либо магнитными контактными реле, механически срабатывающими, когда намагниченный участок с соответствующей полярностью находится поблизости от контакта. Намагниченные участки могут быть стерты, если удостоверение попадет под воздействие достаточно сильного магнитного поля, но опыт показал, что эта проблема возникает крайне редко. Количество информации, которое может быть записано с помощью магнитного точечного кода, не превышает 60 бит. Так как существует возможность изготовления оборудования, копирующего или изменяющего конфигурацию намагниченных участков, вероятно изготовление поддельных удостоверений.

На практике используется редко.

Виганд-карты. Данный тип идентификатора использует физический эффект, открытый в 1975 г. американским исследователем Джоном Вигандом (John R. Wiegand). При исследовании воздействия электромагнитных полей на различные типы проводников он обнаружил, что при наличии магнитного поля сверхкороткие проводники строго определенного состава, названного позже Виганд-сплавом, вызывают гигантский индукционный отклик. Причем если магнитное поле направлено в одну сторону, то наблюдается большой положительный, а если в противоположенную, то большой отрицательный выбросы индукционного тока.

В 1976 г. американская корпорация Echlin Inc. выкупила все права на данное открытие и в 1980 г. ее дочерняя фирма Sensor Engineering Co. начала выпускать считыватели магнитных карт, использующие обнаруженный эффект.

Виганд-карты изготавливают, запрессовывая в пластик два ряда кусочков проволоки из Виганд-сплава (специальный сплав, имеющий практически идеально прямоугольную петлю гистерезиса с достаточно большой амплитудой). Структура Виганд-карты показана на рис. 3.16,а.



а) **б)**

Рис. 3.16. Структура Виганд-карты (а) и внешний вид комплекса «карта-считыватель» (б)

Проволочки располагаются в уникальной последовательности, определяющей код карты (более 30 бит).

Считыватель карт практически представляет собой индукционную катушку с двумя магнитами противоположной полярности, причем все это находится в пластиковом или металлическом корпусе и для полной герметичности залито специальным изоляционным материалом. Внешний вид такого считывателя с образцом Виганд-карты показан на рис. 3.16,б.

При проведении пластиковой карты вдоль считывателя система контроля доступа получает двоичный код, записанный на карте. При считывании данных карта не контактирует со считывателем, тем не менее, карту необходимо помещать рядом с считывателем определенным образом. Поэтому Виганд-технологию называют «условно-бесконтактной».

К основным достоинствам данного типа идентификаторов и считывателей можно отнести следующие:

- хорошая износостойкость;
- высокая надежность в силу простоты устройства;

•устойчивость карты к электромагнитному излучению и физическим воздействиям;

•высокая защищенность от подделки (состав сплава хранится в секрете);

•приемлемая стоимость считывателей и карт.

Биометрическая аутентификация

Биометрические устройства ввода идентификационного признака используют индивидуальные физические признаки человека как субъекта доступа. В данном случае могут использоваться следующие биометрические признаки: рисунок радужной оболочки и сетчатки глаза, геометрия ладони, отпечатки пальцев, голос, динамика подписи, стиль нажатия клавиш при вводе информации и так далее.

Пред тем как более подробно рассмотреть данные идентификационные признаки, необходимо определить характеристики, по которым их можно сравнивать, и определить порядок проведения биометрической аутентификации.

Основными характеристиками биометрической аутентификации являются:

1. Суммарное время, необходимое для ввода идентификационных данных в систему, их обработку и принятие решения на пропуск или не пропуск на объект субъекта доступа – *Tc.*

2. Цена биометрической системы аутентификации, которая определяется ценой считывателя и затратами на обработку данных. Необходимо отметить, что цены на современные системы биометрической аутентификации по мере расширения их использования заметно снижаются.

3. Точностные характеристики: вероятности ошибочного отказа уполномоченному субъекту (*False Reject Rate, FRR*); вероятно-

сти ошибочного пропуска субъекта, не имеющего полномочий (*False Acceptance Rate, FAR*). Если определить эти характеристики в зависимости от точности обработки изображений при вводе данных в систему КУД (или временной длительности вычислений *T*в), то можно получить характерное поведение этих характеристик, показанное на рис. 3.17.

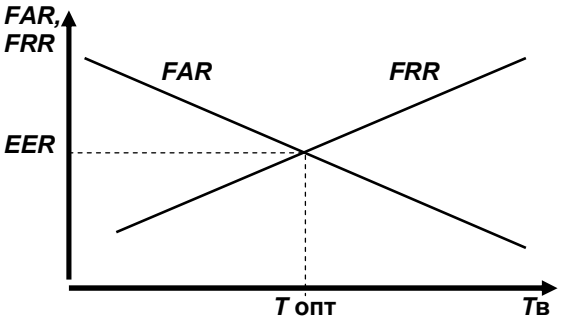


Рис. 3.17. Графики зависимости точностных характеристик от времени обработки данных при идентификации

Анализ приведенных характеристик показывает, что при увеличении времени (*T*в*)* обработки идентификационных данных при их вводе в систему КУД, вероятность того, что будет отказано в проходе на объект уполномоченному субъекту (*FRR*), растет, а вероятность того, что ошибочно будет пропущен на объект неуполномоченный субъект (*FAR*), снижается.

Признано считать, что оптимальное время обработки данных *T*опт (оптимальная точность ввода данных) определяется при условии, когда вероятность отказа уполномоченному субъекту и вероятность пропуска неуполномоченного субъекта будут равны (*FRR=FAR*). Эта ситуация соответствует точке пересечения двух графиков. При этих условиях определяется еще одна точностная

характеристика: ордината точки пересечения кривых *FRR(T*в*)* и *FAR(T*в*) – ERR (Equal Error Rate).*

Следует отметить, что события, связанные с задержкой уполномоченного субъекта и пропуском неуполномоченного субъекта, не являются однозначными с точки зрения последствий для безопасности объекта физической защиты. С ошибочной задержкой уполномоченного субъекта можно достаточно быстро разобраться с использованием других процессов аутентификации (например, проверив удостоверяющие документы). Ошибочный пропуск на объект неуполномоченного субъекта (потенциального нарушителя) может иметь катастрофические последствия для объекта. Поэтому при использовании описанных выше точностных характеристик необходимо учитывать специфику объекта. В дальнейшем будет проведено сравнение различных систем биометрической аутентификации на основе анализа следующих характеристик: *FRR, FAR, Tc.*

Независимо от выбранного метода биометрической аутентификации порядок осуществления процесса аутентификации будет един:

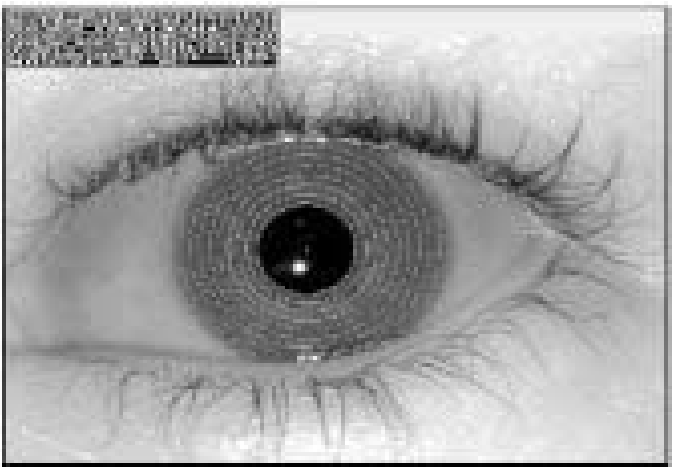
- фиксация биометрической характеристики;
- ввод ее в систему КУД (чаще всего вводится изображение, возможен ввод звука или других характеристик);
- выделение зон аутентификации;
- получение интегрального цифрового кода, соответствующего данной характеристике;
- поиск в базе данных, сформированной ранее, данных, близких к полученному коду;
- сравнение этих кодов;
- принятие решения о разрешении или не разрешении прохода (выдача команды на исполнительное устройство).

Рисунок радужной оболочки. Радужная оболочка (окрашенная часть, ирис) каждого глаза абсолютно уникальна. Даже у однояйцовых близнецов рисунки радужек разные. Радужная оболочка защищена от внешней среды роговицей и тканевой жидкостью; в отличие от сетчатки, однако, радужная оболочка ясно видна на расстоянии. Случайные рисунки ириса созданы сплетением сетчатой структуры соединительной ткани и других видимых признаков (слоев, борозд, корон, впадин, пятен и т.п.). Рисунок ириса стабилен в течение всей жизни. Пример рисунка ириса показан на рис. 3.18,а, а вводимое изображение в систему с результатом обработки (двумерный код) – на рис. 3.18,б.

Для фиксации и ввода данной биометрической характеристики используются специальные считывающие устройства, применяющие телевизионную технику. Примеры реализации таких считывающих устройств приведены на рис. 3.19.

Процесс идентификации по ирису начинается с получения изображения глаза. Для считывания пользователю достаточно посмотреть на специальное отверстие считывающего устройства с расстояния примерно 1 м. Далее на изображении выделяются границы зрачка и радужки, исключаются зоны, прикрытые веком, устраняются блики, определяется фокус для обработки изображения. Затем изображение ириса обрабатывается и кодируется. Поиск в базе данных осуществляется в реальном времени, поэтому скорость идентификации достаточно высока (при 10 тыс. зарегистрированных пользователей она составляет 2 с). Непосредственно в устройстве может храниться информация о большом количестве субъектов доступа (например, 1500). При хранении данных на компьютере число таких субъектов не ограничено.

а)



б)

Рис. 3.18. Изображение радужной оболочки глаза (а), обрабатываемое изображение с результатом обработки (б)

Очки и контактные линзы не являются помехой работе системы. Реакция ириса на свет и естественное колебание зрачка делают невозможным обмануть систему при помощи подстановки фотографии.

Характеристики некоторых из систем представлены в табл. 3.2. Системы аутентификации на основе анализа радужной оболочки

глаза обладают очень высокой точностью. В частности, система фирмы *IriScan* считается одной из самых точных биометрических систем в настоящее время.

Рис. 3.19. Считыватели рисунка радужной оболочки глаза

Расположение кровеносных сосудов сетчатки глаза. Ряд биометрических систем проводит автоматическую аутентификацию человека на основании уникальной картины расположения кровеносных сосудов сетчатки глаза (глазного дна). Внешний вид такой системы показан на рис. 3.20.

При работе подобных систем пользователи должны смотреть в видоискатель прибора. Участок сетчатки сканируется неполяризованным светом низкой интенсивности. Различная интенсивность отраженного света отображает расположение кровеносных сосудов.

Характеристики одной из систем аутентификации по расположению кровеносных сосудов сетчатки глаза *Icam 2001* (фирмы *EyeDentify)* приведены в табл. 3.2.

Рис. 3.20. Считыватели рисунка расположения кровеносных сосудов сетчатки глаза

Сравнение характеристик двух систем аутентификации, связанных с анализом изображения элементов глаза человека, показывает, что оба подхода обладают, во-первых, малой вероятностью ошибочного пропуска неуполномоченного субъекта, что говорит о высокой эффективности этих систем. Во-вторых, вероятность ошибочного отказа уполномоченному субъекту в первой системе существенно ниже аналогичной характеристики у второй системы. В-третьих, и быстродействие у этой системы выше. Все это дает определенные преимущества первой системе.

Кроме этого к недостаткам второй системы можно отнести более высокую цену и неудобство ее использования. Процесс получения изображения сетчатки глаза неприятен пользователям – многие стараются избежать аутентификации, защищая свои глаза. Поэтому область применения технологий аутентификации по расположению кровеносных сосудов сетчатки глаза – объекты высокой степени секретности.

Папиллярные узоры. Кожа человека состоит из двух слоев. Наружный слой называется эпидермисом, а второй, более глубокий, – дермой. Поверхность дермы, прилегающая к эпидермису, образует многочисленные выступы – так называемые дермальные

сосочки. На ладонных поверхностях кистей, в частности пальцев, дермальные сосочки складываются в ряды. Поэтому эпидермис, повторяющий строение внешнего слоя дермы, на этих участках тела образует небольшие складки, отображающие и повторяющие ход рядов дермальных сосочков. Эти складки называются папиллярными линиями и отделяются друг от друга неглубокими бороздками. Папиллярные линии, особенно на поверхностях пальцев кисти, образуют различные узоры, называемые папиллярными узорами.

Таблица 3.2. Характеристики систем биометрической аутентификации

Биометрическая характеристика	**Тип/ фирма**	***FRR*, %**	***FAR*, %**	***Tc*, с**
Радужная оболочка глаза	*System 2000EAC/ IriScan*	0,00066	0,00078	2
	EC-I 400/ Evermedia Co., Ltd	0,00001	0,0001	1
Сетчатка глаза	Icam 2001/ *EyeDentify*	0,4	0,001	4
Отпечаток пальца	Identix	1	0,0001	0,5
	U.are.U 4000/ DigitalPersona	1,4	0,01	1
	StartekBioMet	1	0,0001	1
	«Кордон»	1	0,0001	1
	DS-100	-	0,001	1-3
Кисть руки	Partners Recognition	0,1	0,1	1
	Systems	0,1	0,1	1
	Digi-2	0,01	0,01	1
	HandKey-II/ Recognition Systems	0,001	0,00001	1
Особенности голоса	Voice Guardian	5	2	-
	SpeakerKey	4,3	0,66	-
	«Кристалл»	2-4	0,7	-
Особенности почерка	«Кристалл»	1-3	1,0	-
	IBM	0,2	0,4	12,5

Рисунок папиллярного узора (рис. 3.21) на протяжении всей жизни человека остается неизменным, размер узора окончательно фиксируется к 18 – 20 годам. Папиллярный узор каждого пальца любого человека индивидуален и присущ только этому пальцу. После любых повреждений эпидермиса, не затрагивающих сосочков дермы, папиллярный узор в процессе заживления восстанавливается в прежнем виде. Если повреждены сосочки дермы, то образуется рубец, в определенной мере деформирующий в этом месте узор, но не изменяющий его первоначального общего рисунка и деталей строения в других местах.

Рис. 3.21. Рисунок папиллярного узора пальца человека

Для ввода образа отпечатка пальца используется несколько типов датчиков. Существуют датчики, измеряющие электроемкость выступов и впадин на коже пальца. Действие оптических датчиков основано на том факте, что зоны контакта выступающих папиллярных линий имеют более низкий коэффициент отражения света. Ультразвуковые датчики позволяют минимизировать влияние на результат распознавания грязи и пыли. Перспективна технология получения, обработки и хранения голограмм отпечатков.

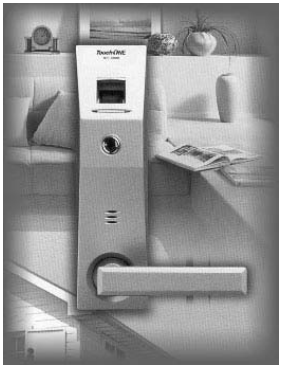
Конструкции считывателей различного типа показаны на рис.3.22. При этом они могут быть автономными (рис. 3.22,а,б), комбинироваться с другими средствами аутентификации, напри-

мер, со считывателями ПИН-кода (рис. 3.22,в) или выполняться в едином конструктиве с исполнительным устройством – замком (рис. 3.22,г).

а)

б)

в)



г)

Рис. 3.22. Считыватели отпечатка пальца

В некоторых системах предусмотрены меры защиты от использования муляжей пальцев, а также корректировка изображения в соответствии с состоянием кожи пальца – возможны настройки контрастности и яркости, регулировка уровня белого.

Характеристики наиболее популярных систем аутентификации по отпечаткам пальцев приведены в табл. 3.2. Их анализ показывает наличие высокого быстродействия, низкой вероятности ошибоч-

ного пропуска неуполномоченных субъектов и большую по сравнению с первыми двумя методами вероятность ошибочного задержания уполномоченных субъектов.

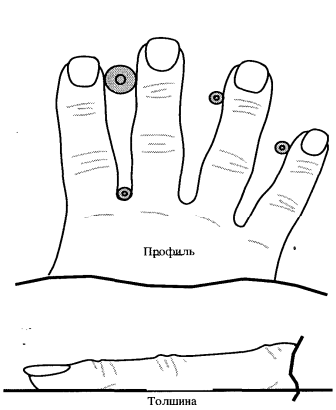
Достоинства систем идентификации по *папиллярным узорам* – небольшие размеры устройств, удобство (можно встраивать сканеры даже в клавиши), невысокая (и постоянно снижающаяся) стоимость систем, высокая точность. К недостаткам технологии следует отнести возможность влияния на результат следов предыдущего отпечатка, порезов, грязи. Имеется и психологическая проблема – у некоторых людей снятие отпечатков пальцев устойчиво ассоциируется с криминалистикой.

Области применения технологии – управление доступом в режимные помещения, к источникам информации (в том числе компьютерам и вычислительным сетям), юридическое подтверждение права на использование различных документов и пластиковых карт.

Форма кисти руки. В некоторых биометрических системах при аутентификации человека анализируется форма кисти руки.

Несмотря на изменение формы кисти как с течением жизни человека, так и за относительно короткие сроки, практически постоянными остаются отношения размеров, форма пальцев, расположение суставов. В современных системах распознавания по форме руки применяется компенсация – образец корректируется при каждой успешной аутентификации. Принцип аутентификации по кисти руки человека поясняет рис. 3.23, а некоторые характеристики наиболее распространенных систем приведены в табл. 3.2.

Данный метод предусматривает сличение профиля руки входящего человека с ранее полученным шаблоном по размеру ладони, длине, ширине и толщине пальцев и по ряду других параметров (рис. 3.22, а). Первоначальная запись шаблона геометрии руки реализуется с помощью трехразового сканирования кисти руки сотрудника и усреднения полученной информации.



а) **б)**

Рис. 3.23. Аутентификация по форме кисти руки

Для того чтобы биометрическая система могла произвести считывание, человек должен положить ладонь руки на панель устройства, а специальные штырьки-фиксаторы помогают скорректировать ее расположение (рис. 3.23,а,б). Встроенные светодиоды на панели считывателя сигнализируют о корректности расположения ладони, что упрощает взаимодействие человека с устройством.

Процедура верификации кисти руки осуществляется с помощью инфракрасной подсветки и регистрации данных специальной CCD-телекамерой. За счет боковых зеркал, которые попадают в обзор телекамеры, устройство также получает информацию о толщине и габаритах кисти руки. Отсканированное изображение биометрических показателей преобразуется по специальному алгоритму в цифровую информацию (размер шаблона – 9 байт), после чего происходит сравнение данных с шаблоном, хранящимся в памяти. По результатам соответствия полученной информации шаблону биометрическая система принимает соответствующее решение.

Считыватель геометрии кисти руки, как правило, комбинируется с устройством ввода ПИН-кода (рис. 3.23, б) и может сочетаться с карточными системами идентификации.

Двухэтапная или даже трехэтапная процедура идентификации пользователя, с одной стороны, существенно повышает уровень безопасности, а с другой стороны, позволяет практически мгновенно осуществить проверку из базы данных. То есть, набирая свой индивидуальный код на клавиатуре системы (или, как вариант, используя карту доступа), человек, перед тем как пройти верификацию по форме кисти руки, заранее «сообщает» биометрическому считывателю, с каким именно шаблоном сравнивать полученные данные. Таким образом, время верификации по форме кисти руки не превышает 1 с, а общее время идентификации в системе с учетом набора кода или использования электронной карты составляет 1 – 5 с.

Как и многие другие биометрические системы доступа, современные системы аутентификации по форме кисти руки (например, HandKey-II) позволяют регулировать идентификационный порог верификации формы кисти руки, что позволяет настраивать каждый отдельно взятый считыватель в соответствии с необходимым уровнем безопасности. При высоком уровне идентификационного порога неизбежно снижается скорость считывания и распознавания, а при низком – возрастает вероятность ошибок FRR («ложный отказ») и ошибок FAR («ложный допуск»).

Для обеспечения максимального уровня безопасности биометрическая система доступа может быть настроена на максимальный уровень идентификационного порога, при котором, например, у системы HandKey-II ошибка FRR составит 0,001 %, а FAR – всего лишь 0,00001 % (см. табл. 3.2).

Учитывая то, что процесс верификации формы руки субъекта сопровождается предварительным вводом индивидуального кода, ошибка «ложный допуск» полностью исключена.

Системы аутентификации по форме кисти руки просты и удобны в эксплуатации. К недостаткам следует отнести громоздкость считывателей и меньшую, чем, например, у считывателей радужной оболочки глаза, точность. Области применения – аутентификация посетителей в офисах, производственных помещениях, т.е. в местах, где из-за грязи затруднено применение сканеров отпечатков пальцев.

Особенности голоса. Использование технологии распознавания человека по голосу основано на анализе таких характеристик голоса, как тембр, спектр сигнала, акцент, интонация, сила звука, скорость речи, вибрации в гортани, носовые звуки и т.д.

В зависимости от того, необходима ли идентификация (узнавание) или аутентификация (подтверждение) личности, применяются различные методы распознавания.

Основная техническая проблема при распознавании голоса – зашумленность сигнала.

Характеристики некоторых биометрических систем голосовой аутентификации приведены в табл. 3.2.

Достоинством таких систем является низкая цена оборудования (причем необходимое аппаратное обеспечение входит в стандартную комплектацию современных компьютеров). Цена подобных систем формируется, в основном, стоимостью специализированного программного обеспечения.

Недостатки – малая скорость работы, более низкая надежность по сравнению с большинством биометрических методов. На результатах проверки может сказываться небрежность, физическое и эмоциональное состояние человека, болезнь и тому подобное.

Особенности почерка. Методы аутентификации по особенностям почерка делятся на две группы: анализ только изображения

(определение содержания написанного) и анализ изображения вместе с анализом динамики письма (аутентификация написавшего субъекта).

При анализе особенностей динамики письма сбор информации может происходить двумя способами. Во-первых, может использоваться перо со средствами восприятия силы его нажима на поверхность. Во-вторых, информация может быть получена при использовании чувствительной пластины со средствами восприятия положения точки на поверхности пластины. При появлении на поверхности написанных от руки символов регистрируются одновременно динамические усилия, воздействующие на кончик узла при письме, и положение наносимых обозначений относительно точки отсчета (рис. 3.24,а). Далее могут анализироваться такие динамические характеристики письма, как скорость, ускорение, порядок штрихов и т.д.

На рис. 3.24,б показан внешний вид системы распознавания почерка.

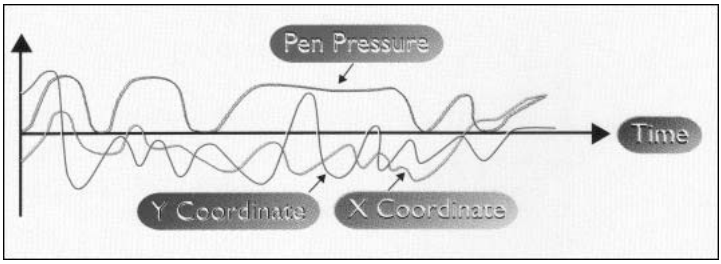
Табл. 3.2 содержит данные о некоторых биометрических системах аутентификации человека по почерку. Например, система, разработанная фирмой *IBM*, имеет три пьезоэлектрических датчика: один измеряет давление вдоль оси пера, два других – ускорение. За 12,5 с выполняется около 1000 измерений параметров.

В некоторых системах (например, *SmartPen* фирмы *IMEC)* ручка, которой осуществляется написание символов, беспроводная, в нее вмонтирован радиопередатчик с криптографической защитой.

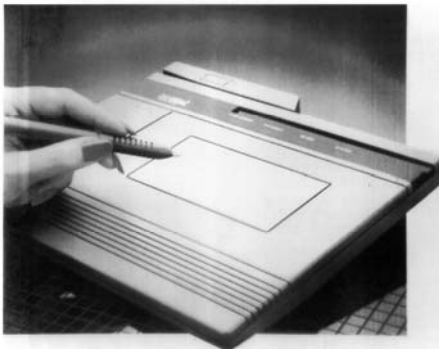
Известны биометрические системы, анализирующие до 42 статических и динамических параметров подписи.

Системы аутентификации по *почерку* имеют относительно невысокую стоимость. Недостатком таких систем является то, что на результатах распознавания может сказываться физическое и эмоциональное состояние человека. Системы имеют невысокую скорость работы.

Области применения этих БС – удостоверение подписей и подтверждение личности субъектов.



а)



б)

Рис. 3.24. Аутентификация по особенностям почерка

Динамические характеристики работы на клавиатуре. Рассматриваемая биометрическая технология основана на уникальности динамических характеристик («клавиатурного почерка») каждого человека.

В системах аутентификации по динамическим характеристикам измеряются промежутки времени между нажатиями клавиш, длительности их удержания и взаимного перекрытия.

Приближенная оценка точностных характеристик для данной биометрической технологии составляет соответственно FRR=9 %, FAR=8 %.

Недостаток биометрической технологии лежит в юридической области — при использовании программного обеспечения, анализирующего клавиатурный почерк, возможен скрытый контроль над сотрудниками (наблюдение за активностью их работы на компьютере). Другой недостаток – система может быть эффективно использована только лицами, обладающими устойчивым клавиатурным почерком и имеющими достаточно высокую скорость ввода.

Область применения – системы управления доступом к компьютерам и терминалам.

Особенности лица. Наиболее распространенный метод аутентификации лиц основан на так называемых картах линий одинаковой интенсивности. Эти карты состоят из линий, соединяющих элементы изображения с равным уровнем яркости (интенсивности отраженного света). Аутентификация человека выполняется путем сравнения формы линий одинаковой интенсивности. Метод имеет ряд достоинств: легко реализуется программными и аппаратными средствами, позволяет отражать в описании трехмерную структуру лица, обеспечивает высокую точность распознавания личности, даже если человек в очках или с бородой.

Применяется метод аутентификации человеческого лица по профилю, извлеченному из трехмерных данных изображения лица. Точность распознавания в данном методе слабо зависит от расстояния между наблюдаемым объектом (лицом) и камерой, а также от угла поворота головы.

Например, система *FaceIt PC* корпорации *Visionics Corp.* сканирует изображение лица в режиме реального времени, что увеличивает стоимость оборудования (требуется плата захвата видеоизображения и предъявляются повышенные требования к производительности компьютера). Система способна анализировать дви-

жущиеся лица, может выделять лицо в группе людей. Утверждается, что предусмотрена защита от обмана системы посредством предъявления фотографии. Время идентификации в режиме «движущегося изображения» составляет 0,1-0,2 с, а в режиме «статического изображения» – 3 с. Точностные характеристики для этой биометрической технологии: FRR=1 %, FAR=1 %.

Системы аутентификации, анализирующие особенности *лица*, отвечают практически всем требованиям, предъявляемым к биометрическим системам. Такие системы просты и удобны в использовании, имеют приемлемую скорость работы, хорошо воспринимаются пользователями, дешевы. Недостатки – возможность ввести систему в заблуждение, сильная зависимость точности распознавания от освещенности.

Области применения – криминалистика, сфера компьютерной безопасности.

Далее рассмотрим некоторые биометрические методы, которые находятся на стадии исследований и разработки. В настоящий момент надежность и практичность этих технологий пока не доказана. Их применение в системах КУД возможно в будущем.

Термографическая карта лица. Метод лицевой термографии базируется на результатах исследований, показавших, что вены и артерии лица каждого человека создают уникальную температурную карту. Специальная инфракрасная камера сканирует фиксированные зоны лица. Результат сканирования – термограмма – является уникальной характеристикой человека. Даже у однояйцовых близнецов термографическая картина различается. На точность системы не влияет ни высокая температура тела, ни охлаждение кожи лица в морозную погоду, ни естественное старение организма человека. Термограмма сохраняется после пластической операции, не зависит от освещенности (можно проводить идентификацию даже в темноте).

Рисунок вен за запястье. Рисунок сухожилий и сосудов на запястье человека индивидуален. На этом основано устройство аутентификации, сканирующее поверхность запястья с помощью инфракрасного излучения.

Преимущество предлагаемой технологии – невозможность случайного или умышленного повреждения рисунка сосудов запястья, в отличие, например, от рисунка отпечатков пальцев.

Форма уха. Результаты исследований, опубликованные в Европе, США и Японии, показывают, что уши людей сильно различаются по морфологическим и анатомическим признакам. Параметры ушей в целом формируются в возрасте 16–17 лет. Несмотря на то, что уши немного изменяются и далее на протяжении всей жизни человека, для практических приложений этим изменением можно пренебречь.

Если сравнивать средства биометрической аутентификации по их использованию в системах КУД, то можно воспользоваться экспертной оценкой, сделанной в 2007 г. организацией Internation Biometric Groop. Соответствующие данные (объем рынка продаж систем, использующих различные методы аутентификации) представлены в табл. 3.3.

Таблица 3.3. Сравнительные характеристики рынка продаж систем биометрической аутентификации (2007 г.)

Система биометрической аутентификации	**Объем рынка, %**
Отпечатки пальцев	48
Особенности лица	12
Форма кисти руки	11
Радужная оболочка глаза	9
Голос	6
Почерк	2
Прикладное ПО	12

Анализ данных, приведенных в табл. 3.3, показывает, что наибольшее распространение получила система биометрической аутентификации, использующая отпечатки пальцев (48 %). Объемы продаж систем, анализирующих особенности лица человека, систем, использующих данные о форме кисти руки, сравнимы с затратами на прикладное программное обеспечение, используемое в различных системах биометрической аутентификации. Наименьшее распространение получили системы, анализирующие почерк человека, что объясняется наличием существенных недостатков у данного метода аутентификации.

В заключении рассмотрения методов биометрической аутентификации необходимо отметить увеличивающуюся динамику использования этих средств КУД, о чем говорит экспертная оценка фактических затрат компаний США в млн.долларов по годам до 2007 г. включительно (рис. 3.25).

3.4. Считыватели как элементы системы контроля и управления доступом

Ввод идентификационной информации в системы КУД обеспечивается считывателями.

Согласно ГОСТу, для считывателей как для аппаратных элементов систем КУД должны быть определены:

- устойчивость к взлому;
- устойчивость к манипулированию;
- устойчивость к наблюдению (для парольных);
- устойчивость к электромагнитным помехам;
- требования к надежности;

•требования по устойчивости к внешним факторам (климатическим, механическим);

•требования к электропитанию;

•требования к безопасности эксплуатации и к конструкции.

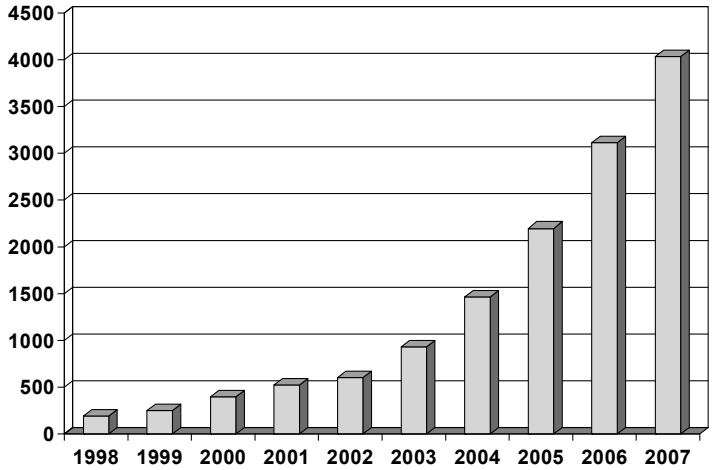


Рис. 3.25. Объем продаж в США биометрических систем КУД до 2007 г.

Одна из проблем, с которой приходится сталкиваться при аутентификации пользователя – так называемый «проход под принуждением», когда злоумышленник совершает насильственные действия над пользователем с целью проникновения через преграждающее устройство. Некоторые считыватели (как парольной, так и жетонной и биометрической технологий) позволяют пользователю ввести так называемый «пароль под принуждением». Система в этом случае пропустит пользователя и злоумышленника, а на пульт охраны подаст сигнал «тихой тревоги».

Иногда необходимо контролировать так называемый повторный проход пользователя в зону (“вход без выхода”). Такое воз-

можно в случае, например, когда сотрудник прошел на объект и каким-то способом передал свой идентификатор другому человеку, находящемуся снаружи. Соответствующим образом отконфигурированная система (поддерживающая технологию antipassback) может обнаружить факт того, что сотрудник, не покинув объект, снова проходит на него. Для реализации технологии antipassback необходима идентификация пользователей как при входе в зону, так и при выходе из нее, что требует двойного количества считывателей.

Частично контролировать повторный проход без применения двойного количества считывателей можно, ограничивая время между двумя последовательными проходами одного сотрудника.

3.5. Исполнительные устройства систем контроля и управления доступом

Для того чтобы пересечь точку доступа, контролируемую системой КУД, субъект доступа должен предъявить идентификатор, подтверждающий права доступа. Специальное устройство (считыватель) считывает идентификационную информацию, передает ее в контроллер, который, обрабатывая ее, выдает управляющую информацию на исполнительные устройства. Исполнительные устройства устанавливаются в проходных (точках доступа) и при определенных условиях обеспечивают беспрепятственный доступ субъектам доступа на объект.

Исходя из возможных видов субъектов доступа (персонал, транспорт) различают две группы исполнительных устройств: для прохода людей; для пропуска транспорта.

Исполнительные устройства для обеспечения прохода персонала

К исполнительным устройствам систем КУД, предназначенных для обеспечения прохода персонала (первая группа), относят: замки, двери, шлюзы и турникеты.

Замки могут быть классифицированы по следующим направлениям:

- по типу крепления: врезные, накладные, навесные;
- по расположению: обычный, распорный, типа «балка»;
- по времени действия: «дневные», «ночные»;
- по принципу действия: механические (цилиндровые, дисковые), электрические (электромеханические – соленоидные, моторные, курковые; электромагнитные – электромагнитные защелки);
- по режиму работы: нормально открытый, нормально закрытый.

Наиболее применимыми в системах КУД являются электрические замки. Их рекомендуется использовать в качестве основного запирающего устройства в дневное время. Эти замки в отличие от механических открываются дистанционно по электрическому сигналу и используются совместно с домофонами, кодовыми панелями, считывателями карточек различных типов.

Электрические замки делятся на два класса: электромагнитные и электромеханические.

Электромагнитные замки представляют собой корпус с электромагнитом и ответную металлическую пластину. Пластина крепится на дверном полотне, а сам замок – на коробке двери. Электромагнитный замок удерживает дверь в закрытом состоянии за счет усилия мощного электромагнита. При обесточивании замка дверь остается открытой, поэтому для обеспечения работы в условиях пропадания питания необходимо применять устройства бесперебойного питания.

Электромеханический замок имеет механический ригель (засов), удерживающий дверь в закрытом состоянии, а управление этим ригелем осуществляется относительно маломощным соленоидом. При закрытии двери взводящий ригель замка взводит имеющуюся в замке пружину, при этом рабочий ригель входит в ответную часть замка и удерживает дверь в закрытом состоянии. При подаче напряжения соленоид сбрасывает фиксатор пружины, и рабочий ригель под действием пружины втягивается в замок – дверь может быть открыта. После того как дверь будет открыта, а затем закрыта, она вновь окажется в запертом состоянии. Предусматривается режим, исключающий автоматическое запирание замков и случайное закрывание двери.

В соленоидных электрозамках ригель приводится в движение усилием электромагнита. Оборудованная таким замком дверь может быть открыта только в период действия управляющего сигнала. После снятия этого сигнала закрытая дверь останется запертой независимо от того, открывалась ли она. Существуют также другие разновидности электромеханических замков: электромоторные (ригель приводится в движение электромотором с редуктором), с ручным приводом ригеля (ригель приводится в движение поворотом ручки, а электромагнит разблокирует механизм привода). Электромеханические замки могут быть накладного и врезного типа.

Электрозащелки представляют собой ответную часть замка и используются совместно с обычным механическим замком. При подаче управляющего напряжения разблокируется фиксатор электрозащелки и дверь может быть открыта при выдвинутом положении ригеля механического замка. При этом используемый механический замок не должен открываться снаружи поворотом ручки. При наличии ручки с внутренней стороны двери она может быть открыта изнутри поворотом ручки без подачи управляющего напряжения на защелку.

Специальные модели соленоидных замков и электрозащелок предназначены для оборудования аварийных выходов. Такие замки открываются при пропадании питающего напряжения.

При выборе модели замка необходимо учитывать, какие помещения и для каких целей предполагается оборудовать. При этом необходимо учитывать: массу, конструкцию, материал двери, тре-

буемую интенсивность использования, различные функциональные особенности системы, включающей замок.

Внешний вид образцов механических замков показан на рис. 3.26.

а) **б)**

Рис. 3.26. Образцы механических врезных (а) и накладного (б) замков

Внешний вид образцов электрических замков показан на рис. 3.27.

а) **б)**

Рис.3.27. Образцы элекромагнитного (а) и электромеханического (б) замков

В некоторых случаях замки комбинируются с другими средствами аутентификации: по отпечатку пальца (рис. 3.22,г) или по карточке (рис. 3.28).

Рис. 3.28 Комбинированный замок (с карточной системой)

Двери могут быть классифицированы по следующим направлениям:

- материал – *металлические, деревянные, пластиковые, стеклянные;*
- сочетание с определенным типом замка*;*
- наличие кабелепровода для подключения электрических замков*;*
- требования к коробке двери (надежность определяется всей конструкцией)*;*
- наличие изнутри механизма открытия (обязательное требование при наличии системы КУД)*;*
- использование доводчиков.

Следует отметить, что любая дверь как исполнительное устройство системы КУД должна оснащаться доводчиком (закрывате-

лем), который служит для принудительного закрывания двери и обеспечивает надежную работу электрических замков. Для дверей разного размера можно подобрать соответствующий доводчик. Модели также отличаются конструктивным исполнением, дизайном, рядом дополнительных функций: фиксация двери в положении "открыто", регулировка скорости закрывания двери, ускорение в завершающей фазе закрывания – "прихлоп", и так далее.

Шлюзы – технические средства (исполнительные устройства), обеспечивающие санкционированный доступ на объект при взаимоувязанном последовательном пересечении двух точек доступа в пределах одной проходной (рис. 3.29).

Рис. 3.29. Образцы шлюзов

Структура шлюза: дверь; закрытое ограниченное пространство (тамбур); дверь. В некоторых случаях шлюз называют тамбуром безопасности.

Порядок работы шлюза: субъект предъявляет идентификатор перед первой дверью (например, проксимити-карту); при подтверждении полномочий открывается первая дверь: субъект входит в тамбур; первая дверь закрывается; субъект предъявляет второй идентификатор (например, вводит ПИН-код или используется биометрическая аутентификация); при наличии полномочий открывается вторая дверь; субъект проходит на объект.

Особенностью порядка работы шлюза является выполнение требования реализации открытия только одной двери.

Шлюзы отличаются конструктивным исполнением, использованием различных механизмов и устройств аутентификации, а также наличием дополнительного оборудования, как правило, устанавливаемого в тамбуре, и пропускной способностью. Таким дополнительным оборудованием могут быть детектор металла; детектор ядерных материалов; рентгеновский аппарат; система взвешивания. Пропускная способность шлюза зависит от его конструкции, используемых средств аутентификации и наличия определенного дополнительного оборудования и, чаще всего, не превышает 5…10 человек в минуту.

Образцы конструкций шлюзов показаны на рис. 3.29.

Шлюзы достаточно часто встречаются в банках, хранилищах материальных ценностей и на некоторых производствах.

Турникеты – исполнительное устройство, которое в управляемом системой КУД режиме открывает проход субъекту, который предъявил идентификатор и получил подтверждение своих полномочий. Образцы конструкций турникетов показаны на рис. 3.30.

Действующий турникет разделяет поток людей по одному, обеспечивая при этом высокую пропускную способность. В режиме однократного прохода через турникет в разрешенном направлении может пройти один человек, после чего турникет автоматически возвращается в закрытое положение.

При необходимости пропуска группы лиц устанавливается режим многократного прохода в нужном направлении, возможен режим свободного прохода. Направление прохода высвечивается на табло. В случае экстренных ситуаций возможна механическая разблокировка турникета. При отключении сетевого питания турникет может перейти на работу от аккумулятора.

а)

б)

г)

в)

д)

Рис. 3.30. Образцы турникетов

Турникеты могут изготавливаться из различных материалов и иметь разную конструкцию (вращающиеся, сдвижные, однонаправленные, двунаправленные). Различают турникеты в полный рост или в половину роста (поясной). Турникеты могут быть оснащены дополнительным оборудованием: счетчик прохода, устройство блокировки (закрыто, открыто), световая индикация состояния, устройство дистанционного управления, считыватели различ-

ного типа, регистрирующие датчики, устройство блокировки прохода двух. Пропускная способность современных турникетов составляет 15, 30, 60 чел./мин.

Рассмотрим особенности наиболее используемых типов турникетов.

Турникет **«Калитка»** выполнен в виде моторизованной или ручной калитки (рис. 3.30,а). Существуют двунаправленные электромеханические калитки с пультом дистанционного управления. Разблокировка калитки может осуществляться от пульта дистанционного управления или от любого типа считывателя (контроллера) системы контроля доступа с релейными выходами.

После прохода человека створка калитки автоматически возвращается в закрытое состояние с помощью встроенного механического позиционирующего устройства и блокируется соленоидом. При пропадании напряжения питания калитка разблокируется, освобождая проход в обоих направлениях.

Турникет **«Трипод»** имеет вращающиеся преграждающие планки и является наиболее популярным типом турникета (рис. 3.30,б). Это обусловлено невысокой стоимостью, компактностью, возможностью гармонично вписать в любой интерьер. Такой турникет удобен для случаев, когда необходимо перекрыть проход при минимальных размерах самого турникета. Корпус турникета может вместить электронные модули систем контроля доступа и устройства управления. Для быстрой эвакуации людей в турникетах реализован режим «антипаника», действующий следующим образом: при пропадании питания турникет автоматически разблокируется в обоих направлениях.

Полупрофильный турникет (рис. 3.30,в) имеет большую степень защищенности, чем «трипод», но требует большего пространства для установки. Полупрофильные роторные турникеты обеспечивают более надежное перекрытие прохода, чем турникеты типа «трипод». Турникеты обеспечивают четкую фиксацию в закры-

том положении после прохода человека. Плавный ход, безынерционное вращение и бесшумная работа обеспечиваются электроприводом.

Принцип действия роторного турникета: проходящий толкает преграждающие планки в разрешенном направлении, затем включается электропривод, и после прохода человека происходит автоматический доворот турникета в исходное закрытое положение. Для обеспечения свободного передвижения в любую сторону устанавливается режим свободного прохода.

Полнопрофильные турникеты (рис. 3.30,г) обеспечивают максимальную степень защиты. Они имеют конструкцию в полный рост человека, могут быть выполнены в виде вращающихся брусьев, вращающихся стеклянных створок и тому подобное. Ряд моделей предназначены для установки на улице и обеспечивают контроль доступа на охраняемые территории. Турникет может работать как в автономном режиме и управляться от любого типа считывателя (контроллера) с релейными выходами, так и в режиме управления от ручного пульта.

Полнопрофильные турникеты серии Full-O-Stile фирмы Gunnebo Italdis представляют собой конструкции высотой 2270 мм, которые полностью предотвращают перелезание или перепрыгивание и обеспечивают высокий уровень безопасности. В основном они предназначены для установки вне помещений для организации контролируемого доступа через периметровые ограждения, а модели со стеклянными створками часто используются внутри помещений. Турникет состоит из вращающегося ротора с укрепленными на нем горизонтальными стальными брусьями или стеклянными створками из триплекса толщиной 10 мм, специального механизма контроля с гидравлическим демпфером и неподвижной части. Конструктивно неподвижная часть турникета представляет собой стальной каркас с крышей и стенками из стекла триплекс толщиной 10 мм или вертикальных брусьев.

Турникеты сконструированы таким образом, чтобы обеспечивать проход только одного человека и предотвратить одновременное проникновение двух и более людей.

Положение ротора контролируется замковой системой с магнитными сенсорами, которая управляется через встроенный электронный модуль считывателями карт либо иных идентификаторов или с ручного пульта управления. Изменение направления вращения ротора возможно только после окончания заданного цикла прохода.

Полнопрофильные турникеты могут быть одно- и двухпроходными. В двухпроходных моделях в едином конструктиве выполнены два прохода, используемые обычно для входа и выхода. Как и другие модели турникетов, полнопрофильные турникеты могут быть не только электромеханическими с возможностью управления от систем контроля доступа или ручных пультов, но и чисто механическими. Для обеспечения безопасного прохода в случае пропадания сетевого напряжения турникет автоматически разблокируется. При необходимости турникет может быть также установлен в режим блокировки или разблокировки в одном направлении и блокировки в другом направлении для двухпроходных турникетов.

Скоростные турникеты обеспечивают наибольшую пропускную способность (рис. 3.30,д). Они могут иметь конструкцию как с дверцами небольшой высоты, так и высокими створками.

Турникеты этого типа могут работать в двух режимах: нормально-открытом или нормально-закрытом.

В нормально-открытом режиме створки турникета постоянно открыты и закрываются только при попытке несанкционированного прохода. Этот режим обеспечивает высокую пропускную способность.

В нормально-закрытом режиме створки турникета закрыты, и открываются только после авторизации (предъявления пользователем авторизованной карты или другого идентификатора).

В корпус турникета встроены инфракрасные датчики, фиксирующие попытки неавторизованного прохода, а также попытку пройти вслед за авторизованным пользователем. Верхняя крышка турникета может быть дополнительно оборудована датчиками давления для повышения уровня контроля безопасности.

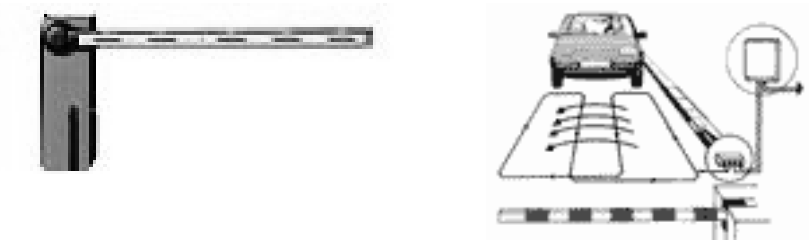
Раздвижные створки турникета расположены в середине корпуса и изготовлены из термоформованного полиуретана, а выступающие из стойки ограничивающие панели – из тонированного стекла толщиной 12 мм. Стандартная высота створок и заграждающих панелей от уровня пола – 1200 мм. При необходимости можно использовать створки высотой 1700 мм.

Исполнительные устройства для обеспечения пропуска транспорта

К исполнительным устройствам систем КУД, предназначенных для обеспечения пропуска транспорта (вторая группа), относят шлагбаумы и ворота.

Шлагбаумы используются для оперативного управления потоками автотранспорта, регулирования въезда/выезда на автомобильные парковки, территории предприятий и организаций, торговых центров и так далее. Шлагбаумы могут быть неавтоматические (ручное управление) и автоматические, управляемые системой контроля доступа или самим субъектом (рис. 3.31,а и 3.31,б соответственно).

Автоматический шлагбаум состоит из стойки с силовым механизмом, стрелы и электронного блока управления. По принципу действия шлагбаумы могут быть электромеханическими и гидравлическими. Длина стрелы шлагбаума может достигать нескольких метров, для перекрытия широких проездов можно использовать два шлагбаума, установленные навстречу друг другу и работающие синхронно.



а) **б)**

Рис. 3.31. Образцы шлагбаумов

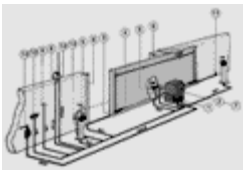
Важным параметром шлагбаума является время открывания / закрывания. В некоторых моделях предусмотрена установка на стреле элементов световой сигнализации и бордюра безопасности – резинового профиля в нижней части стрелы, чувствительного к соприкосновению с препятствием. Управление шлагбаумом может осуществляться дистанционно от кнопки, подключенного считывателя карточек, кодовой клавиатуры, с помощью миниатюрного радиобрелка.

К блоку управления могут подключаться различные элементы обеспечения безопасности проезда: фотоэлементы, индукционные металлодетекторы для фиксации факта присутствия автомобиля в заданной зоне проезжей части.

Ворота могут быть разной конструкции и оснащаться различными механизмами автоматики. Образцы ворот представлены на рис.3.32.

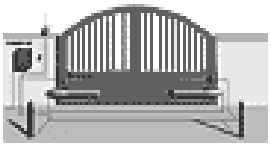
Автоматика для ворот предназначена для обеспечения комфортного и безопасного управления воротами как бытового, так и промышленного назначения. Механический привод, осуществляющий открывание и закрывание ворот, соответствует типу ворот: откатные (рис. 3.32,а), подъемно-поворотные (рис. 3.32,б), распаш-

ные (рис. 3.32,в). Кроме того, при выборе привода необходимо учитывать размер и массу ворот, а также интенсивность нагрузки.



а)

б)



в)

Рис. 3.32. Образцы ворот

Все приводы ворот оснащаются элементами безопасности (фотоэлементы, датчики и т.п.), исключающими возможность повреждения машины, находящейся в створе ворот.

Кроме того, все комплекты автоматизации ворот снабжаются удобными устройствами управления, которые могут быть дистанционными с использованием инфракрасных или радиопередающих брелков-ключей или автоматическими, управляемыми системой КУД.

3.6. Классификация средств и систем КУД по устойчивости к несанкционированному доступу

Средства КУД классифицируют по устойчивости к несанкционированному доступу, которая определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости: нормальной, повышенной, высокой.

Устройства преграждающие управляемые и устройства ввода идентификационных признаков классифицируют по устойчивости к разрушающим воздействиям: по устойчивости к взлому, пуле стойкости и устойчивости к взрыву.

По устойчивости к неразрушающим воздействиям средства и системы КУД в зависимости от их функционального назначения классифицируют по следующим показателям:

•устойчивости к вскрытию для исполнительных устройств (замков и запорных механизмов);

•устойчивости к манипулированию;

•устойчивости к наблюдению – для считывателей кода (клавиатуры, кодовые переключатели и т.п.);

•устойчивости к копированию (для идентификаторов);

•устойчивости защиты средств вычислительной техники системы КУД от несанкционированного доступа к информации.

Классификация по устойчивости к вскрытию, манипулированию, наблюдению, копированию должна быть указана в стандартах и других нормативных документах на средства КУД конкретного типа.

Класс защищенности от несанкционированного доступа к информации должен быть указан в нормативных документах на средства или системы КУД конкретного типа.

Классификация систем КУД по защищенности от несанкционированного доступа к информации проводят в соответствии с Руководящим документом Гостехкомиссии России [3.6]. При этом система КУД рассматривается как автоматизированная система [3.1]. В ней выделяются три подсистемы (управления доступом, регистрации и учета, обеспечения целостности). Для каждой из подсистем сформулированы требования исходя из трех групп (третья группа имеет минимальные требования; первая группа – максимальные требования) и пяти классов (3Б, 3А, 2Б, 1Г, 1В).

Классификацию средств КУД по устойчивости от несанкционированного доступа к информации проводят в соответствии с Руководящим документом Гостехкомиссии России [3.4]. При этом средства КУД рассматриваются как средства вычислительной тех-

ники [3.1]. Для них выделены определенные характеристики (например, принцип контроля доступа – дискреционный или мандатный, наличие очистки памяти, изоляции модулей, идентификации и аутентификации и т.д.), для которых сформулированы определенные требования исходя из трех классов защищенности (шестой – с минимальными требованиями, пятый, четвертый – максимальные требования).

3.7. Сравнительные характеристики систем контроля и управления доступом

Рассмотрев основные методы и средства аутентификации, особенности компонентов систем КУД, можно сравнить уровень эффективности таких систем при использовании различных средств аутентификации. На рис. 3.33 перечислены методы аутентификации, и каждому методу сопоставлен уровень надежности систем противостояния действиям потенциальных нарушителей в виде длины утолщенной линии.

Наименее стойкие воздействию нарушителей являются системы КУД (наименьшая эффективность), использующие электронные кодовые замки. Далее идут системы на основе электронных карт и жетонов. Более высокой эффективностью будут обладать системы, комбинирующие использование кодов и карт или жетонов (К+К). Увеличение эффективности систем достигается использованием биометрических методов. Причем имеется определенная иерархия этих методов (наиболее эффективным является использование радужной оболочки глаза; наименее – почерк). Максимальная эффективность достигается при комбинации кода, карт и биометрии (К+К+Б).

Для оценки уровня использования методов и средств КУД на конкретном объекте можно воспользоваться перечнем показателей, приведенных в ГОСТе [3.1]:

- проход на территорию объекта – только через систему пропускного контроля;
- контроль как входа, так и выхода;
- проверка как персонала, так и транспорта;
- обеспечение контроля материалов;
- пропускная способность – соответствие нагрузки в часы пик;
- наличие средств вторичной проверки;
- блокировка допуска до окончания контроля;
- использование средств контроля (индивидуальных, специальных знаний, биометрии);
- взаимодействие с центральной станцией тревожного оповещения;
- возможность участия вооруженной охраны (защита охранников).

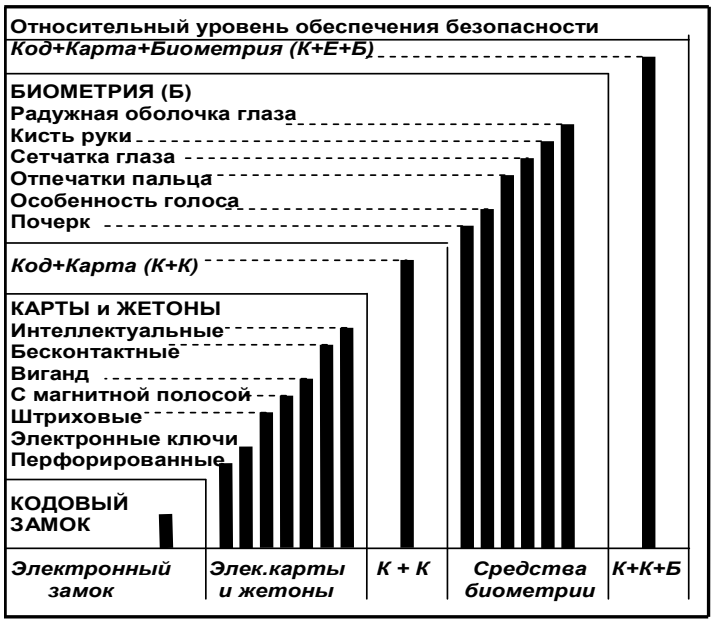


Рис. 3.33. Сравнительные характеристики систем КУД

Вопросы для самоконтроля

1. Какие основные задачи решает подсистема контроля и управления доступом (СКУД)?
2. Опишите модель управления доступом.
3. Что такое идентификация и аутентификация?
4. Какие предъявляются требования к аппаратурным элементам СКУД?
5. Какие существуют методы и средства аутентификации (парольная, жетонная, удостоверения, штриховой код)?
6. Какие существуют методы и средства аутентификации с помощью карт и ключей (карты с магнитной полосой, проксимити-карты, смарт-карты, электронные ключи и др.)?
7. Какие существуют основные методы биометрической аутентификации (рисунок радужной оболочки глаза, расположение кровеносных сосудов, сетчатки глаза, папиллярные узоры, форма кисти руки, рисунок вен на запястье, особенности лица, термографическая карта лица, форма уха, особенности голоса, особенности почерка, динамические характеристики работы на клавиатуре)?
8. Какова роль считывателей, управляющих и преграждающих устройств в системах контроля и управления доступом?
9. Назовите способы защиты кодонаборников от подсматривания.
10. Каковы принципиальные недостатки систем аутентификации, основанных на измерении биологических характеристик человека?
11. Каковы принципиальные достоинства биометрических систем аутентификации?
12. Приведите примеры преграждающих устройств.

4. ПОДСИСТЕМА ТЕЛЕВИЗИОННОГО НАБЛЮДЕНИЯ

Подсистема (далее – система) телевизионного наблюдения (СТН) как составляющая СФЗ объекта применяется для оценки ситуации на объекте. Она используется не только для наблюдения за обстановкой на объекте, но и для контроля доступа, и для обнаружения несанкционированного проникновения на объект, т.е. выполняет функцию обнаружения.

В данном разделе рассматриваются основные вопросы, связанные с выбором и построением систем телевизионного наблюдения: выполняемые задачи СТН; выбор компонентов СТН (телекамеры и объективы, устройства отображения, обработки и хранения информации); особенности применения [4.1, 4.2].

4.1. Задачи и характерные особенности современных систем телевизионного наблюдения

Основной задачей системы телевизионного наблюдения является наглядное представление видеоинформации об оперативной обстановке на контролируемом объекте. Это позволяет в реальном масштабе времени получать наиболее полную и достоверную информацию о ситуации на охраняемом объекте.

Применение СТН не исключает возможности установки средств охранно-пожарной сигнализации или средств контроля доступа; наоборот, их интеграция ведет к достижению максимального уровня безопасности объекта. На сегодняшний день СТН является неотъемлемой частью СФЗ любого объекта (будь то маленькая коммерческая организация или крупный ядерный центр). Грамотное использование возможностей современных систем телевизионного наблюдения позволяет поднять уровень безопасности объектов на качественно новую ступень. Системы телевизионного

наблюдения позволяют сократить количество сотрудников служб охраны и безопасности и существенно снизить степень их риска.

Характерные особенности интеграции СТН. Использование в современных СТН новейших достижений в области электроники и компьютерной техники резко расширило возможности этого вида технических средств физической защиты. Небольшие габаритные размеры (миниатюрные компоненты – ПЗС-матрицы и микропроцессоры) и использование цифровых методов обработки видеосигнала позволили создавать системы наблюдения с широкими функциями, включая возможность применения этих систем в качестве средств охранной сигнализации (видеодетекторы движения). По ряду функций СТН и системы охранной сигнализации дублируют друг друга. Так как оборудование СТН значительно дороже оборудования охранной сигнализации, то прибегать к использованию первых целесообразно при решении следующих задач:

- документирование материалов об оперативной обстановке для последующего анализа (видеозапись);
- использование видеоизображения для идентификации личности;
- наблюдение за большой территорией объекта ограниченным количеством сотрудников службы безопасности;
- применение в качестве детекторов движения.

Особенности конкретного вида оборудования определяются рядом технических требований, которые накладываются на создаваемую СТН. И дорогие, и дешевые компоненты СТН обладают характеристиками, необходимыми для передачи и обработки видеоизображения. Однако при создании СТН на больших объектах, при наращивании возможностей системы резко возрастают требования к качеству и надежности системы в целом. Качество и надежность любой сложной системы зависят от входящих в ее состав компонентов. Возможны ситуации, когда высококачественное обо-

рудование не может реализовать свои показатели из-за низкого качества устройств, входящих в состав системы (даже из-за соединительных проводов). Если же речь идет о СТН, призванной обеспечивать контроль за ситуацией на особо важных объектах, то требования к качеству и надежности входящих в состав комплекса компонентов еще более ужесточаются. Обеспечение высокого качества работы всей системы заключается в выборе согласованных и качественных компонентов. Как правило, подобрать все необходимое оборудование у одного производителя невозможно. В такой ситуации при создании интегрированной системы приходится «собирать» ее из разнородных компонентов, различных по качеству и не всегда полноценно совместимых, что может привести к ухудшению характеристик всей СТН в целом.

Устройства (компоненты) СТН. Основные устройства СТН можно разделить по выполняемым функциям следующим образом:

- устройства получения видеоинформации: телекамеры и их неотъемлемая часть – объективы;
- устройства отображения видеоинформации: видеомониторы, видеопринтеры, мониторы персональных компьютеров (ПК);
- средства передачи видеосигнала;
- устройства обработки видеосигнала: коммутаторы, мультиплексоры, квадраторы, видеодетекторы движения, ПК;
- устройства регистрации и хранения видеоинформации: специальные видеомагнитофоны; системы цифровой записи;
- устройства удаленного управления: системные контроллеры; пульты управления (ПУП) телекамерами, ПУП поворотными устройствами и коммутаторами; ПК.

Также имеется ряд дополнительных вспомогательных устройств, к которым можно отнести:

- блоки питания;
- светофильтры;

- дежурное освещение;
- кожухи и устройства крепления для телекамер и средств освещения;
- муляжи телекамер.

4.2. Характеристики объектов, на которых создаются системы телевизионного наблюдения

Современные СТН используются в широком диапазоне окружающих условий (по сравнению с другими подсистемами СФЗ, например, системой пожарной сигнализации). В самых жестких условиях работают телекамеры (ТК) и вспомогательные устройства для них. Когда телекамера установлена в помещении (например, в офисе), то в этом случае температура не опускается ниже 10 °С, и телекамера никогда не окажется под прямым дождем. Если же ТК устанавливается на улице, где колебания температуры и влажности очень большие (например, в центральной части России колебания температуры возможны от -40 до +50 °С и высокая (100 %) влажность), существует несколько способов компенсации условий окружающей среды. Например, для телекамер применяются термозащитные кожухи, или существуют уже телекамеры, адаптированные для работы при низких и высоких значениях температуры.

Работа ТК напрямую связана с освещенностью на объекте. Есть объекты, где освещенность круглые сутки постоянна (например, торговый зал магазина, где даже ночью поддерживается дежурное освещение). Но если ТК предназначены для работы на улице (на участке охраняемого периметра), то диапазон колебаний освещенности достигает 10^9. Диапазоны и примеры типичных уровней освещенности на объекте приведены в табл. 4.1.

Таблица 4.1. Значения освещенностей на объекте

Условия применения	***Освещенность, лк***
Освещенная автомагистраль ночью	10
Помещение	
Склад	20-70
Пожарная лестница	30-75
Коридор или лестница	75-200
Офис	200-500
Торговый зал	300-500
Улица	
Ясный солнечный день	10^5
Облачный/пасмурный день	$10^2 – 10^4$
Сумерки	1 – 10
Ночь (полная луна)	1 – 0,1
Ясная звездная ночь	$10^{-2} – 10^{-3}$
Пасмурная звездная ночь	$10^{-3} – 10^{-4}$

Большие колебания освещенности приводят к недопустимым изменениям уровня выходного видеосигнала телевизионной камеры (например, при недостаточной или чрезмерной освещенности мы ничего не увидим на экране монитора). Чтобы работать в широком диапазоне освещенности, необходимо выбирать телекамеру с устройствами стабилизации видеосигнала.

Создавая СТН, следует изучить характеристики объекта. Это необходимо для правильного выбора средств наблюдения. При расчете освещенности на объекте понадобится оценить коэффициент отражения объекта наблюдения. Значения коэффициентов отражения реальных объектов приведены в табл. 4.2.

Средства СТН могут применяться для работы в статическом и динамическом режиме. Можно установить телекамеру в хранилище ценностей, которая будет «смотреть» только на один сейф. Либо установить ТК в торговом зале, которая будет просматривать в

режиме сканирования весь зал, для этого применяются специальные поворотные устройства. При использовании телекамеры в динамическом режиме накладываются ограничения на скорость сканирования. Если установить ТК для наблюдения за движением автомашин, то здесь уже понадобятся телекамеры, способные отслеживать динамичные объекты (в данном случае автомашины).

Таблица 4.2. Характеристики освещенности объектов

Объект	***Коэффициент отражения, %***
Белая одежда	80-90
Снег	65-85
Белая краска	55-75
Серая одежда	20-60
Автостоянка	40
Лицо человека	15-25
Трава/деревья	20
Вспаханная земля	7

При размещении ТК в помещении необходимо подумать и о том, как установленные телекамеры впишутся в интерьер помещения. Надо определить, где телекамеры необходимо установить скрыто, а где в декоративных кожухах. В любом случае следует стремиться к тому, чтобы установленные телекамеры не создавали дискомфортной обстановки на объекте для сотрудников и посетителей.

В связи с накладываемыми ограничениями и сложными условиями работы возрастают требования к выбору устройств проектируемой СТН.

4.3. Телекамеры и объективы

Основными и центральными элементами всех СТН являются телекамеры. От выбора ТК зависит качество передаваемой информации. Если необходимо не только наблюдать общую обстановку на объекте, но и проводить идентификацию, то к выбору телекамер следует подходить с большим вниманием. В большинстве случаев нелегко разобраться в многообразии представленных ТК и выбрать именно те телекамеры, которые будут оптимально подходить для выполнения поставленной задачи. Ниже рассмотрены основные технические характеристики телекамер, которые потребуются при построении качественной СТН, а также основные методы их выбора.

Современные телекамеры

Структура. Телевизионная камера – устройство, преобразующее световой поток, отраженный от объекта, в электрические сигналы, используя физические и химические свойства фоточувствительных материалов. Цель ТК – обеспечить быстрое получение надежной видеоинформации. Телевизионная камера содержит следующие основные компоненты (рис. 4.1):

- датчик изображения;
- устройство формирования сигнала;
- устройство синхронизации;
- усилитель видеосигнала;
- схема автоматической регулировки уровня (АРУ) сигнала;
- блок питания (не во всех телекамерах).

Ниже представлены назначение и принципы работы отдельных блоков и узлов телевизионных камер.

Все современные телевизионные камеры строятся на основе использования в качестве чувствительного элемента полупровод-

никовых ПЗС-матриц (ПЗС – прибор с зарядовой связью). Существовали ТК на электронно-лучевых трубках типа «видикон», которые в настоящее время уже не используются. Свет, падающий на ПЗС-матрицу, преобразуется в электрический сигнал, который затем обрабатывается и выводится на монитор. Поверхность ПЗС-матрицы состоит из множества светочувствительных элементов – *пикселей*, которые являются самыми маленькими деталями датчика изображения. Количество пикселей определяет такую характеристику ТК, как *разрешающая способность*. Чем больше пикселей содержит ПЗС-матрица, тем выше четкость и качество получаемого от телекамеры изображения. Количества пикселей по вертикали и горизонтали является характеристикой ПЗС-матрицы, которое должно указываться производителем ТК в ее паспорте.

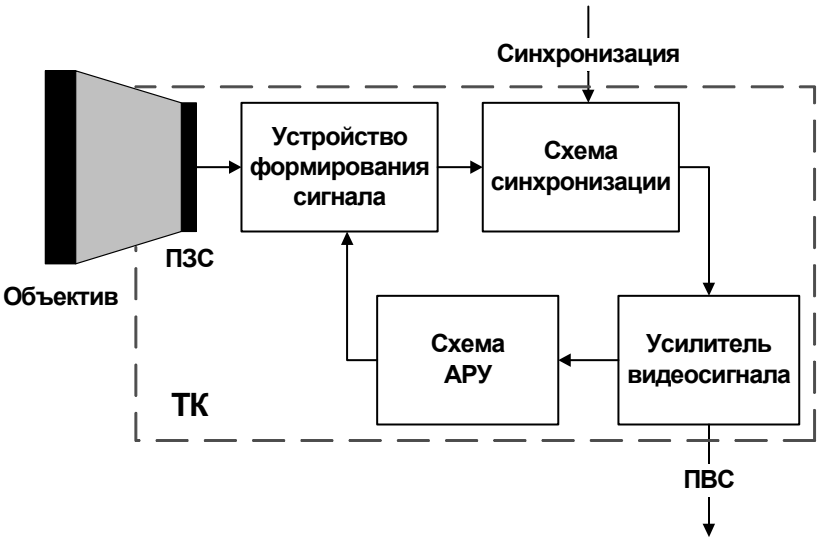


Рис. 4.1. Структурная схема телекамеры

Полный видеосигнал, синхронизирующие импульсы. Для правильного понимания алгоритма образования и передачи видеосиг-

нала необходимо знать состав полного видеосигнала (ПВС), что также целесообразно для правильного понимания необходимости синхронной работы компонентов СТН.

В телевидении используется принцип последовательной во времени передачи изображения – элемента за элементом. Этот принцип лежит в основе происходящего на ПЗС преобразования изображения в электрический сигнал. Оптическое изображение объекта проецируется с помощью объектива на светочувствительную поверхность (ПЗС-матрицу). Величина зарядов, образующихся на каждом пикселе ПЗС-матрицы, пропорциональна яркости отдельных элементов изображения. Последовательно происходит считывание накопленных на ПЗС-матрице зарядов. Считывание происходит одновременно по горизонтали и по вертикали. При считывании слева направо развертывается строка изображения. Заряды считываются последовательно: элемент за элементом и строка за строкой (рис. 4.2). В результате образуется сигнал изображения, несущий информацию об изменении яркости элементов передаваемого изображения. Эффект движения достигается путем передачи достаточного количества неподвижных изображений (кадров) в секунду, представляющих собой отдельные статические фазы движения.

Согласно принятому в России телевизионному стандарту, формирование сигнала изображения производится таким образом, что наиболее темным местам передаваемого изображения соответствует наибольшей величины электрический сигнал. Если принять максимально возможный уровень видеосигнала за 100 %, то окажется, что сигнал изображения будет занимать место между уровнем 15 % (уровень белого) и 75 % (уровень черного).

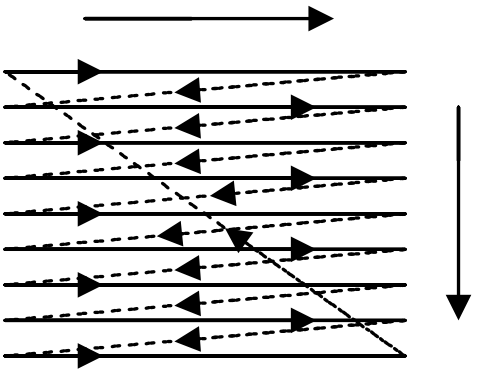


Рис. 4.2. Последовательность считывания строк кадра

Синхронная и синфазная работа считывающих устройств на передающей стороне и развертывающих устройств на приемной стороне обеспечивается с помощью синхронизирующих импульсов, создаваемых схемой синхронизации. В ней вырабатываются также гасящие импульсы, предназначенные для закрывания приемной трубки кинескопа монитора на время обратных ходов развертки по строкам и кадрам (наличие светлых линий на экране кинескопа – следов обратных ходов – мешало бы наблюдению за изображением). Гасящие импульсы вводятся в видеосигнал во время обратного хода луча. Они следуют после передачи каждой строки и кадра и называются соответственно строчными и кадровыми гасящими импульсами [4.1]. Амплитуда гасящего импульса всегда соответствует уровню черного, т.е. занимает 75 % от общего уровня видеосигнала. Синхронизирующий импульс по своему уровню занимает место от 75 до 100 % общего уровня видеосигнала, т.е. располагается в области «чернее черного» [4.3].

В интервалах гасящих импульсов в видеосигнал вводится сигнал синхронизации приемников, состоящий из строчных и кадровых синхронизирующих импульсов. Эти импульсы должны быть такими, чтобы можно было с помощью простых средств отделить

их от сигнала изображения и друг от друга. Уровень синхронизирующих импульсов расположен выше уровня гасящих импульсов. Это позволяет легко отделить синхронизирующие импульсы от сигнала изображения. Чтобы отделить строчные синхронизирующие импульсы от кадровых синхронизирующих импульсов (например, с помощью дифференцирующих и интегрирующих цепочек), их делают разными по длительности.

Между уровнями «черного» и гасящих импульсов имеется защитный интервал, равный 0...5 % размаха полного видеосигнала. Этот интервал предохраняет от захода сигнала изображения за уровень гасящих импульсов и, следовательно, возможного срыва синхронизации генераторов разверток.

Полный видеосигнал включает сигнал изображения, строчные и кадровые синхронизирующие импульсы и гасящие импульсы. Параметры всех импульсов, вводимых в телевизионный сигнал, нормируются соответствующим стандартом.

Синхронизация ТК может быть внутренняя (от встроенного в телекамеру кварцевого генератора) и внешняя. В свою очередь, телекамеру с внешней синхронизацией можно синхронизировать:

- от сети питания;
- от специального устройства – синхрогенератора;
- от другой, выбранной ведущей, телекамеры.

Функции отдельных схем телевизионных камер. При использовании ТК в условиях сильно изменяющейся освещенности для поддержания выходного видеосигнала в определенных пределах в телекамерах предусмотрены специальные устройства и схемы.

Компенсация заднего света – способность телекамеры автоматически устанавливать выдержку, диафрагму и параметры усиления по некоторому фрагменту изображения (обычно по центру).

Во многих современных моделях телекамер предусмотрена специальная функция – аппаратная «компенсация заднего света». В простейшем случае телекамера с компенсацией заднего света настраивается не на среднюю освещенность, а на освещенность центральной части изображения. Тогда, за счет некоторого ухудшения качества изображения в засвеченной части матрицы, получается хорошее качество в центре поля обзора.

Электронный затвор. В течение суток освещенность на контролируемом объекте претерпевает существенные изменения. Для того чтобы поддерживать на постоянном уровне видеосигнал, используется встроенный в телекамеру автоматический электронный затвор (Electronic Shutter или Auto-Shutter).

Электронный затвор – устройство, которое встроено в ПЗС-матрицу телекамеры, изменяющее чувствительность телекамеры путем управления временем накопления электрического заряда – аналог выдержки фотоаппарата. В некоторых случаях электронный затвор может заменить объектив с автоматической диафрагмой. Время «выдержки» может изменяться в пределах от 1/50 до 1/10000 с, что позволяет работать телекамерам при освещенности от 1 до 8000 лк. Телекамеры с объективами без диафрагмы следует использовать только внутри помещений, так как возможностей электронного затвора не достаточно, чтобы отработать яркий солнечный свет или его отражение.

Уровень черного – уровень электрического сигнала в полном видеосигнале, представляющего собой черный цвет. В телекамере может применяться специальное устройство автоматической привязки к черному цвету, которое определяет самую темную часть изображения как оптически черный цвет, повышая в некоторых случаях контрастность изображения.

Ограничитель белого – схема внутри телекамеры, ограничивающая максимальное значение напряжения белого цвета в выходном видеосигнале на определенном уровне.

Гамма-коррекция – нелинейная обработка сигнала, которая корректирует шкалу градаций серого на изображении. Использование данной коррекции улучшает визуальное восприятие изображения.

Наличие в ТК гамма-коррекции влияет на точность передачи контраста изображения. Эта корректировка необходима из-за несоответствия преобразования изображения в телекамере и мониторе.

Кинескоп в мониторе имеет степенную зависимость яркости от сигнала (показатель степени 2,2), что приводит к уменьшению контрастности в темных участках и к увеличению в ярких; в то же время современные ПЗС-матрицы производят линейный сигнал. Для компенсации общей нелинейности в телекамеру встраивается устройство гамма-корректор, искажающее сигнал с показателем степени 1/2,2 (0,45). На некоторых телекамерах есть возможность выбрать коэффициент искажения (0,6 или 0,45).

Объективы

Очень важно правильно подобрать объектив для телекамеры. Если установить объектив неграмотно, то это приведет к ухудшению характеристик всей СФЗ. При выборе объектива возникают вопросы:

- какую территорию необходимо обозревать;
- насколько мелкие детали изображения нужно различать;
- как компенсировать изменения освещенности.

Чтобы ответить на эти вопросы, необходимо определить требования к оборудованию (в частности, к объективам). Для правильного подбора объектива необходимо рассмотреть технические характеристики используемых объективов.

Характеристики объективов. Фокусное расстояние (ФР) измеряется в миллиметрах и связано с углом получаемого поля обзо-

ра ТК. Объективы с маленьким ФР обладают широким углом обзора, а объективы с большим ФР обладают меньшим углом обзора. На рис. 4.3 показано, как зависит угол обзора объектива от его ФР.

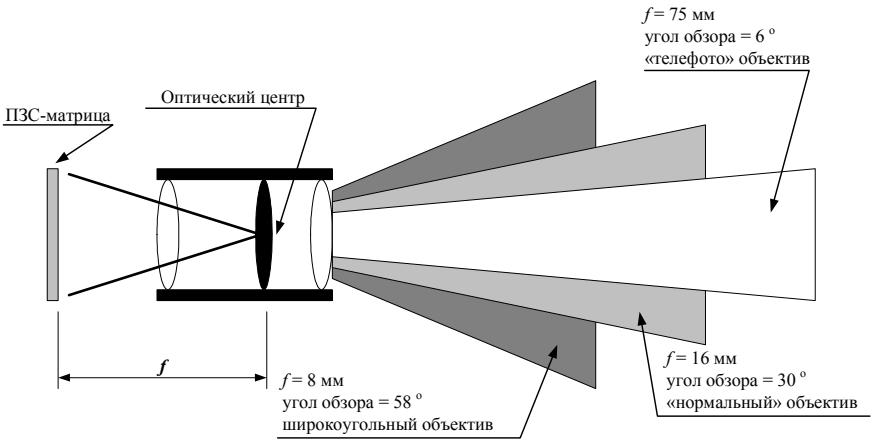


Рис. 4.3. Типы объективов: f – фокуское расстояние

В зависимости от задач применяют объективы с углом обзора от нескольких градусов (концентрация внимания на удаленном объекте) до 180 ° (для обзора большой территории). В системах телевизионного наблюдения, как правило, применяют объективы с фокусным расстоянием от 2,8 мм (широкоугольные) до 12 мм. Необходимо отметить, что угол обзора телекамеры зависит не только от фокусного расстояния применяемого с телекамерой объектива, но и от размера ПЗС-матрицы в телекамере.

В табл. 4.3 представлена зависимость угла обзора телекамеры от ФР применяемого с телекамерой объектива и размера ПЗС-матрицы телекамеры.

Если заранее известны габариты и удаление объекта наблюдения, то фокусное расстояние можно рассчитать по формулам:

$$f = v \times \frac{D}{V};\ f = h \times \frac{D}{H},$$

где f – фокусное расстояние, D – расстояние до объекта, V и H – вертикальный и горизонтальный размеры объекта соответственно, v и h – размеры изображения объекта на ПЗС-матрице.

Чтобы изображение занимало максимальную площадь матрицы, для расчета в качестве v и h берут габариты матрицы (например, для телекамеры с ПЗС-матрицей 1/2" – v=4,8 мм, h=6,4 мм).

Таблица 4.3. Зависимость угла обзора телекамеры от фокусного расстояния объектива и размера ПЗС-матрицы

Фокусное расстояние объектива, мм	***Формат ПЗС-матрици телекамеры, дюйм***			
	1/3	1/2	2/3	1
2,8	98°			
4	64°	86°		
6	42°	58°		
8	33°	42°	55°	
12	22°	30°		
16	17°	23°	30°	43°
25	11°	14°	19°	28°
50	5,5°	7°	10°	15°
75	3,6°	5°	6,6°	10°
100			5°	
150				4,9°
235				3,1°

Объективы с переменным фокусным расстоянием называются *трансфокаторами*. В процессе работы, возможно, понадобится изменить угол обзора телекамеры, например, при необходимости идентифицировать мелкие объекты (номера автомобилей). В этом случае применяются трансфокаторы и поворотные устройства для ТК.

Формат. При выборе объектива для телекамеры необходимо обратить внимание на формат объектива и соответствие его формату ПЗС-матрицы, используемой в телекамере. Формат объектива должен быть равен либо больше формата матрицы. При использовании объектива форматом, меньшим, чем формат телекамеры, на мониторе получится «эффект туннеля» – часть поля останется черным. Применение объективов форматом, большим формата матрицы, уменьшает угол зрения.

Диафрагма. Диафрагма необходима для изменения входного отверстия объектива, что позволяет регулировать количество света, проходящего через объектив. Объективы делятся по типу диафрагмы на:

- объективы без диафрагмы;
- объективы с ручной регулировкой диафрагмы;
- объективы с автоматической регулировкой диафрагмы.

Объективы без диафрагмы применяются только вместе с телекамерами, в которых есть схемы поддержки видеосигнала на постоянном уровне (компенсация заднего света, электронный затвор и др.). При работе телекамеры в условиях изменяющейся освещенности рекомендуется применять объективы с автоматической диафрагмой, что позволяет более широко регулировать уровень проходящего света через объектив и поддерживать освещенность ПЗС-матрицы на постоянном уровне. Диапазон изменения освещенности ограничен, например *F*1,4–64, значит, диаметр относительного отверстия объектива изменяется в 45,7 раз. Освещенность ПЗС-матрицы пропорциональна квадрату относительного отверстия,

таким образом, диапазон освещенности ПЗС-матрицы меняется в 2089 раз. Существуют объективы, светосила которых равна *F*0,75. В таких объективах применяются асферические линзы. Диапазон изменения освещенности, в котором может использоваться телекамера, оснащенная объективом с автоматической диафрагмой, достигает отношения 700000/1 (табл. 4.4).

Таблица 4.4. Автодиафрагма

Автодиафрагма объектива	***Диапазон изменения освещенности***
*F*1,2-64	2845/1
*F*1,4-300	45918/1
*F*1,8-360	40000/1
*F*1,2-720	360000/1
*F*1,4-1200	734694/1

Применение объективов с автодиафрагмой предпочтительнее в следующих случаях:

- когда ТК работает в условиях изменяющейся освещенности;
- когда требуется максимальная глубина резкости, которая достигается максимально закрытой диафрагмой;
- когда необходимо более четко передать границы ярких объектов.

Управление диафрагмой. Объективы с автодиафрагмой бывают следующих типов:

- с управлением удаленным внешним устройством;
- с прямым управлением;
- с управлением видеосигналом.

Диафрагма объектива может изменяться оператором дистанционно. Объективы с управлением автодиафрагмой видеосигналом

имеют встроенную схему, которая преобразует выходной видеосигнал в сигнал управления двигателем диафрагмы, т.е. на объектив подается только видеосигнал. Если автодиафрагма объектива имеет прямое управление, то ТК должна содержать электронную схему преобразования видеосигнала в постоянное напряжение, управляющее двигателями автодиафрагмы.

Светосила объектива характеризует долю световой энергии, пропускаемой объективом. Отношение площади входного зрачка к квадрату фокусного расстояния передней (по отношению к объекту) линзы (объектива оптического прибора) называется светосилой (геометрической светосилой) объектива. Освещенность изображения объекта (E) пропорционально светосиле объектива (I).

На рис. 4.4 представлен пример построения изображения.

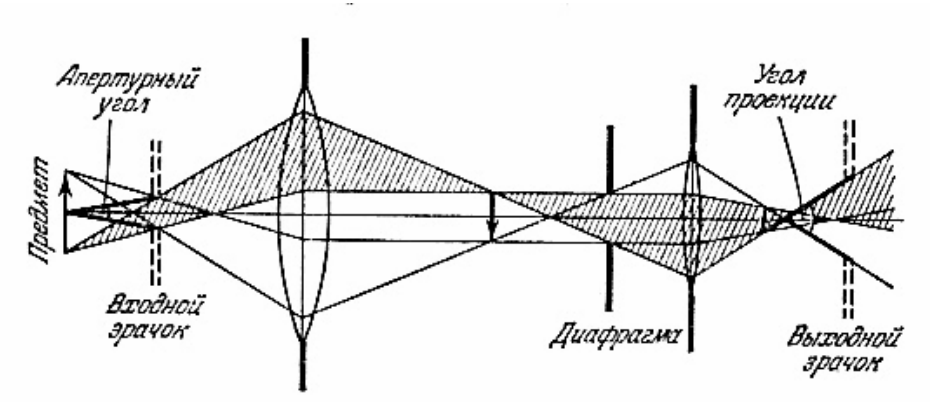


Рис. 4.4. Пример построения изображения

Отношение диаметра входного зрачка к фокусному расстоянию объектива называется относительным отверстием объектива Ω (см. рис. 4.4). Освещенность изображения объекта (E) пропорциональна квадрату относительного отверстия объектива ($E \sim \Omega^2$). В иностранной литературе в качестве аналогичной характеристики

объектива используют так называемое «фокальное число» F. Под фокальным числом понимают отношение фокусного расстояния объектива к диаметру входного зрачка. Светосила объектива обратно пропорциональна квадрату фокального числа

$$I = \frac{\pi}{4F^2} .$$

Обычно в характеристиках объективов указываются два значения фокального числа. Например, F1,2-360. Первое значение F1,2 соответствует состоянию объектива, когда диафрагма полностью открыта, второе значение F360 – состоянию, когда диафрагма полностью закрыта. Более низкое первое значение (например, F1,2 против F1,4) свидетельствует о том, что объектив пропускает больше света в условиях плохой освещенности, а это означает, что телекамера ночью передаст изображение лучшего качества. Более высокое второе значение (F360 против F64) предпочтительно при ярком свете.

Глубина обзора. Глубиной обзора (ГО) называется зона области обзора, которая находится в фокусе. Большее значение ГО означает, что большая часть поля зрения находится в фокусе – от объектов, находящихся вблизи объектива, до объектов, удаленных на бесконечность. Глубина обзора определяется углом обзора и светосилой объектива. Объективы с большим углом обзора имеют большую ГО. При изменении диафрагмы – чем меньше светосила объектива, тем больше ГО. При использовании объектива с автоматическим управлением диафрагмой стоит обратить внимание на то, что объекты, которые были днем в фокусе, будут не сфокусированы вечером, а тем более ночью. На рис. 4.5 приведена зависимость ГО от светосилы объектива.

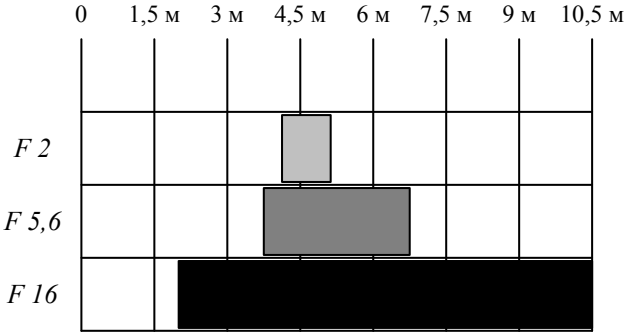


Рис. 4.5. Глубина обзора объектива

Крепление объективов. Существуют два стандарта на резьбовое соединение объектива с камерой – «С» и «CS». Эти резьбовые соединения имеют одинаковую соединительную резьбу 25,4х0,8, но различные задние отрезки: 17,526 и 12,5 мм соответственно. На рис. 4.6 наглядно представлены отличия объективов «С» и «CS» стандартов. Телекамеры с «С»-резьбой могут работать только с объективами, имеющими «С»-резьбу. А телекамеры с «CS»-резьбой допускают подсоединение объектива любого стандарта. Для совместимости стандартов выпускаются переходные кольца.

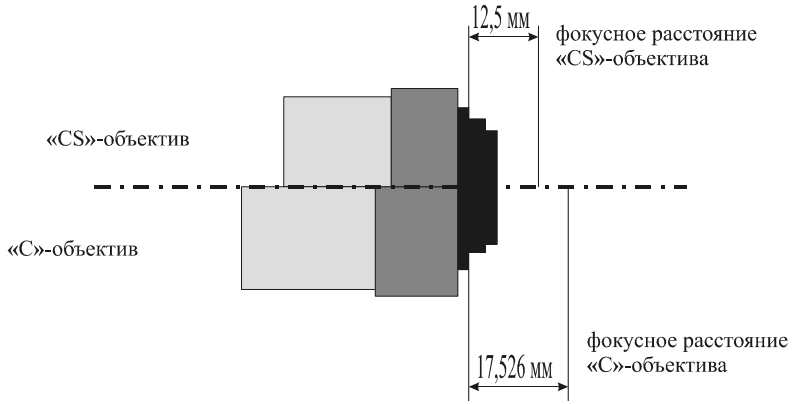


Рис. 4.6. Объективы «С» и «CS» стандартов

Асферические объективы. В таких объективах используется линза со сложной несферической формой поверхности, что позволяет значительно улучшить качество изображения, повысить оптические характеристики, устранить искажения, а также уменьшить размеры и массу оптических приборов. Такие объективы имеют большее значение светосилы, чем обычные многолинзовые объективы, так как уменьшается число отражающих плоскостей. Асферические объективы используются в системах с высокой чувствительностью.

Объективы «Pin-hole» (объектив с вынесенным входным зрачком) – специальный объектив с маленьким входным зрачком (диаметр от 0,8 до 4 мм). В основном применяются для скрытой установки.

Термин «вынесенный входной зрачок» применяют в тех случаях, когда плоскость диафрагмы совпадает с входным зрачком. В обычных объективах диафрагма находится внутри объектива. Если объектив имеет вынесенный входной зрачок, то уменьшение отверстия входного зрачка не приводит к уменьшению угла поля зрения объектива, а лишь снижает светосилу объектива, как это происходит при закрытии диафрагмы у обычных объективов. В реальных «Pin-hole» объективах вынос зрачка осуществляется на 0,5 – 5 мм, в зависимости от длины фокусного расстояния конкретного объектива.

Хорошее качество получаемого изображения и достаточная светосила достигаются в оптических системах (объективах), имеющих 4 – 5 или более линз в своем составе.

Технические характеристики телевизионных камер

Технические характеристики ТК можно разбить на две группы: электрические и конструктивные.

Электрические характеристики

Размер ПЗС-матрицы описывается параметром, называемым «формат». Формат – диагональный размер матрицы. Он измеряется в дюймах. Отношение высоты к ширине ПЗС-матрицы составляет 3/4. На самом деле, размеры эффективной рабочей поверхности ПЗС-матрицы – 75 % от размеров матрицы, что составляет для:

- ПЗС 1 дюйм – 12,8 х 9,6 мм;
- ПЗС 2/3 дюйма – 8,6 х 6,6 мм;
- ПЗС 1/2 дюйма – 6,4 х 4,8 мм;
- ПЗС 1/3 дюйма – 4,8 х 3,6 мм;
- ПЗС 1/4 дюйма – 3,2 х 2,4 мм.

Матрицы большого формата 1" и 2/3" практически перестали выпускать, так как телекамеры на их основе получаются громоздкими. Датчики изображения (ПЗС-матрицы) размером 1/4" применяются для сверхминиатюрных телекамер (например, для телекамер скрытого наблюдения). Совершенствование технологий позволяет производить уменьшение формата без ухудшения качества передаваемого изображения.

Размер матрицы важен при определении необходимого угла обзора телекамеры. С одинаковыми объективами телекамера на основе матрицы 1/2" имеет больший угол зрения, чем телекамера с матрицей 1/3". На рис. 4.7 представлена зависимость получаемого угла обзора изображения от применения объектива формата 1" с телекамерами разных размеров ПЗС-матрицы.

Разрешение. Важной характеристикой ТК является разрешение, которое измеряется в телевизионных линиях и зависит не только от числа пикселей на матрице, но и от параметров электронной схемы ТК. Разрешение (разрешающая способность) определяется как количество переходов от черного к белому или обрат-

но, которые могут быть переданы телекамерой. Поэтому единица измерения разрешения называется телевизионной линией (ТВЛ). Разрешение по вертикали у всех телекамер (кроме камер плохого качества) одинаково, ибо ограничено стандартом телевизионной развертки (например, 625 строк для стандарта СЕКАМ). Основное различие телекамер состоит в разрешении по горизонтали, именно оно должно указываться в техническом описании.

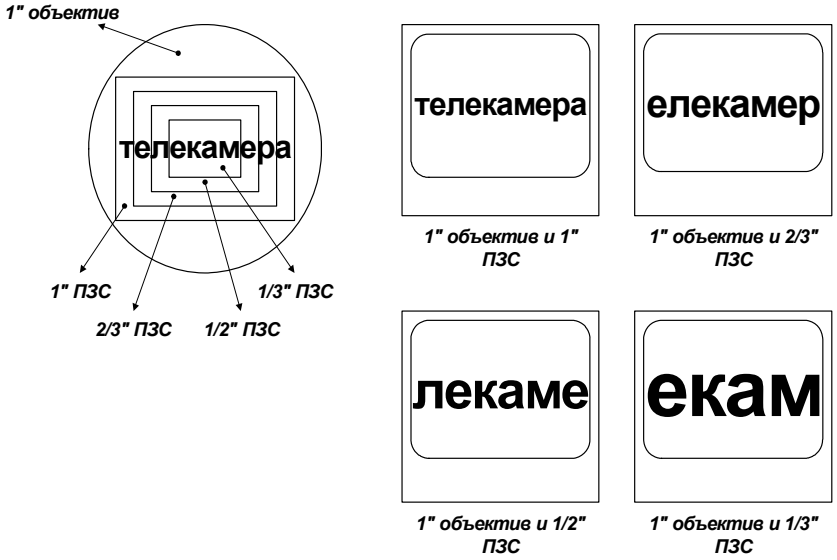


Рис. 4.7. Зависимость угла обзора изображения от размера ПЗС-матрицы

В большинстве случаев разрешение 380-400 ТВЛ вполне достаточно для ведения наблюдения. Существуют телекамеры, имеющие более высокое разрешение (например, 570 ТВЛ). Такие телекамеры позволяют четко видеть мелкие детали изображения (номера машин, лица людей и т.д.).

Разрешение цветных телевизионных камер несколько хуже, чем разрешение черно-белых: 300-350 ТВЛ. В настоящее время

появились цифровые цветные телекамеры, разрешение которых составляет 480 ТВЛ.

На разрешение телекамеры влияют два фактора:

1. Количество чувствительных элементов ПЗС-матрицы (пикселей).

Дискретная точечная структура матрицы приводит к эффекту «биения» при наблюдении полосатой картинки. Например, если у матрицы 400 пикселей по горизонтали, то, направив ее на тестовую таблицу, содержащую 200 черных и 200 белых линий, мы увидим четкую картинку из 400 линий. Однако, если сместить изображение на половину ячейки матрицы, то на каждую ячейку попадет половинка черной и половинка белой линии. Таким образом, эта телекамера может, в принципе, передать 400 линий, однако очень неустойчиво. Существует мнение, что надежно в таком случае передается количество линий, не превышающее 3/4 от числа ячеек. Например, если количество пикселей по горизонтали составляет 400, то в этом случае разрешение по горизонтали 300 ТВЛ. В настоящее время такой подход еще не закреплен в стандартах, так что нередко производители указывают завышенное значение разрешения своих телекамер.

2. Полоса частот видеосигнала, выдаваемого телекамерой.

Для передачи сигнала 300 ТВЛ необходима полоса частот 2,75 МГц (150 периодов на 55 мкс строки телевизионной развертки). В настоящее время использование высококачественных полупроводниковых усилителей не составляет проблемы, поэтому полоса пропускания усилителей ТК обычно значительно (в 1,5-2 раза) превосходит необходимую. Таким образом, разрешение ограничивается именно дискретностью ПЗС-матрицы.

Однако есть случай, когда современная электроника не позволяет поднять полосу пропускания видеосигнала выше 3,8 МГц. Это полный цветной видеосигнал. Поскольку сигнал цветности передается на поднесущей частоте (в стандарте PAL на частоте около

4,4 МГц), то сигнал яркости принудительно ограничивается полосой 3,8 МГц. Это соответствует разрешению около 420 ТВЛ. Некоторые производители указывают разрешение цветных телекамер 480 и более, но при этом, как правило, не акцентируют внимание, что это разрешение реализуется только если сигнал снимается с Y-C (Super-VHS) или компонентного (RGB) выхода. В этом случае сигналы яркости и цветности от телекамеры передаются двумя (Y-C) или тремя (RGB) отдельными коаксиальными кабелями. При этом все промежуточное оборудование (мониторы, коммутаторы, видеомагнитофоны) должны обладать входами/выходами типа Y-C или RGB. В противном случае, единственный промежуточный элемент, обрабатывающий полный видеосигнал, ограничит полосу пропускания 3,8 МГц.

Чувствительность. Еще один важный параметр ТК – чувствительность. Чаще всего под чувствительностью понимают минимальную освещенность на объекте, при которой можно различить переход от черного к белому, но иногда подразумевают минимальную освещенность на ПЗС-матрице. С теоретической точки зрения более правильно было бы указывать освещенность на матрице, так как в этом случае не нужно оговаривать характеристики используемого объектива. Но пользователю при подборе телекамеры удобней работать с освещенностью объекта, которую он заранее знает. Поэтому обычно указывают минимальную освещенность на объекте, измеренную в стандартизированных условиях – коэффициент отражения объекта 0,75 и светосила объектива 1,4.

Формула, связывающая освещенность на объекте и на матрице:

$$E_{\text{ПЗС}} = \frac{E_{\text{объект}} R}{\pi F^2},$$

где $E_{\text{ПЗС}}$ и $E_{\text{объект}}$ – освещенность ПЗС-матрицы и объекта наблю-

дения, R – коэффициент отражения объекта (см. табл. 4.2), F – светосила объектива.

На рис. 4.8 показан график зависимости относительной чувствительности человеческого глаза и черно-белой телекамеры от длины волны светового излучения. По сравнению с человеческим глазом чувствительность черно-белых телекамер существенно сдвинута в инфракрасную (ИК) область. Это позволяет при недостаточной освещенности использовать специальные инфракрасные прожекторы. Инфракрасное излучение не видно человеческому глазу, но фиксируется телекамерами.

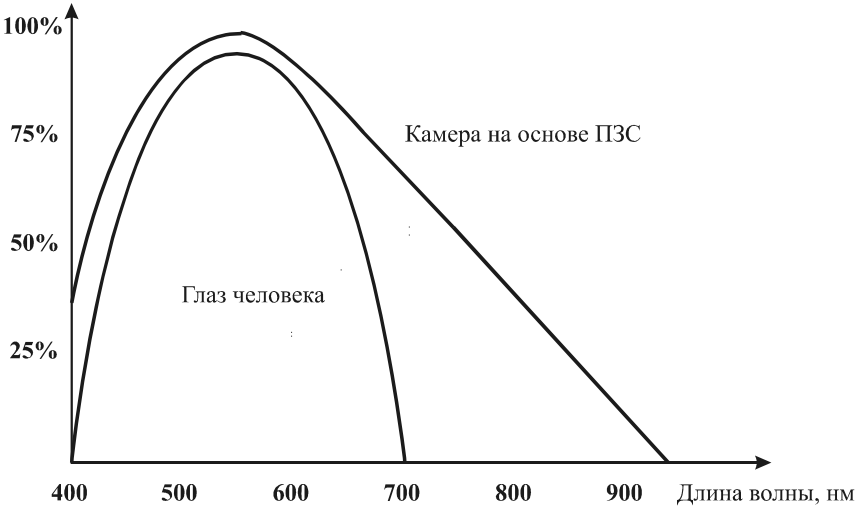


Рис. 4.8. График зависимости относительной чувствительности глаза человека и черно-белой телекамеры от длины волны излучения

Цветные ТК обладают меньшей чувствительностью, чем черно-белые телекамеры, так как характеристика спектральной чувствительности цветных ТК близка к характеристике спектральной

чувствительности человеческого глаза. Но это не сильно ограничивает возможности применения цветных телекамер.

Чувствительность современных черно-белых телекамер составляет порядка 0,01–1 лк при *F*1,2. Самые чувствительные телекамеры можно использовать ночью для наблюдений без инфракрасной (ИК) подсветки. Такие ТК обеспечивают приемлемое качество видеосигнала при лунном свете (см. табл. 4.1).

Отношение «сигнал/шум». В данных, приводимых в описаниях телекамер, указываются значения «сигнал/шум» для оптимальных условий, например при освещенности на матрице 10 лк и при выключенной автоматической регулировке усиления и гамма-коррекции. По мере уменьшения освещенности сигнал становится меньше, а шум, вследствие действия автоматической регулировки усиления (АРУ) и гамма-коррекции, больше.

Нередко чувствительность телекамеры указывают для «приемлемого сигнала», под которым подразумевается такой сигнал, при котором отношение «сигнал/шум» составляет 24 дБ. Это эмпирически определенное предельное значение зашумленности, при котором изображение еще можно записывать на видеопленку и надеяться при воспроизведении что-то увидеть.

Другой способ определения «приемлемого» сигнала – шкала IRE (Institute of Radio Engineers). Сигнал изображения (амплитуда 714 мВ) принимается за 100 единиц IRE (полный видеосигнал 140 IRE – амплитуда 1 В). «Приемлемым» считается сигнал около 30 IRE. Некоторые производители, в частности BURLE, указывают чувствительность при величине «приемлемого» сигнала для 25 IRE, некоторые для 50 IRE (уровень сигнала – 6 дБ). Выбор «приемлемого» уровня определяется отношением «сигнал/шум». Усилить электронный сигнал нетрудно, но при этом и шум усилится тоже.

Конструктивные характеристики

Конструкция узла крепления объектива. Если телекамера не имеет встроенного объектива, в ее конструкции предусмотрен узел присоединения для установки сменных объективов. Существуют два стандарта узлов присоединения объективов на телекамеры с резьбой 2,54x0,8, но с разными расстояниями до опорной плоскости:

- 17,526 мм для «C» стандарта;
- 12,5 мм для «CS» стандарта.

На некоторых моделях ТК имеется узел регулировки «C» или «CS» положения принимающего прибора (ПЗС-матрицы). Телекамеры с фиксированным «C»-креплением могут работать только с объективами типа «C», при попытке поставить на «C»-камеру «CS»-объектив изображение получиться размазанным, а телекамеры с фиксированным «CS»-креплением допускают подсоединение объективов типа «C» с адаптером крепления (см. крепление объективов).

Конструкция узла крепления телекамеры. Узел крепления предназначен для установки телекамеры в кожухе, на кронштейне и тому подобное. Существуют следующие стандарты для крепления выпускаемых ТК:

- 1/4" – 20 UNC;
- 3/8" – 16 UNC.

Комплектация. Большинство выпускаемых ТК имеют стандартный дизайн и поставляются без объектива, источника питания и другого вспомогательного оборудования, которое приходится выбирать отдельно в соответствии с потребностями. Однако выпускаются и оборудованные ТК, такие как:

- миниатюрные бескорпусные и корпусные ТК со встроенным объективом;
- офисные телевизионные камеры, имеющие встроенный объектив, кронштейн и оригинальный декоративный кожух, а также, если необходимо, аудиоканал;
- герметизированные телевизионные камеры. Состоят собственно из ТК, объектива и прочного герметичного кожуха, заполненного сухим азотом, с встроенным нагревателем;
- высокоскоростные поворотные телекамеры типа AutoDome с предустановками. Включают в себя собственно ТК с объективом, оснащенным трансфокатором, высокоскоростное поворотное устройство и декоративный кожух с кронштейном. Данные телекамеры способны запомнить до 99 положений, включая все установки ТК и объектива;
- телекамеры со встроенным радиочастотным передатчиком видеосигнала или передатчиком по телефонной линии.

Классификация телевизионных камер

Стандарт видеосигнала. Существуют стандарты для цветных и черно-белых камер. Для черно-белых СТН используются следующие стандарты выходного видеосигнала:

- CCIR – разрешение по вертикале 625 ТВЛ;
- EIA – разрешение по вертикале 525 ТВЛ.

Для систем цветного видеонаблюдения используются стандарты выходного видеосигнала:

- PAL;
- SECAM;
- NTSC.

Система PAL на 625 строк принята как стандарт в 1967 г. для телевизионного вещания в ряде стран Европы, в Австралии и дру-

гих регионах. Система PAL – трехсигнальная одновременная с квадратурной амплитудной модуляцией (одновременно передаются сигнал яркости и два цветоразностных сигнала). Название PAL – аббревиатура полного названия системы «Phase Alternation Line», что означает: система с переменной по строкам фазой сигнала цветности на поднесущей.

Система SECAM – двухсигнальная: одновременно передаются два сигнала – сигнал яркости (во всех строках) и один из цветоразностных на поднесущей частоте путем частотной модуляции колебаний частотной поднесущей. SECAM в переводе означает «Последовательная передача цветов и их воспроизведение при помощи запоминания».

Система NTSC (Nation Television System Committee) – трехсигнальная, т.е. одновременно во всех строках передаются три видеосигнала: сигнал яркости и два цветоразностных видеосигнала.

Чувствительность. Телевизионные камеры характеризуются значением минимальной освещенности, при котором телекамера обеспечивает приемлемый сигнал. Таким образом, телекамеры можно разделить по этому минимальному значению освещенности, которое определяется чувствительностью телекамеры. Итак, телекамеры, работающие при:

- дневном освещении (до заката) – примерно 50 лк;
- низком освещении (до сумерек) – примерно 4 лк;
- лунном свете (при освещенности, соответствующей свету четверти луны безоблачной ночью) – примерно 0,1–0,4 лк;
- свете звезд безоблачной ночью – примерно 0,0007–0,002 лк;
- инфракрасные ТК, в которых используются инфракрасные источники для работы при полном отсутствии видимого освещения.

Диапазоны и примеры типичных уровней освещения приведены в табл. 4.1.

Разрешение. Одной из основных характеристик телекамеры является ее разрешение. В связи с этим телекамеры можно разделить на:

- ТК обычного разрешения (до 380 ТВЛ);
- ТК повышенного разрешения (от 380 до 500 ТВЛ);
- ТК высокого разрешения (свыше 500 ТВЛ).

Условия применения. Диапазон применения современных средств СТН очень широк. Существуют разные способы и методы адаптации ТК к условиям окружающей среды (защитные кожухи, термокожухи), но даже необорудованные ТК приспособлены для работы при определенных условиях. По виду защиты от условий окружающей среды телекамеры можно разделить следующим способом: внутренние; внутренние общие; наружные; наружные общие.

Внутренние ТК предназначены для работы в отапливаемом помещении или офисе.

Внутренние общие ТК – для работы в закрытом от прямых осадков помещении (например, склад), но при этом диапазон допустимых колебаний температуры существенно шире по сравнению с внутренними телекамерами.

Наружные ТК защищены от прямого попадания дождя и солнечного света. К наружным телекамерам можно отнести также внутренние телекамеры с экстремальными условиями применения.

4.4. Устройства отображения видеоинформации

В системах телевизионного наблюдения используются специальные устройства отображения (мониторы), отличающиеся повышенной надежностью. Основными параметрами мониторов являются диагональ экрана, разрешение и цветность. Мониторы с небольшим экраном (5", 7”, 9" и 12") используются для вывода изо-

бражения в полноэкранном режиме, они удобны для компактного размещения в стойке. Для просмотра мультикартины (одновременный вывод изображения от нескольких телекамер) применяют мониторы 14", 15”, 17", 19” и 20". При выборе размера монитора для конкретной системы необходимо учитывать тот факт, что рекомендуемое расстояние от оператора до монитора должно быть 5 диагоналей экрана.

В системах телевизионного наблюдения применяются в основном мониторы двух типов: созданные на основе электроннолучевых трубок (ЭЛТ) и жидкокристаллические (ЖК) мониторы. Мониторы на ЭЛТ трубках всем хорошо известны и их аналогами являются осциллографы и телевизоры.

Жидкокристаллические мониторы используются в ноутбуках и в качестве дисплеев персонального компьютера. Но недавно появились и модели ЖК мониторов для СТН систем физической защиты объектов.

Принцип функционирования ЖК отличается от принципов ЭЛТ [4.4]. В ЖК мониторах изображение формируется не сканирующим электронным лучом, а путем адресации жидкокристаллических ячеек, которые поляризуются в различных направлениях, когда к их электродам прикладывается напряжение. Величина напряжения определяет угол поляризации, что, в свою очередь, определяет прозрачность каждого пикселя, формируя таким образом элементы видеоизображения. Стоит отметить следующие преимущества ЖК мониторов относительно ЭЛТ мониторов: отсутствуют элементы высокого напряжения; срок службы экрана не ограничен (не выгорает); плоский экран; меньше габаритные размеры; нет геометрических искажений; низкое энергопотребление; нет влияний электромагнитных полей.

Существуют две ЖК технологии. Первая – это пассивные ЖК мониторы. Кристаллическая матрица в пассивных ЖК мониторах состоит из пассивных жидких кристаллов, которые поляризуются в

зависимости от приложенного напряжения. Во второй технологии используются тонкие пленочные транзисторы в каждой ЖК ячейке, а так как транзисторы являются активными компонентами, то такие мониторы называются активной матричной ЖК панелью (TFT LCD).

Из недостатков ЖК мониторов необходимо отметить следующее. Во-первых, так называемый эффект «смазывания» из-за медленного пиксельного отклика на процесс строчной развертки, выглядит он как вертикальный ореол. Во-вторых, размеры пикселя определяют максимальную разрешающую способность монитора. В ЖК мониторах небольших размеров легко достигается разрешение уровня S-VGA.

Иногда в СТН используются 14-дюймовые телевизоры вместо соответствующего видеомонитора из-за выигрыша в цене. Телевизионные приемники производятся сотнями тысяч и стали дешевыми. В этом случае понадобится ТВ приемник с аудио/видео входом. Телевизоры обычно размещаются в пластмассовом корпусе, который не защищает аппаратуру от электромагнитного излучения соседних устройств. В СТН рядом могут находиться несколько видеомониторов, поэтому они выполняются в металлическом корпусе. Металлический корпус частично снижает уровень электромагнитного излучения для оператора системы и уменьшает вероятность возгорания прибора. Видеомониторы рассчитаны на круглосуточную работу в течение многих лет, а телевизоры нет.

Некоторые модели мониторов имеют встроенные переключатели и квадраторы. Существуют также специальные портативные (мобильные) модели мониторов, предназначенные для настройки и регулировки ТК. Монтажник при настройке системы подключает этот монитор к ТК и видит на нем то, что передает телекамера. Монитор легко умещается в руке и питается от батареек.

4.5. Средства передачи видеосигнала

Изображение объекта наблюдения, преобразованное телевизионной камерой в электрический сигнал, передается или вернее поступает на устройства отображения и обработки видеоинформации (монитор, коммутатор или устройство записи). Для того чтобы видеосигнал прошел путь от ТК до монитора, он должен пройти через передающую среду. Это относится и к сигналам управления поворотными и исполнительными устройствами телекамер, только направление следования этих сигналов противоположное.

Ниже представлены используемые в СТН средства передачи видеоинформации [4.4]:

- коаксиальный кабель;
- кабель «витая пара»;
- микроволновая связь;
- радиочастотная связь;
- связь с помощью инфракрасного излучения;
- телефонная линия;
- волоконно-оптический кабель.

Наиболее часто в СТН для передачи видеосигналов применяются коаксиальный кабель и кабель «витая пара», а также все большую популярность приобретает волоконная оптика [4.4].

Коаксиальные кабели

На сегодняшний день коаксиальный кабель – это самое распространенное средство передачи видеосигналов, а также сигналов управления поворотными и исполнительными устройствами ТК (поворотное устройство, трансфокатор, диафрагма).

Поперечное сечение коаксиального кабеля показано на рис. 4.9. Кабель имеет симметричную и соосную структуру. Видеосигнал

передается по центральной жиле, а экран используется для уравнивания нулевого потенциала концевых устройств (ТК и, например, монитора). Экран также защищает центральную жилу от внешних электромагнитных помех (ЭМП).

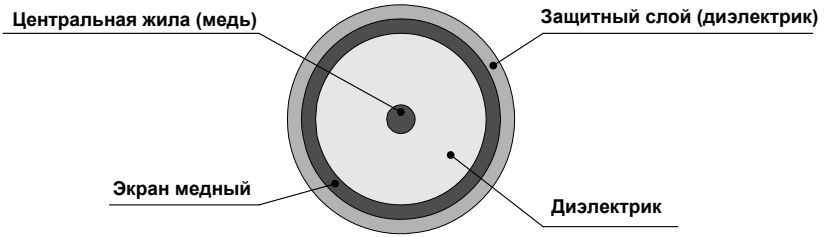


Рис. 4.9. Поперечный разрез коаксиального кабеля

Благодаря соосному строению кабеля все ЭМП индуцируются только в экране. Если экран должным образом заземлен, то наведенный шум разряжается через заземления ТК и монитора. Центральная жила коаксиального кабеля является сигнальным проводом, а экран – заземляющим.

Для концевой заделки коаксиального кабеля используются BNC-разъемы (сокращение от первых букв фамилий создателей Bayonet, Neil и Concelman) (рис. 4.10).

Существуют три типа BNC-разъемов: под пайку, под обжим и с резьбой. Паяные разъемы, очевидно, самые надежные, но наиболее удобными и требующими минимальных трудозатрат являются разъемы под обжим. Существует недорогой специальный инструмент, позволяющий быстро и качественно устанавливать BNC-разъемы под обжим. Стыковку коаксиального кабеля лучше производить с помощью специальных разъемов, например, BNC-разъемов для стыковки кабеля.

Рис. 4.10. BNC-разъемы: слева под пайку, справа под обжим

Передача видеосигнала по «витой паре»

Кабель «витая пара» используют в ситуациях, когда необходимо проложить линию длиной больше двухсот метров. Если используется обычный кабель «витая пара», то это обходится довольно дешево, но если используется специальный кабель (рекомендованный производителями), с минимум 10-20 скрутками на один метр и защитной оболочкой (экраном), то этот кабель будет существенно дороже. Передачу видеосигнала при помощи витой пары называют симметричной видеопередачей. В отличие от несимметричной (коаксиальной) передачи видеосигнала, концепция передачи видеосигнала по витой паре заключается в том, что для минимизации внешних электромагнитных помех по витой паре передается сбалансированный сигнал. Все нежелательные электромагнитные помехи и шум, в конечном счете, одинаково воздействуют на оба провода. Поэтому лучше использовать специальные кабели, в которых оба провода одинаково подвержены наводкам и имеют одинаковое падение напряжения. В отличие от передачи по коаксиальному кабелю с заземленным экраном, в концепции передачи видео-

сигнала по витой паре не заложено уравнивание потенциалов между конечными точками. Когда сигнал достигает приемного конца линии на основе витой пары, он попадает на вход дифференциального усилителя с хорошо сбалансированным фактором коэффициента ослабления синфазного сигнала (КОСС). Этот усилитель считывает дифференциальный сигнал между двумя проводами. Если два провода имеют схожие характеристики и достаточно закруток на метр (чем больше, тем лучше), на них будут одинаково воздействовать шумы, падение напряжения и наводки. Усилитель с хорошим КОСС на приемном конце линии устранит большую часть нежелательных шумов.

Недостаток этого типа передачи состоит в том, что в дополнение к кабелю необходимы одно передающее и одно приемное устройство (см. рис. 4.11). Они увеличивают не только стоимость системы, но и риск потерять сигнал, если какой-либо из этих двух компонентов выйдет из строя. На рис. 4.11 представлена функциональная схема системы передачи видеосигнала по «витой паре».

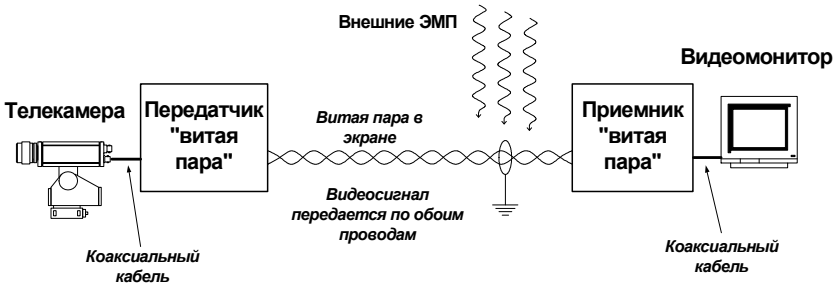


Рис. 4.11. Передача видеосигнала по кабелю «витая пара»

При использовании специального кабеля «витая пара» можно передать видеоизображение на большие расстояния (по сравнению с коаксиальным кабелем) с минимальными потерями и искажениями. Производители устройств передачи видеоинформации по витой

паре указывают расстояния более 2000 м для черно-белых сигналов и более 1000 м для цветных без промежуточных усилителей, в то время как по коаксиальному кабелю – до 600 м без корректоров и усилителей. При симметричной передаче видеосигнала (по витой паре) не возникает «земляных петель», что возможно при передаче по коаксиальному кабелю на расстояния уже более 200 м. Концевая заделка кабеля «витая пара» не требует специальных инструментов и разъемов.

Микроволновая связь

Микроволновая связь является беспроводным каналом передачи видеоинформации. На рис. 4.12 представлена функциональная схема беспроводной системы передачи видеосигнала. Видеосигнал сначала модулируется частотой, которая соответствует микроволновому диапазону электромагнитного спектра. Длины волны этого диапазона варьируются от 1 мм до 1 м. Практически для микроволновой передачи видеосигнала обычно используются частоты от 1 до 10 ГГц [4.4], что соответствует СВЧ диапазону.

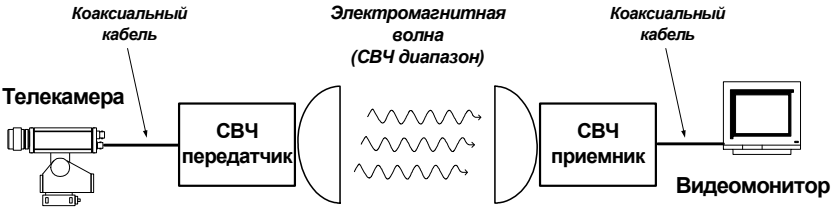


Рис. 4.12. Беспроводная передача видеосигнала

Многие государственные и коммерческие структуры — военные, милиция, скорая помощь, курьеры, служба авиасвязи и нави-

гации – работают в указанном выше радиодиапазоне. Поэтому, используя микроволновую связь в СТН (и не только в СТН), следует учитывать то, что каждую частоту и микроволновый источник излучения необходимо согласовать с соответствующими регулирующими органами власти, чтобы исключить или свести к минимуму возможность наложения сигналов от нескольких СВЧ передатчиков. Это позволяет защитить зарегистрированных пользователей, но является недостатком или, вернее, неудобством использования для использования данного беспроводного канала связи [4.4].

Микроволновая связь позволяет передавать очень широкую полосу частот видеосигналов, а также, если необходимо, других данных (звук и сигналы управления поворотными устройствами и объективами ТК). Микроволновая передача может осуществляться в одном направлении, когда передается только видеосигнал и звук с ТК, либо в двух направлениях, когда в одном направлении передается видео- и аудиосигнал, а в обратном – сигналы управления исполнительными устройствами телекамер.

При передаче аудио- и видеосигналов одновременно видеосигнал кодируется при помощи амплитудной модуляции (АМ), а аудиосигнал – при помощи частотной модуляции (ЧМ), так же как в телевещании.

Передающие и приемные антенны представляют собой параболические антенны, аналогичные тем, что используются для приема спутникового телевидения. Передатчик и приемник при такой передаче сигнала должны находиться на линии прямой видимости. Расстояния, которые можно покрывать при помощи этой технологии, зависят от выходной мощности передатчика и диаметра антенны, что определяет коэффициент усиления передатчика и чувствительность приемника. На качество принимаемого сигнала влияют окружающие (атмосферные) условия. Если система спроектирована недостаточно грамотно, то микроволновая связь, обеспечивающая отличное изображение в погожий день, может давать

значительную потерю и искажения сигнала в проливной дождь. Туман и снег также влияют на передаваемый сигнал. Если параболическая антенна не закреплена должным образом, то качающий ее ветер может повлиять на связь, приводя к периодической потере прямой линии видимости [4.4].

Существуют системы микроволновой связи для передачи видеоизображения, которые позволяют передавать сигнал на расстояния до 30 км. Для микроволновой связи на более коротких расстояниях могут использоваться стержневые антенны или другие типы непараболических антенн. В данном случае возникают проблемы безопасности, связанные с ненаправленной передачей сигнала.

Радиочастотная связь

Радиочастотная (РЧ) передача видеосигнала по модуляции напоминает микроволновую беспроводную передачу. Однако основные различия заключаются в том, что частота модуляции лежит в высокочастотном (ВЧ) и ультравысокочастотном (УВЧ) (VHF и UHF) диапазонах и осуществляется «всенаправленная» передача сигнала. Направленная антенна, например, типа «волновой канал» (подобно внутренним антеннам, используемым для приема определенного телеканала), позволяет получать сигнал в более удаленных точках. Следует отметить, что в зависимости от принятых норм, мощность излучения не должна превышать определенный предел, а в случае такого превышения потребуется разрешение соответствующего органа на использование необходимой частоты [4.4].

Радиочастотные передатчики обычно снабжены видео- и звуковыми входами, а методы модуляции напоминают методы модуляции микроволн, т.е. для видеосигнала используется амплитудная модуляция, а для звукового сигнала – частотная.

Существенным недостатком использования радиочастотной связи в СТН является то, что сигнал может быть получен любым ТВ приемником, находящимся на незначительном расстоянии. Радиочастотная связь в отличие от микроволновой связи не требует прямой видимости, поскольку РЧ излучение (в зависимости от того, УВЧ это или ВЧ сигнал) может проходить через кирпичные стены, дерево и другие неметаллические объекты. Расстояние распространения радиосигнала зависит от многих факторов, и лучше всего проверять это в местах будущего применения этих систем.

Связь с помощью инфракрасного излучения

Инфракрасные (ИК) системы передачи видеосигнала используют оптические средства. Источником света является инфракрасный светодиод. Яркость световой несущей передаваемого сигнала модулирована видеосигналом. Для подобной передачи сигнала необходима линия прямой видимости. На рис. 4.13 изображена функциональная схема беспроводной системы передачи видеосигнала с помощью ИК излучения. Для беспроводной передачи сигналов в ИК диапазоне разрешения не требуется, что является преимуществом этого типа связи [4.4].

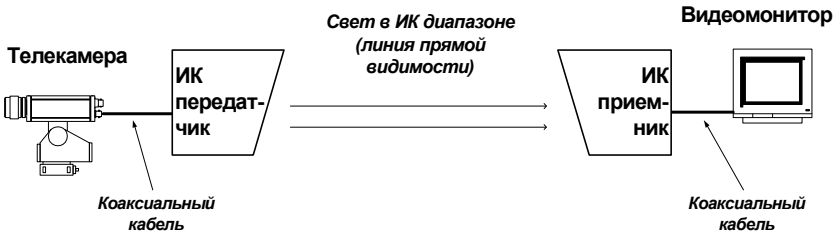


Рис. 4.13. Инфракрасная система передачи видеосигнала

Необходимо принять специальные меры предосторожности для обеспечения благоприятного температурного режима в зоне установки передающей системы, иначе на приемник могут попасть инфракрасные частоты, излучаемые горячими стенами, раскаленными крышами и металлическими объектами. Такие погодные условия, как дождь, туман и ветер влияют на инфракрасный канал связи больше, чем на связь в СВЧ диапазоне [4.4].

Передача изображений по телефонным каналам связи

Технологии и системы передачи изображений по телефонным (ТЛФ) линиям связи существуют с 1950-х годов. Системе «медленного сканирования», принадлежащей к старому поколению таких систем, требовалось 32 с, чтобы передать изображение низкого качества с тревожного пункта на станцию слежения. А если еще добавить время дозвона и соединения, в результате реально более минуты уходило на передачу первого изображения. Сегодня существуют более прогрессивные способы передачи видеосигналов по телефонной линии. Новая технология – «быстрое сканирование» – опирается на более мощные методы обработки изображений и алгоритмы сжатия, что позволяет менее чем за 1 с передать полноцветное изображение. Манипулирование изображением осуществляется в цифровой форме, при этом используются различные методы сжатия. Задержка в 1 с в передаваемом изображении (вернее, передача изображения со скоростью 1 кадр в секунду) является минимально допустимым пределом для СТН СФЗ. Исходя из этого, можно сделать вывод, что подобные системы недопустимо использовать в системах физической защиты важных объектов.

Передача изображений (не видеосигнала) по мобильным телефонам сегодня является доступной и привлекательной технологией. В распространенных цифровых сотовых сетях можно получить скорость в 14,4 кбит/с, но этого не достаточно для применения данной технологии в СТН СФЗ.

Волоконно-оптические линии связи

Волоконная оптика – это технология, в которой в качестве носителя информации используется свет. Обычно используется инфракрасный свет, а средой передачи служит стекловолокно. Передача сигналов (не только видеосигналов) по стекловолокну имеет следующие преимущества перед существующими кабельными средствами передачи.

- Более широкая полоса пропускания.
- Низкое ослабление сигнала, порядка 1,5 дБ/км (по сравнению с 30 дБ/км для коаксиального кабеля RG-59).
- Волокно (являющееся диэлектриком) создает электрическую (гальваническую) изоляцию между передающим и принимающим концом линии связи, поэтому невозможно возникновение «земляных петель».
- Свет как носитель сигнала полностью остается внутри волоконно-оптического кабеля, поэтому не вызывает помех в соседних кабелях или других волоконно-оптических кабелях.
- Стекловолокно не чувствительно к внешним сигналам и электромагнитным помехам, поэтому не важно, рядом с каким источником напряжения будет проходить кабель – 110 В, 240 В, 10 000 В переменного тока или совсем близко от мегаваттного передатчика. Даже если молния ударит в одном сантиметре от кабеля – никаких наводок в нем не будет [4.4].
- Невозможно сделать ответвление волоконно-оптического кабеля, не повредив при этом качества сигнала, что немедленно обнаруживается на принимающем конце линии.

Из недостатков волоконно-оптического кабеля стоит отметить следующие.

- Концевая заделка волоконно-оптического кабеля проводится с помощью специальных инструментов и специально подготовленным персоналом.
- Возникают трудности с переключением и маршрутизацией сигналов, передаваемых по волоконно-оптическим линиям связи.

Волоконно-оптический (ВО) кабель (рис. 4.14) имеет больше преимуществ, чем какой-либо другой. Многие годы волоконно-оптический кабель использовался в телекоммуникациях и теперь становится все более популярен в СТН и системах безопасности.

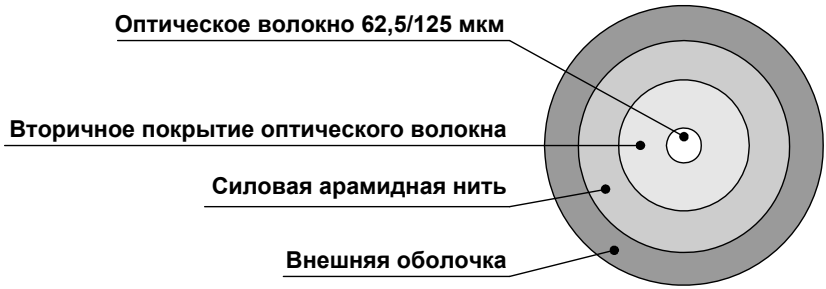


Рис. 4.14. Поперечное сечение волоконно-оптического кабеля

При использовании волоконно-оптических линий связи в СТН требуются преобразователи (передатчики) электрического сигнала в оптический и дешифраторы (приемники) оптического сигнала в электрический, аналогично всем рассмотренным выше (исключая коаксиальные) методам передачи видеосигнала. При «односторонней» связи (передача изображения и звука только в одном направлении) потребуется только одна жила волоконного кабеля, а при «двусторонней» связи, когда передаются сигналы управления на исполнительные устройства телекамер, необходимо использовать два волокна. На рис. 4.15 изображен простой пример использова-

ния ВО линий связи в СТН. Все выше описанные преимущества и недостатки применения ВО линий связи относятся в полной мере и к СТН. При использовании ВО линий связи в СТН можно передать изображение на несколько километров с минимальными потерями качества изображения, что является очень полезным для организации СФЗ протяженных объектов, территория и периметр которых простирается на десятки километров.

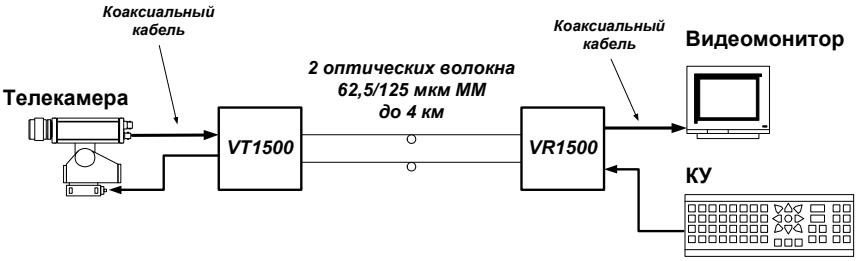


Рис. 4.15. Пример ВО линии связи в СТН: *VT1500 и VR1500* – приемопередатчики оптического сигнала фирмы *ifs,* КУ – клавиатура управления

Значительно более широкая полоса пропускания оптических кабелей (по сравнению с «металлическими») позволяет передавать одновременно по одному оптическому волокну несколько видеосигналов. Для этого применяются так называемые волоконно-оптические мультиплексоры. Пример использования такого устройства изображен на рис. 4.16.

По мере усовершенствования технологии концевой заделки и сращивания волоконно-оптического кабеля, а также его удешевления все больше в СТН будет использоваться волоконная оптика.

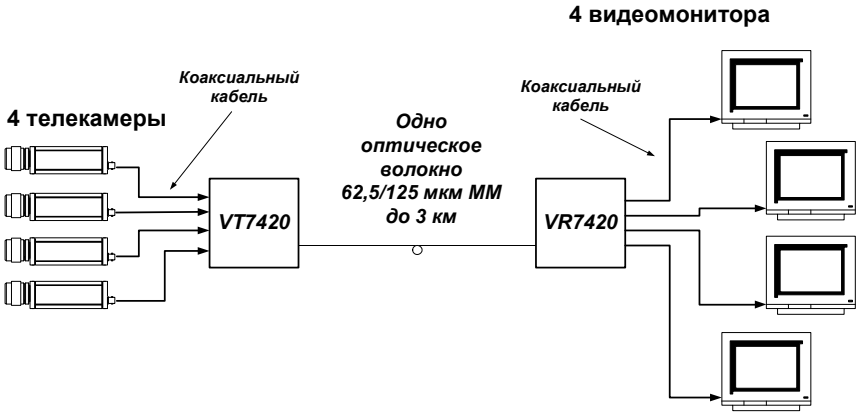


Рис. 4.16. Пример применения волоконно-оптического видеомультиплексора: *VT7420 и VR7420* – приемопередатчики оптического сигнала фирмы *ifs*

4.6. Устройства обработки видеоинформации

Основными устройствами обработки видеоинформации являются видеокоммутаторы, квадраторы, матричные коммутаторы и мультиплексоры. Рассмотрим их особенности по отдельности.

Видеокоммутаторы

При наличии в СТН нескольких телекамер возникает вопрос о методах представления оператору потока визуальной информации на экране видеомонитора. Возможны следующие методы представления визуальной информации:

- последовательный (поочередное переключение телекамер);
- параллельный (одновременное отображение на экране видеомонитора изображений от всех телекамер);

- последовательно-параллельный (поочередное переключение групп телекамер).

Выбор того или иного метода и типа необходимого оборудования представления видеоинформации с объекта зависит от задач физической защиты, количества телекамер в системе и требований, налагаемых на качество видеозаписи и выводимого на экран изображения.

Видеокоммутаторы (коммутаторы, последовательные переключатели или свитчеры) созданы для управления выводом изображения от набора телекамер на один монитор. Они применяются в небольших СТН (до 16 телекамер). Видеокоммутаторы просты в обращении, надежны, дешевы и не ухудшают качество изображения, как это возможно при цифровой обработке изображения либо при наблюдении нескольких изображений на одном мониторе.

Самые первые коммутаторы были ручными. К ним подключался набор телекамер, и оператор нажатием кнопки выводил на монитор изображение с той или иной телекамеры по своему выбору. Со временем процесс переключения телекамер автоматизировался. Через заданное время (от 1 до 90 с) все телекамеры поочередно автоматически подключаются к монитору, и оператор может последовательно просматривать передаваемое с них изображение. При условии последовательного переключения всех телекамер наблюдения существует «неконтролируемое» оператором время для каждой из телекамер. Пусть время наблюдения по каждой телекамере $t_н$ = 5 с, количество видеокамер n=16 шт., тогда неконтролируемое время по каждой из зон равно 1 мин 15 с. За такой промежуток времени даже неподготовленный нарушитель может совершить противоправное действие (например, пересечь контрольно-следовую полосу периметра объекта, проникнуть в здание и т.д.).

Распределив все телекамеры СТН на группы и подключая каждую группу к отдельному коммутатору, можно уменьшить «некон-

тролируемое» время в системе. Подобный метод отображения информации называется последовательно-параллельным. В приведенном выше примере, разбив телекамеры на две группы (два коммутатора в системе), «неконтролируемое» время в СТН уменьшится в два раза. Также надо отметить, что значение времени наблюдения по каждой телекамере $t_н = 5$ с обусловлено тем, что меньшее время будет приводить к быстрой утомляемости оператора. Увеличение числа применяемых в системе видеокоммутаторов также повышает утомляемость оператора, так как при этом увеличивается число одновременно наблюдаемых изображений.

Большинство видеокоммутаторов имеет возможность подключения тревожных сигналов с датчиков обнаружения. При срабатывании датчика обнаружения, подключенного к одному из этих тревожных входов, на экране видеомонитора появляется изображение тревожной зоны от заданной телекамеры. При одновременном срабатывании нескольких датчиков тревожные зоны отображаются поочередно в соответствии с выбранным временем наблюдения.

Записывать с видеокоммутаторов на видеомагнитофон можно только то изображение, которое в данный момент просматривается на подключенном к коммутатору мониторе.

Достоинства использования видеокоммутаторов:

- отсутствие потери информации из-за уменьшения разрешающей способности (в режиме мультиизображения или цифрового преобразования изображения);
- возможность применения видеомониторов с небольшим размером экрана.

Недостатки:

- невозможность наблюдения за обстановкой во всех контролируемых зонах одновременно;
- утомляемость оператора при непрерывном переключении изображений;

- невозможность видеорегистрации событий по всем зонам без потери информации с помощью одного видеомагнитофона.

Параметры видеокоммутаторов. Видеокоммутаторы характеризуются следующими параметрами:

- количество входов видеосигнала;
- количество выходов видеосигнала;
- ширина полосы пропускания (обычно не менее 10 – 20 МГц, чтобы существенно не влиять на разрешающую способность по горизонтали всей видеосистемы);
- уровень перекрестных искажений (как правило, на уровне 40 – 50 дБ, во избежание «пролезания» видеосигналов из канала в канал);
- наличие входов тревоги (их число соответствует числу видеовходов);
- наличие аудиоканалов, коммутируемых синхронно с видеоканалами;
- возможность дистанционного управления (для организации многопостовой видеосистемы);
- возможность регулировки времени наблюдения – одинакового по всем зонам или программируемого для каждой зоны наблюдения в отдельности (например, для выбора приоритетных зон наблюдения или с целью нарушения монотонности работы оператора, которая может приводить к снижению его внимания и работоспособности);
- возможность синхронизации момента переключения каналов кадровыми синхроимпульсами видеосигнала с целью исключения срыва кадровой синхронизации при коммутации (что уменьшает утомляемость оператора при использовании телекамер без внешней синхронизации),

- наличие встроенного генератора текста, позволяющего оператору идентифицировать местоположение отображаемой зоны, что необходимо в момент тревоги;
- возможность программирования видеокоммутатора по экранному меню – порядок переключения зон (включая обход зон), время наблюдения по каждой зоне, входное сопротивление и прочее.

Квадраторы

Для удобного просмотра изображения от нескольких (четырех) телекамер применяют квадраторы. С помощью квадратора на один монитор выводится одновременно изображение от четырех телекамер (экран монитора делится на четыре равных части). В этом случае на мониторе можно наблюдать четыре изображения в реальном времени. Квадраторы можно использовать и для записи на видеомагнитофон – одновременно записываются четыре телекамеры. Так как изображение от каждой телекамеры занимает лишь часть (четверть) экрана монитора, то качество записи ухудшается.

Существуют квадраторы, которые содержат встроенный переключатель (коммутатор) и тревожные входы. Некоторые модели квадраторов имеют функцию «картинка в картинке». Квадраторы используются как основной элемент систем охраны малых объектов (до 12 телекамер).

Матричные коммутаторы

Матричный коммутатор позволяет построить гибкую и легко наращиваемую СТН, в которую будут входить не только системы видеонаблюдения, но и системы охранной сигнализации (подсистема обнаружения) и контроля доступа. Все коммутаторы можно разделить на три класса: коммутаторы для малых систем, коммута-

торы для средних систем и коммутаторы, позволяющие строить сателлитные соединения.

Коммутация видеовходов с видеовыходами. Матричный коммутатор (МК) позволяет вывести видеосигнал с любой из подключенных телекамер на любой монитор или видеомагнитофон, подсоединенный к одному из видеовыходов коммутатора. Например, коммутатор фирмы «Burle» TC8800 позволяет подключить до 256 источников видеосигнала (телекамер) и до 64 приемников (мониторов, видеомагнитофонов).

Матричный коммутатор – устройство программируемое. Оператор системы задает при программировании последовательности вывода видеосигналов на мониторы и предустановки для поворотных устройств и трансфокаторов телекамер. Для каждой ТК возможно задавать индивидуальное время вывода изображения на заданный монитор. Некоторые модели МК позволяют выводить изображение на мониторы в «залповом» режиме, т.е. на выбранную группу мониторов автоматически переключается заданная последовательность телекамер. Например, можно запрограммировать коммутатор так, чтобы в течение дня наблюдение велось за техническим процессом на объекте, а ночью – за периметром объекта.

Программирование и управление МК осуществляется и при помощи внешних клавиатур управления, либо с клавиатуры управления, встроенной на лицевой панели прибора. К МК можно подсоединить несколько внешних клавиатур управления. С клавиатур также можно управлять поворотными устройствами и трансфокаторами телекамер.

Осуществлять программирование и управление МК можно также через персональный компьютер, связанный с коммутатором через порт RS-232 либо RS-485. Специальное программное обеспечение позволяет быстро и удобно реализовать все функции программирования и управления коммутатором, а также контроля оперативной обстановки на объекте.

К матричному коммутатору можно подключить интерфейс тревожных контактов, к которому подводятся кабели от элементов системы охраны. При программировании матричного коммутатора составляются таблицы соответствия тревожных контактов, телекамер и мониторов, на которые будут выводиться «тревожные» телекамеры в случае поступления сигнала на определенный контакт тревожного интерфейса. Таким образом, если в каком-то месте произошло нарушение (например, движение какого-то объекта вызвало срабатывание детектора движения), то по сигналу тревоги изображение с телекамеры, наблюдающей за местом тревоги, будет выведено на соответствующий монитор. В случае тревоги коммутатор предпринимает действия согласно заданной программе: активизирует сирену, выводит на монитор запрограммированную «тревожную» надпись, выдает сигнал управления на внешнее исполнительное устройство или другой интерфейс тревожных контактов. Затем система в зависимости от заданной программы либо будет ждать, пока на сигнал тревоги не обратит внимание оператор, либо включит магнитофон на запись, либо дозвонится по заранее запрограммированному номеру телефона, либо автоматически сбросит тревогу через определенное время.

Сателлитное соединение. В случае очень больших систем или в системах с пространственно разнесенными телекамерами (например, разные корпуса предприятия) используют систему из нескольких матричных коммутаторов, соединенных между собой. В такой системе один коммутатор является центральным, а остальные сателлитными. Почему рекомендуется применять несколько МК? Например, в системе 100 телекамер. Если все телекамеры подвести к одному коммутатору, то пучок из коаксиальных кабелей будет очень толстым. Если же коммутатор выйдет из строя, то «ослепнет» сразу вся система видеонаблюдения. Отказоустойчивость системы с одним МК очень маленькая, и на особо важных объектах требуется устанавливать дублирующую аппаратуру.

Использование сателлитного соединения позволяет побороть оба эти недостатка. Во-первых, в случае выхода из строя одного из коммутаторов, даже центрального, все остальные продолжают автономно работать. Во-вторых, не нужно тянуть от коммутатора к коммутатору десятки кабелей, их число в сателлитном соединении, как правило, не выходит за пределы одного десятка. Кроме этого сателлитная схема позволяет организовать разграничение в уровне доступа. Например, большой объект, на котором ряд цехов и лабораторий ведут секретные работы. Если все телекамеры объекта подсоединены к одному коммутатору, то оператор будет иметь возможность просматривать изображение со всех телекамер, в том числе и с расположенных в секретных помещениях. Если в этих подразделениях установить сателлитные коммутаторы, то, чтобы просмотреть изображение с телекамер, потребуется разрешение местного персонала.

Мультиплексоры

Мультиплексоры являются многофункциональными приборами, позволяющими проводить интеграцию системы телевизионного наблюдения с другими подсистемами СФЗ на объекте (системой обнаружения, системой контроля доступа). Мультиплексоры повышают уровень защиты объекта и значительно облегчают труд оператора службы безопасности.

Основная функция мультиплексоров – организация одновременной записи изображения от нескольких телекамер на один видеомагнитофон. Затем эти изображения с помощью мультиплексора можно восстановить и просмотреть на мониторе.

Существуют три основных режима работы мультиплексоров:

- наблюдение в реальном масштабе времени (используется режим мультиизображения);
- запись изображений;
- просмотр записей.

Наблюдение в реальном масштабе времени – наблюдение за реальной картинкой с объекта в разных режимах (например, при подключении 16 телекамер): последовательное переключение телекамер, многоэкранное изображение (мультиизображение), наблюдение за ограниченным набором изображений (например, 4 из 16 телекамер). При просмотре изображения можно также выводить на монитор название изображения (например, «телекамера № 1 – переход»), дату, время.

Запись изображения – запись на один видеомагнитофон суммарного изображения разделенных по времени изображений (мультиплексная запись) с определенного набора телекамер, т.е. запись полных кадров (или полукадров) видеоизображения последовательно от каждой из подключенных ТК. Мультиплексоры позволяют справиться с проблемой несинхронизации телекамер. В мультиплексорах применяется процессор цифровой обработки изображения с буферной кадровой памятью, в которую на короткое время записывается изображение от ТК. Если даже запись на видеомагнитофон запрограммирована – один полный кадр в секунду (режим с пропуском кадров), то бояться потери полукадра изображения не стоит. Мультиплексор хранит в памяти оцифрованное изображение от каждой телекамеры. Из целых полукадров мультиплексор формирует суммарную последовательность полных кадров или полукадров, которая записывается (посылается мультиплексором) на пленку видеомагнитофона. При записи полукадров разрешение изображения будет в два раза хуже.

Возможно записывать на видеомагнитофон разные мультиизображения, при этом воспроизводиться будут также мультиизображения.

До появления мультиплексоров для записи изображений от нескольких телекамер применялись фреймсвитчеры – переключатели видеосигнала, в которых переключение осуществляется в момент кадрового синхроимпульса, при этом необходимо, чтобы все телекамеры были синхронизированы друг с другом.

В процессе формирования выходного сигнала для записи в невидимые строки кадра изображения записывается служебная информация (номер и описание ТК, время и т.д.). Эта информация понадобится при воспроизведении записанной информации. Мультиплексор можно запрограммировать на определенную последовательность (процедуру) выдачи изображения от нескольких телекамер на запись. Например, последовательная запись по одному полному кадру от каждой из 16-ти телекамер (режим записи с пропуском кадров). В режиме воспроизведения мультиплексор позволяет просматривать записанное изображение с определенной (заданной) телекамеры (например, просмотр телекамеры № 1). При этом на экране монитора, который подключен к мультиплексору, мы увидим «дискретное» изображение с телекамеры № 1. Изображение дискретное, потому что в нормальном режиме записывается 25 полных кадров в секунду (50 полукадров), а в нашем примере запись с телекамеры № 1 была сделана в 16 раз медленнее, т.е. записано на пленке видеомагнитофона 25/16 полных кадра в секунду. Но и значение 25/16 кадра в секунду завышено или даже идеально, так как выходной сигнал с мультиплексора имеет увеличенный интервал между кадрами изображения. Также этот интервал может быть увеличен программированием (например, при режиме записи «24 часа на 3-часовую кассету») или изменением режима работы системы (тревога в системе). Невидимая служебная информация, записанная на пленку видеомагнитофона, используется мультип-

лексором для выбора необходимых кадров при просмотре из всей последовательности кадров от 16-ти телекамер.

В мультиплексорах применяется способ динамического распределения времени записи, который основан на анализе изменений изображения. При обнаружении изменений в изображении от телекамеры частота записи изображения от этой телекамеры увеличивается или даже становится непрерывной, что уменьшает вероятность пропуска важной информации.

Просмотр записи – мультиплексор позволят просматривать необходимую телекамеру из последовательности записанных кадров от разных телекамер. Возможен просмотр в режиме мультиизображения при последовательной записи.

Существующие мультиплексоры могут работать в одном из указанных выше режимов (симплексные мультиплексоры), либо одновременно в двух (дуплексные мультиплексоры) или даже трех режимах (триплексные мультиплексоры).

Разрешающая способность мультиплексора измеряется в точках (пикселях), так как мультиплексор – цифровой прибор, а в цифровой технике разрешение измеряют количеством отображаемых на экране точек (количество точек на дюйм – DPI). Разрешение мультиплексора определяется объемом (структурой) его оперативной памяти и быстродействием процессора цифровой обработки изображения (быстродействием АЦП, ЦАП и самого процессора).

Мультиплексор позволяет программировать автоматическое последовательное переключение изображений с разных ТК при просмотре в режиме реального времени и при просмотре видеозаписи в полноэкранном формате (последовательность ТК, время задержки на ТК, время задержки при поступлении сигнала тревоги).

Мультиплексор позволяет определить количество и размер одновременно наблюдаемых на видеомониторе изображений. Форматы мультиизображения могут быть следующими: стандартные 2x2, 3x3, 4x4; неравномерное распределение изображений 8+2, 4+3,

12+1; и «картинка в картинке» 1+1 и 1+4. Все обозначенные форматы мультиизображения могут быть записаны на видеомагнитофон. При этом воспроизвести запись можно будет только в формате записанного мультиизображения.

Функция маскирования изображения применима при установке на рабочем месте оператора (внешний пульт управления мультиплексором и монитор) различных прав доступа. Можно запретить просмотр изображения с определенных ТК операторам с низким уровнем доступа, но при этом изображение с этих телекамер будет записываться на видеомагнитофон.

Детектор активности или детектор движения. Существуют мультиплексоры, в которые уже встроен детектор активности. Детектор активности и детектор движения являются разными устройствами по своим выполняемым функциям. Детектор активности реагирует на любые изменения в поле зрения телекамеры, например локальное изменение освещенности (автоматическое или автономное включение/выключение освещения), появление нового объекта, движение объекта в поле зрения и т.д. Алгоритмы обнаружения в этом случае строятся на анализе изменения яркости изображения. Детектор движения реагирует только на появление движущегося объекта и не реагирует на изменения яркости стационарного изображения, поэтому алгоритмы обнаружения движения более сложные, чем анализ изменения яркости изображения.

Существуют мультиплексоры, выполняющие функции детектора движения. В этих приборах детектор движения позволяет задавать зоны срабатывания, размеры и скорость перемещения объекта срабатывания и другие параметры.

Использование функции детектора активности или движения во внешних (уличных) условиях влечет за собой большое количество ложных тревог. Улица является источником помех различного рода (животные и птицы, движущийся транспорт и свет от него и других источников, погодные явления и т.д.).

Имеется возможность управления внешними удаленными исполнительными устройствами через мультиплексор (поворотные устройства телекамер, объективы с внешним управлением и т.д.). Таким образом, может быть запрограммирована не только ТК, с которой идет просмотр или запись изображения, но и положение поворотного устройства, на котором установлена эта телевизионная камера.

Стандартный последовательный интерфейс RS-232 или RS-485 позволяет управлять мультиплексорами при помощи специального управляющего устройства (пульт дистанционного управления) или персонального компьютера, а также создавать «сеть» телевизионного наблюдения. Единого протокола обмена данными для этих целей не существует, поэтому мультиплексоры разных производителей в одной системе телевизионного наблюдения могут работать только отдельно.

Внешние входы/выходы («сухие контакты»), которые также полностью программируются мультиплексором. Например, при поступлении сигнала тревоги от внешнего датчика мультиплексор переходит в ранее запрограммированный режим записи, или оператору предоставляется возможность выбора дальнейшего режима работы системы (выполнение указанной последовательности работы мультиплексора может быть реализовано и при поступлении сигнала тревоги со встроенного детектора активности). При выработке мультиплексором сигнала тревоги (встроенный детектор активности либо внешние «входные» контакты) внешний выход может использоваться для включения видеомагнитофона, который находился до этого в «ждущем» режиме, на запись; и подать сигнал управления на внешние исполнительные устройства (устройства оповещения, блокирования возможности выхода из здания и т.д.).

К мультиплексору возможно подключить внешнюю синхронизацию. Эта функциональная возможность переключает мультиплексор от телекамеры к телекамере по внешнему сигналу управле-

ния (синхросигналу). Внешний сигнал синхронизации можно подать на мультиплексор от подключенного к нему видеомагнитофона либо от общего для всей системы синхрогенератора. В последнем случае режим переключения всей системы от кадра к кадру устанавливается автоматически. Если сигнал синхронизации на мультиплексор подавать с видеомагнитофона, то при изменении скорости записи/воспроизведения магнитофона мультиплексор автоматически отслеживает это изменение, что позволяет решить проблему синхронной работы системы мультиплексор-видеомагнитофон.

Новые модели мультиплексоров совмещают в себе функции матричного коммутатора – позволяют выводить изображения от любой подключенной телекамеры на любой из подключенных мониторов. Использование интерфейса RS-232 или RS-485 дает возможность объединять несколько мультиплексоров в «сеть» и управлять ими с одного пульта и/или персонального компьютера Рабочих мест оператора в этой «сети» может быть несколько (рис. 4.17). На рис. 4.17 изображена функциональная схема «сети» телевизионного наблюдения, построенная на базе видеомультиплексоров Uniplex Series фирмы Dedicated Micros.

Существуют мультиплексоры, у которых 32 и 48 видеовходов. Но при таком большом количестве подключаемых телекамер эффективнее использовать два или более мультиплексоров, так как при записи большого количества изображений с телекамер на один видеомагнитофон возможна потеря важной информации (9 или 16 видеовходов для мультиплексора являются оптимальным значением).

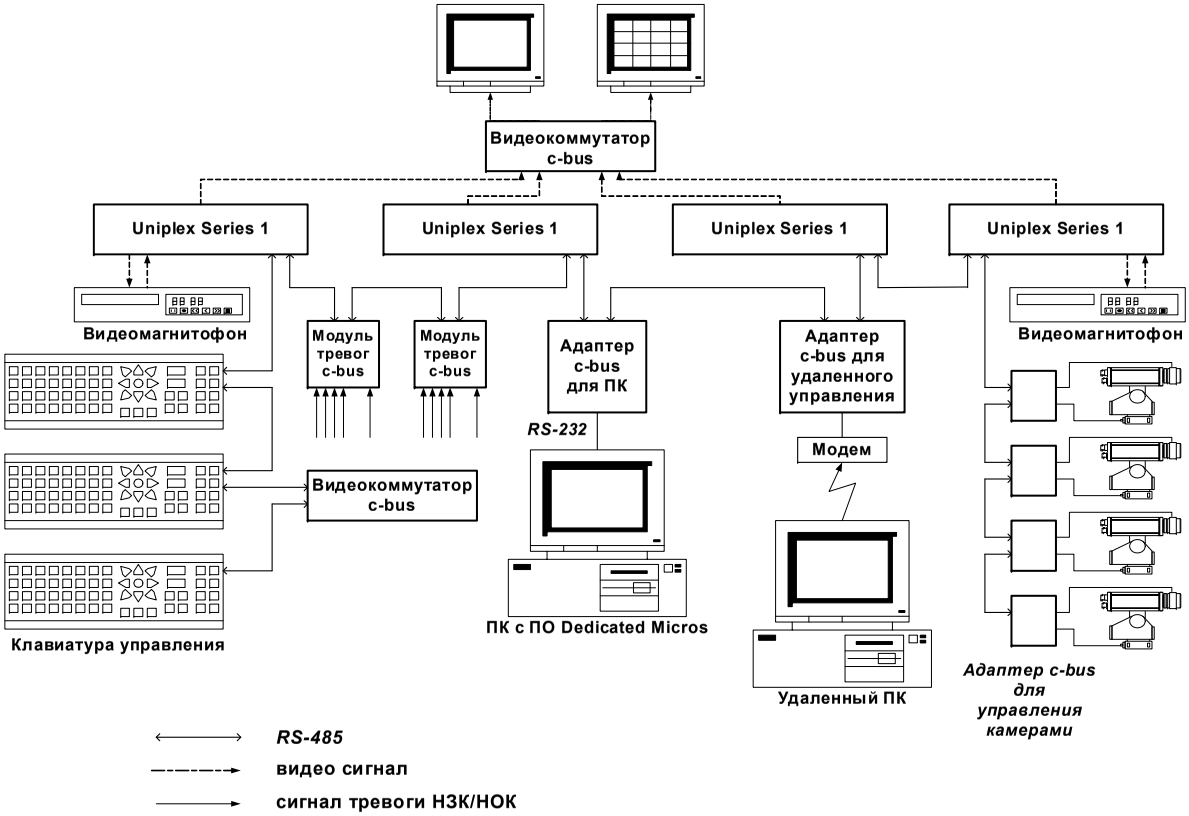


Рис. 4.17. «Сеть» ТСН на основе видеомультиплексоров Uniplex Series фирмы Dedicated Micros

4.7. Устройства регистрации и хранения видеоинформации

Специальные видеомагнитофоны

Существует несколько способов видеозаписи для систем телевизионного наблюдения с помощью видеомагнитофонов (ВМ). Ниже рассматриваются стандартные, хорошо себя зарекомендовавшие видеомагнитофоны стандарта VHS. Относительно небольшая стоимость, распространенность совместимой и вспомогательной техники и расходных материалов обеспечивают популярность специальных кассетных видеомагнитофонов. Вместе с технологией записи на магнитную ленту (стандарт VHS) существует несколько специальных приемов, применяемых для СТН в системах физической защиты объектов. В основном они направлены на повышение времени записи.

Запись с пропуском кадров. Наиболее распространенный вариант – записывается не каждый кадр, а, например, каждый пятый. В этом случае на одну стандартную VHS кассету (E180) умещается 15 ч записи. Если записывать каждый девятый кадр, то уместится и 27 ч. Большинство специальных видеомагнитофонов при этом осуществляют непрерывное медленное движение ленты. Поскольку звук в системе VHS записывается отдельной неподвижной головкой на продольной дорожке, то в таких режимах записи возможна непрерывная запись звука, хоть и с худшим качеством (чем медленнее движется лента, тем уже полоса воспроизводимых частот). При еще более растянутой записи (существуют модели, реализующие запись до 720 или 960 ч на стандартную кассету E180) лента движется непостоянно. В 720-часовом режиме, например, пауза между полукадрами составляет 5 с. Такое медленное (в 240 раз медленнее номинального) движение ленты трудно реализовать. Практически реализуется другое решение – лента движется маленькими шагами. Подвинули ленту, записали кадр, подождали 5 с,

снова подвинули и т.д. В этом режиме о записи звука речь уже не идет. Разные модели специальных видеомагнитофонов отличаются еще одним параметром – кадровая или полукадровая запись. Стандартный телевизионный сигнал состоит из двух чередующихся полукадров: в одном только четные строки, в другом – нечетные. Некоторые магнитофоны в режиме прореживания кадров осуществляют запись полного кадра (оба полукадра), а потом пропускают несколько кадров. Некоторые записывают только один полукадр, пропускают несколько, а затем другой, снова пропускают несколько и т.д. В первом случае лучше качество записи отдельного кадра – это моментальный снимок полного разрешения. Однако пауза между кадрами в 720-часовом режиме составит уже 10 с. Во втором случае ценой возможной потери разрешения достигается уменьшение вдвое паузы между записью отдельных полукадров. Современные модели видеомагнитофонов предлагают на выбор оба режима записи.

Магнитофоны с уплотненной записью. В этих магнитофонах стоят уменьшенные видеоголовки и должны применяться улучшенные видеокассеты. Ценой некоторой потери качества записи и, что хуже всего, совместимости со стандартом VHS, обеспечивается большая плотность записи (чаще лежат дорожки на ленте). Соответственно, на одну кассету умещается до 12 ч записи без пропусков кадров (тройная плотность записи).

Магнитофоны с записью по тревоге. Этот режим в минимальном варианте реализован даже в некоторых бытовых магнитофонах. При срабатывании датчика охраны замыкаются входные контакты видеомагнитофона, и начинается запись. Недостаток бытовых магнитофонов – большое время от замыкания контакта до начала записи. Массивный блок видеоголовок должен раскрутиться до номинальной скорости 10 – 20 оборотов в секунду. В специальных видеомагнитофонах есть специальный режим «готовность 0». В этом режиме (режиме ожидания) лента заправлена, и головка по-

стоянно вращается. Запись начинается буквально мгновенно – уже следующий кадр будет записан, хотя несколько первых кадров, пока движение ленты не стабилизируется, могут быть чуть искажены. Необходимо отметить, что в режиме ожидания лента должна немного двигаться, иначе вращающаяся головка ВМ может протереть ленту насквозь. Таким образом обеспечивается и поддержание нормального натяжения ленты. В большинстве случаев периодическое продвижение осуществляется автоматическим кратковременным включением записи. В таком случае режим ожидания можно рассматривать как особый «сверхдлинный» режим записи – шесть полукадров каждые три минуты (запись полгода на одну кассету). По тревоге может осуществляться также переход из медленных режимов записи в один из более быстрых, вплоть до номинальной скорости записи (3 часа на кассету).

Цифровые системы телевизионного наблюдения

Цифровые технологии в СТН используются для архивирования и хранения видеоинформации. В этой части главы дано краткое описание цифровых СТН и рассмотрены возможности конкретного цифрового устройства записи.

В настоящее время цифровые технологии бурно вторгаются во все сферы нашей повседневной жизни, и телевидение (в частности СТН) – не исключение. Производительность современных средств вычислительной техники позволяет работать в реальном масштабе времени с телевизионным изображением без потери качества и за вполне приемлемые деньги. Для небольших систем (до 16 телевизионных камер) сегодня по ряду причин более подходят аналоговые системы (в основном, потому что они дешевле). Однако, уже начиная с некоего уровня сложности СТН, цифровые системы оказываются экономически эффективнее. Основные преимущества цифровых систем телевизионного наблюдения указаны ниже.

• Возможность хранения записанной информации сколь угодно долго без потери качества.

• Простота и надежность копирования на различные носители (CD, DVD, DDS, стример) при полном сохранении качества исходного материала при копировании.

• Возможность передачи видеоинформации по компьютерным сетям.

• Небольшие затраты на техническое обслуживание, так как не требуется приобретение новых кассет.

• Одновременная работа режимов записи и воспроизведения (в аналоговых системах для этого требуется два специальных видеомагнитофона).

• Простота и скорость поиска нужного фрагмента или кадра.

• Гибкость и адаптивность (возможность гибко настраивать систему в зависимости от выполняемой задачи, стоящей перед пользователем).

• Возможность доработки, модернизации системы, самостоятельной разработки дополнительных приложений для систем, основанных на ПК.

• Возможность получения высококачественного изображения.

• Стабильный и четкий стоп-кадр.

• Возможность распечатки изображений на обычном принтере.

При рассмотрении цифровых систем необходимо различать системы, основанные на персональных компьютерах (операционные системы Windows или Linux), в которые вставляются платы расширения и устанавливается прикладное ПО; и системы на основе специализированных цифровых устройств.

Первые являются более гибкими, но и более сложными. Надежность распространенных операционных систем (ОС) известна. Вторые работают на специализированных ОС, с существенно меньшей функциональностью, а, следовательно, вероятность оши-

бок и склонность к зависанию такой аппаратуры гораздо меньше. Внешне такие устройства напоминают аналоговые, и для работы с ними гораздо легче подготовить персонал. Считается, что более предпочтительным является использование систем второго типа (из-за их надежности).

Есть тенденция устанавливать аналого-цифровой преобразователь (АЦП) в корпус телевизионной камеры. Однако такое решение осложняет выбор ТК с подходящей аналоговой и цифровой частью, что ведет к ее удорожанию. Такое решение является оправданным, когда ТК находится на удалении более нескольких километров от приемника. На такое расстояние передать аналоговый сигнал без помех практически невозможно, если не использовать волоконно-оптические линии связи.

Ниже приведено описание возможностей мультиплексора со встроенным устройством записи видеоинформации.

Мультиплексор с цифровой записью Calibur DVMRe-4eZT

Мультиплексор Calibur DVMRe-4eZT (фирмы Kalatel, США) – это цветной 4-канальный видеомультиплексор, обеспечивающий запись изображений от нескольких телекамер на встроенный жесткий диск с возможностью одновременного просмотра информации, записанной ранее. В отличие от обычных специальных видеомагнитофонов длительной записи, данный мультиплексор обеспечивает более высокое качество изображения. В зависимости от настроек, он позволяет сохранять от нескольких часов до 1 месяца цветного видеоизображения (модель с жестким диском 20 Гб).

Мультиплексор DVMRe Triplex имеет два выхода на мониторы и три основных режима работы:

- просмотр «живого» видео;
- воспроизведение;

• запись.

Все три режима могут быть задействованы одновременно.

Просмотр «живого» видео. Возможно отображение «живого» видеоизображения как в полноэкранном, так и в мультиэкранном формате (четыре сегмента, «картинка-в-картинке»). Выбор телекамеры для просмотра в полноэкранном формате осуществляется нажатием клавиши с номером желаемой телекамеры.

В режиме последовательности мультиплексор поочередно пролистывает изображения от телекамер на выбранном мониторе. Последовательность отображения телекамер и время задержки программируются. В полноэкранном режиме возможно двукратное увеличение изображения. Режим увеличения работает как с динамичными, так и со статичными изображениями (стоп-кадр). Возможно перемещение по увеличенному изображению, при этом ТК остается неподвижной. Режим стоп-кадра работает как в полноэкранном формате, так и в мультиэкранном, при этом возможно «замораживание» только отдельных сегментов. Для каждой телекамеры задается наименование, которое может выводиться вместе с текущим временем.

Воспроизведение. Этот режим позволяет воспроизводить изображение только на одном мониторе (А). Другой монитор (В) в это время отображает «живое» видео в полноэкранном или мультиэкранном формате. Воспроизведение возможно как вперед, так и назад. При этом оператор также может менять скорость воспроизведения. В режиме воспроизведения доступен режим стоп-кадра. Возможен покадровый просмотр.

В режиме воспроизведения есть такие же возможности просмотра, как и в режиме «живого» видео: мультиэкранный формат (кроме «картинка-в-картинке»), полноэкранный формат, полноэкранный формат с последовательностью, масштабирование.

Calibur DVMRe Triplex имеет мощную систему поиска, позволяющую быстро находить записи по интересующей дате, как на встроенном жестком диске, так и на внешнем устройстве архивации. Пользователь может осуществлять поиск по дате, тексту, тревогам или по движению в выбранной зоне экрана.

Запись. Запись производится на встроенный жесткий диск со всех подключенных телекамер. Частота записи при этом может изменяться от 0,066 до 25 кадров в секунду по каждой телекамере, однако частота по всем телекамерам в сумме не может превышать 40 кадров/с.

Отображение «живого» видео и воспроизведение в мультиэкранном формате на мониторах A и B не влияет на режимы записи.

Существует режим скрытых телекамер, когда запись изображения производится, но оно не отображается на мониторе.

Видеомультиплексор имеет таймер включения/выключения записи, дающий возможность настроить дату и время.

При тревогах настраивается период «предсобытия» (до 5 с) и «постсобытия» (до 250 с), когда изображение записывается с частотой кадров, соответствующей частоте записи при тревоге.

Обработка мультиплексором тревожных сигналов. Через интерфейсную плату может быть подключено до четырех нормально-разомкнутых тревожных датчика, которые будут поставлены в соответствие с соответствующими телекамерами.

При поступлении тревоги, в зависимости от настроек, на монитор выводится изображение с соответствующей телекамеры, изменяется частота записи тревожных телекамер, включается встроенный зуммер, активируется реле, выполняются предопределенные макрофункции. При поступлении нескольких тревог одновременно телекамеры выводятся в формате последовательности. Список последних (до 100) тревог сохраняется и может быть просмотрен впоследствии.

Видеомультиплексор DVMRe также имеет встроенный детектор активности, который настраивается отдельно по каждой телекамере.

Связь с внешними устройствами. Мультиплексор DVMRe-4eZT имеет порт SCSI для связи с внешними устройствами архивации. Поддерживаются следующие устройства: дисковый массив Calibur DVSe, RAID-массивы, DAT- или AIT-накопители, CD-R/CD-RW приводы.

Для связи с внешним модемом используется стандартный порт RS-232.

Несколько мультиплексоров и системных клавиатур (CBR-RB3/J или KTD-405) могут быть объединены в сеть по протоколу RS-485. При этом с клавиатур возможно управление и программирование мультиплексоров.

Мультиплексор может быть включен в сеть Ethernet (стек протоколов TCP-IP). При этом с компьютера, на котором установлено ПО WaveReader, возможен просмотр «живого» видео, просмотр видеоархива, программирование видеомультиплексора.

Система меню. Мультиплексоры DVMRe-4eZT имеют развитую структуру меню, защищенного паролем. Используются два пароля: для оператора и инсталлятора. Ввод пароля оператора дает возможность включать/отключать отображение времени и названий телекамер, просматривать историю событий и изменять пароль оператора.

Ввода пароля также требуют изменение языка меню и сброс мультиплексора к заводским настройкам. Пароли оператора и инсталлятора могут быть изменены, остальные пароли – нет.

Есть опция блокировки передней панели прибора. При этом активным остается только меню.

4.8. Дополнительное оборудование в системах телевизионного наблюдения

К дополнительному оборудованию СТН относятся кронштейны, защитные кожухи, поворотные устройства, пульты управления поворотными устройствами и трансфокаторами ТК.

Существует множество различных кронштейнов для размещения телекамер, начиная от пластиковых, рассчитанных на установку в помещении телекамеры с объективом с фиксированным фокусным расстоянием и суммарным весом не более 200 г, и заканчивая цельнометаллическими или даже литыми, рассчитанными на установку телекамеры в кожухе весом до 50 кг и более (при установке телекамеры в кожухе на поворотном устройстве). На рис. 4.18 представлены примеры кронштейнов для установки ТК.

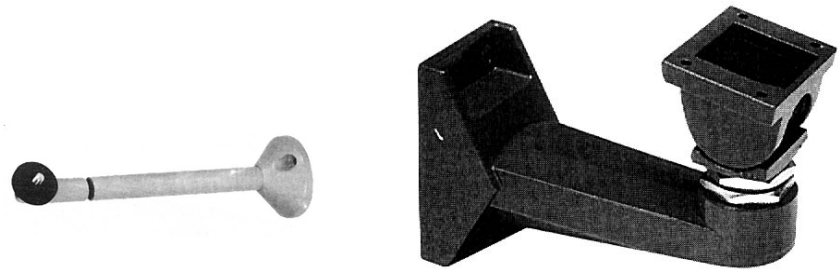


Рис. 4.18. Примеры различных кронштейнов для ТК

Кожухи телевизионных камер

Кожухи используются для защиты телекамер от воздействия внешней среды (пример изображен на рис. 4.19) и/или для маскировки направления наблюдения.

Кожухи могут быть простыми в конструкции, установке и использовании, но они в равной мере могут влиять на качество изображения и срок службы телекамеры, если не защищают ее должным образом от погодных явлений, вандализма и радиации. Существуют кожухи для установки телекамер во взрывоопасной среде. Кожухи бывают самых разных размеров и форм, в зависимости от применения телекамеры и ее длины. В наши дни, с уменьшением размеров телекамер, вместо традиционных кожухов часто используются тонированные купольные системы, которые гораздо лучше вписываются в интерьер помещений и прекрасно сочетаются с архитектурой зданий [4.4].

Рис. 4.19. Защитный кожух камеры на кронштейне

Многие кожухи имеют встроенный подогрев и вентилятор. Подогрев может понадобиться в холодных районах с большой влажностью, где ожидается много льда и снега. Обычно для стандартного кожуха достаточно мощности подогревателя 10 Вт. Нагреватели могут работать от источников электропитания 12 В постоянного тока, 24 В переменного тока или даже от сети 220 В. В

районах с высокими температурами следует использовать вентиляторы кожухов, их можно комбинировать с подогревателями. Источник электропитания для вентилятора может быть либо переменного, либо постоянного тока. Следует выбирать вентиляторы хорошего качества, так как вентиляторы постоянного тока рано или поздно приведут к возникновению искр от вращения щеток, наводящих помехи на видеосигнал.

Если в систему необходимо добавить устройство омыватель/очиститель, то потребуется специальный кожух. Специальный – потому что потребуется согласование между механизмом очистителя и окном кожуха. Следует отметить, что в случае использования такого устройства приемник сигналов телеуправления должен иметь выход для управления этими функциями. Другая проблема при использовании омывателя – всегда нужно проверять, что в емкости омывателя имеется достаточное количество воды.

Большинство кожухов хорошо защищены от воздействия окружающей среды, но для некоторых специализированных систем может потребоваться еще более сильная защита. Системы, которые могут подвергнуться нежелательному вмешательству человека или механизмов, нуждаются в вандало-защищенных кожухах; в этом случае необходимо использовать специальное, небьющееся стекло (пример изображен на рис. 4.20). Для дополнительной безопасности в систему могут быть добавлены датчики несанкционированного вскрытия кожухов. В таком случае сигнал тревоги при вскрытии кожуха поступает на пульт охраны.

Также существуют пуленепробиваемые, взрывостойкие и подводные кожухи, но это редкие, специально разрабатываемые и очень дорогие приспособления. Как уже было отмечено ранее, существуют кожухи, защищающие телевизионные камеры от радиации. Повышенный радиационный фон приводит к выгоранию ПЗС-матрицы. Постепенно изображение становится зернистым («снег» по изображению) и со временем может совсем пропасть.

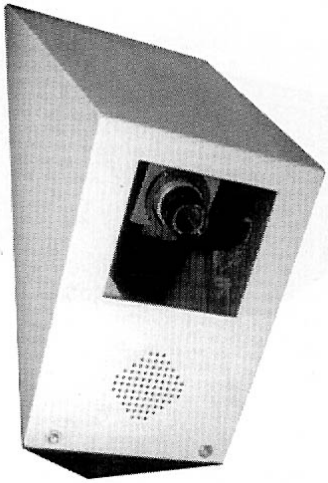


Рис. 4.20. Вандало-защищенный кожух телекамеры

Поворотные устройства телевизионных камер

При проектировании СТН необходимо определить, какие телевизионные камеры будут установлены фиксировано, а какие должны будут двигаться/поворачиваться при оценке обстановки на охраняемом объекте.

Фиксированные ТК устанавливаются на кронштейне, при этом используются объективы с фиксированным фокусным расстоянием.

Альтернативой фиксированным ТК являются телекамеры на поворотных устройствах, с помощью которых можно изменять поле зрения ТК. Такие телевизионные камеры размещаются на поворачивающейся в двух плоскостях платформе, при этом обычно используются объективы с переменным фокусным расстоянием.

Типичные поворотные устройства представлены на рис. 4.21.

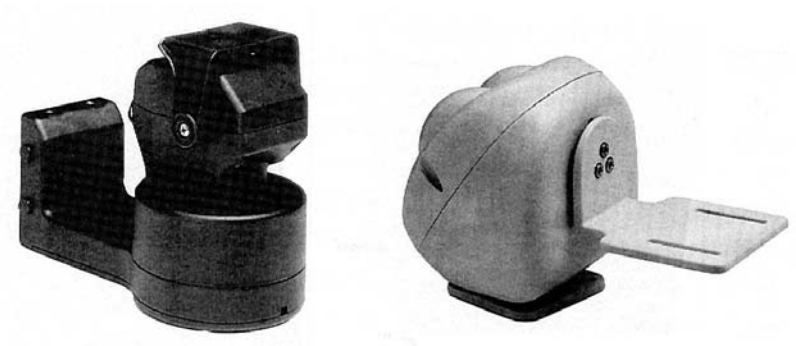


Рис. 4.21. Поворотные устройства телекамер СТН

Существуют поворотные устройства с верхним расположением поворотной платформы и с боковой платформой. Они отличаются по величине номинальной нагрузки, которая зависит от центра тяжести нагрузки. В случае поворотных устройств с боковыми платформами центр тяжести располагается ниже; это означает, что из двух типов устройств (при одинаковых электродвигателях и вращающем моменте) боковая платформа имеет большую номинальную нагрузку [4.4].

С точки зрения применения, можно выделить два типа поворотных устройств:

- наружные (используемые вне помещений);
- внутренние (используемые внутри помещений).

Наружные поворотные устройства делятся на три категории:

- большой нагрузки (нагрузка выше 35 кг);
- средней нагрузки (нагрузка 10–35 кг);
- малой нагрузки (нагрузка до 10 кг).

Наружные поворотные устройства устойчивы к погодным воздействиям, они тяжелее и прочнее — на них устанавливается тяже-

лый кожух, в котором могут стоять дополнительные устройства, такие как блок подогрева и вентиляции, стеклоочиститель и устройство искусственной подсветки.

Внутренние поворотные устройства обычно меньше и легче, в большинстве случаев они попадают в третью категорию, т.е. могут нести не более нескольких килограммов. Поэтому внутренние поворотные устройства часто изготавливают из литой пластмассы, и выглядят они более эстетично, чем уличные [6.4].

В большинстве случаев поворотным устройством управляют синхронные электродвигатели переменного тока напряжением 24 В. Бывают поворотные устройства с питанием от электросети (220/240 В или 110 В переменного тока), но более популярны устройства 24 В из-за фактора безопасности (напряжение меньше 50 В переменного тока для человека безопасно).

Разновидностью поворотных устройств являются так называемые купольные поворотные устройства или даже купольные поворотные телекамеры (купольные телекамеры). На рис. 4.22 представлен внешний вид купольной ТК (в кожухе) и ее «внутренности» (телекамера, объектив, поворотный механизм).

Они работают так же, как и обычные поворотные устройства, но внутри куполов находятся и механизм поворотного устройства, и управляющая электроника. Заключенные в прозрачные или полупрозрачные сферы или полусферы, такие устройства выглядят вполне приемлемо даже в интерьерах, требующих эстетического подхода.

Сегодня, когда размеры и масса телекамер уменьшаются, происходит миниатюризация трансфокаторов и, соответственно, кожухов и поворотных устройств.

В связи с миниатюризацией телекамер и объективов, поворотные купола тоже становятся меньше в диаметре. Сегодня купольные телекамеры имеют 200–300 мм в диаметре. Закрывающие телекамеру сферы могут быть прозрачными или нейтрально-серыми

(тонированными). Часто невозможно понять, куда направлена ТК, и это является одной из самых важных особенностей скоростных поворотных телекамер [4.4].

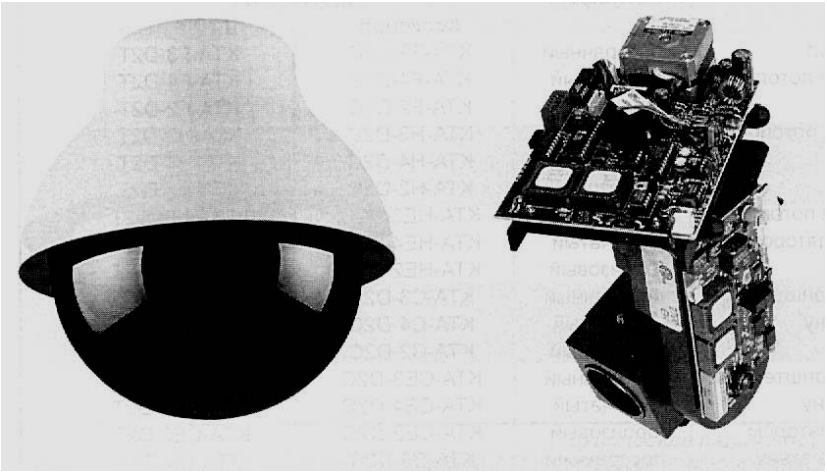


Рис. 4.22. Скоростная поворотная телекамера, содержащая телекамеру, объектив с автоматической фокусировкой и переменным фокусным расстоянием, поворотный механизм и приемник сигналов удаленного управления

4.9. Особенности выбора и применения средств телевизионного наблюдения

Выбирая ТК, следует четко понимать задачи и цели создаваемой СТН. Первым делом следует определить зоны, которые необходимо контролировать с помощью СТН, т.е. зоны видеоконтроля. Чаще всего, этими зонами являются места наиболее вероятного совершения преступления и места сосредоточения ценностей. Зон видеоконтроля может быть сколько угодно: от одной-двух (например, главный вход) до нескольких десятков или сотен. Таким образом, необходимо определить количество телекамер в системе и требования к ним. Только выбрав телекамеры, следует переходить

к подбору вспомогательного оборудования (средств обработки видеоинформации, ее отображения, протоколирования и т.д.).

После определения количества телекамер необходимо решить, черно-белые или цветные ТК следует применять. Цветные телекамеры позволяют получить более информативное изображение, чем черно-белые, однако они обладают худшей чувствительностью, разрешающей способностью (хотя есть и цветные телекамеры высокого разрешения). Выбор цветной телекамеры повлечет за собой соответствующий выбор всего остального оборудования обработки, записи и отображения видеоинформации.

При решении задач общего наблюдения достаточно использовать ТК обычного разрешения, а при необходимости идентификации или наблюдения на большом расстоянии рекомендуется выбирать ТК повышенного и высокого разрешения.

Требуемая чувствительность ТК устанавливается при обследовании объекта, причем необходимо определить освещенность на объекте не только в дневное, но и в ночное время и при необходимости решить вопрос о наличии дежурного освещения или инфракрасной подсветки. При определении чувствительности можно воспользоваться следующим алгоритмом:

- с помощью люксметра (или другим способом) измеряется освещенность в зоне контроля охраняемого объекта;
- определяется значение коэффициента отражения реального объекта контроля (см. табл. 4.2);
- определяется коэффициент прохождения по указанной в описании светосиле выбранного объектива (табл. 4.5);
- рассчитывается минимальная освещенность на датчике изображения $E_{\text{ПЗС}}$, которая может быть получена в зоне контроля телекамеры по формуле:

$$E_{\text{ПЗС}} = E_{\text{объекта}} * R * K,$$

где $E_{ПЗС}$ – освещенность на датчике изображения (ПЗС-матрице); $E_{объекта}$ – освещенность в зоне контроля ТК; R – коэффициент отражения объекта контроля; K – коэффициент прохождения.

Таблица 4.5. Характеристики объективов

Светосила объектива	***Относительное отверстие***	***Коэффициент прохождения***
F 0,8	1:0,8	0,31
F 0,95	1:0,95	0,2
F 1,2	1:1,2	0,14
F 1,4	1:1,4	0,1
F 2	1:2	0,05
F 2,8	1:2,8	0,025
F 4	1:4	0,0125
F 5,6	1:5,6	0,00625
F 8	1:8	0,003125

Полученный результат (освещенность датчика изображения) должен быть выше чувствительности ТК. Если это не так, то стоит подумать об организации дежурного освещения в зоне видеоконтроля, либо выбрать более чувствительную телевизионную камеру.

Если диапазона действия электронного затвора недостаточно для компенсации чрезмерной освещенности, можно использовать объективы с автоматической диафрагмой. Однако следует обратить внимание на совместимость телекамеры и объектива по способу управления автоматической диафрагмой.

Если нет специальных требований (например, Госпожарнадзора) по применению на объекте оборудования с низким напряжением питания или других ограничений, то рекомендуется применять ТК с напряжением питания 220 В. Такие ТК удобно синхронизировать по сети питания, в этом случае нет необходимости в дополнительном оборудовании типа синхрогенераторов или дополнитель-

ного кабеля для сигнала синхронизации. Также надо следить за тем, чтобы источник питания обеспечивал требуемую мощность (особенно при питании нескольких телекамер от одного источника). Необходимо также решить вопрос о возможности работы системы при отключении основного напряжения питания, т.е. обеспечить резервное электропитание.

Поворотные устройства находят широкое применение в СТН для использования как на улице, так и в помещении. Но при расположении ТК на поворотном устройстве следует обратить внимание на соответствие скорости сканирования поворотного устройства скорости перемещения контролируемого объекта (возможно, что поворотное устройство не будет успевать отслеживать перемещение объекта контроля). В большинстве случаев более выгодно поставить несколько ТК с фиксированным положением и углом зрения, чем одну, расположенную на поворотном устройстве.

Не все ТК могут работать при инфракрасном свете. Характеристики цветных ТК отвечают характеристикам человеческого зрения, а большинство черно-белых ТК используют часть красной и инфракрасную область. Поэтому при выборе телекамеры для конкретного объекта необходимо учитывать тип источника света и спектральную характеристику датчика изображения ТК (ПЗС-матрицы).

При построении СТН главным условием является то, что все выбранное для систем оборудование должно быть одного стандарта видеосигнала.

В заключение данной главы необходимо отметить, что параметр «разрешение» имеет отношение не только к ПЗС-матрице на телевизионной камере, но и ко всем цифровым приборам: мультиплексорам, квадраторам, цифровым синхронизаторам и так далее. Они также ограничивают общее разрешение системы телевизионного наблюдения.

Вопросы для самоконтроля

1. Назовите основные компоненты СТН, их характеристики.
2. Опишите состав телевизионной камеры и основные технические характеристики телевизионной камеры.
3. Объясните необходимость синхронизации и методы синхронизации компонентов СТН.
4. Какие существуют методы интеграции подсистем обнаружения и КУД с подсистемой телевизионного наблюдения?
5. Какие существуют методы передачи видеоинформации? Объясните особенности применения тех или иных методов передачи видеоинформации.
6. Какие существуют возможности и преимущества использования волоконно-оптических линий связи в СТН?
7. Какие устройства относятся к коммутирующему оборудованию СТН: примеры оборудования, основные характеристики?
8. Объясните принцип построения интегрированных систем безопасности на базе видеомультиплексора.
9. Какие функции выполняет видеомультиплексор?
10. Какие существуют особенности построения «сети» СТН на базе мультиплексоров? Опишите пример построения «сети» СТН.
11. Какие предъявляются требования по применению и установке телевизионных камер?
12. Какие существуют методы хранения видеоинформации в СТН?
13. Какими преимуществами обладают цифровые системы архивации и хранения видеоинформации?
14. Какие функции выполняют защитные кожухи телевизионных камер?
15. Какие существуют устройства позиционирования телевизионных камер?

5. ПОДСИСТЕМА СБОРА И ОБРАБОТКИ ДАННЫХ

Подсистема (далее – система) сбора и обработки данных обеспечивает передачу сигналов тревоги, вырабатываемых датчиками обнаружения, и выводит информацию на панель индикации. В зависимости от характера этой информации оператор предпринимает те или иные действия.

В данной главе будут рассмотрены возможности и характеристики аппаратуры сбора информации от средств обнаружения (СО), различные методы сбора и обработки информации, аппаратура тревожного оповещения, технологии передачи данных, методы контроля за состоянием линии связи СО, оборудование станции сбора и обработки данных [П.2, 5.1, 5.2].

При создании системы сбора и обработки информации СФЗ необходимо определить: какого рода информация будет выводиться на автоматизированное рабочее место (АРМ) оператора системы, каким образом будет представлена эта информация, каким образом оператор будет взаимодействовать с системой, и каким образом должно быть расположено оборудование АРМ оператора.

5.1. Назначение подсистемы сбора и обработки данных

Функция подсистемы сбора и обработки данных состоит в том, чтобы передавать сигналы, поступающие от датчиков обнаружения нарушения на объекте, и представлять эту информацию оператору системы в удобном и наглядном виде.

В целом можно говорить о том, что во всех системах сбора информации используются простые контактные устройства, например, реле, устанавливаемые на дверях и позволяющие обнаруживать проникновение в помещение. Поступающий от реле сигнал тревоги передается к какому-либо оповещающему устройству. Ранее широко применялись панели для отображения информации (индикаторные

панели), оборудованные световыми индикаторами. Каждый из индикаторов подсоединен к определенному датчику на объекте. Такое оборудование обладает определенными преимуществами: обращение с простыми электрическими компонентами не требует специальной подготовки эксплуатирующего персонала, система не требует сложного технического обслуживания. Простые панели на световых индикаторах имеют и недостатки: их стоимость может быть очень высокой, так как для каждой зоны наблюдения используется отдельная линия связи; на большом объекте потребуется много места для расположения всех индикаторных панелей, и световые индикаторы предоставляют лишь ограниченное количество информации.

На протяжении прошедшего десятилетия были разработаны многие сложные системы, используемые в целях сбора, обработки и представления тревожной информации. К их числу относятся: системы аварийной связи, средства оповещения, управляемые компьютерами, и системы телевизионного наблюдения для оценки тревожной ситуации. Каждая из перечисленных систем выполняет определенные задачи обеспечения физической защиты объекта. Но если каждая из подсистем используется автономно, то существует опасность, что центральный пульт оператора СФЗ превратится в нагромождение оборудования, обращение с которым затруднительно и требует большого опыта. Автономные подсистемы оповещения могут оказаться бесполезными в кризисной ситуации, если большой объем информации поступает настолько быстро, что оператор не успевает отреагировать.

Эффективное использование новых технологий требует интегрирования всех подсистем СФЗ в единую интегрированную и координированную систему. Например, поступающие от датчиков данные могут обрабатываться перед тем, как они передаются к индикаторной панели, в соответствии с установленным порядком очередности действий оператора. Изображения, передаваемые телекамерами,

могут автоматически отбираться в соответствии с поступающими на пульт оператора сигналами тревоги.

Подсистема сбора и обработки информации играет важную роль в процессе успешного принятия мер в ответ на возникновение угрозы. Система обеспечивает управление потоком информации, которой обмениваются системы обнаружения проникновения, оценки аварийной ситуации, задержки продвижения и развертывания ответных действий.

Для эффективной подсистемы сбора и обработки информации характерны: быстрое реагирование, наблюдение за состоянием всех линий связи, простота и быстрота обнаружения неисправностей в отдельных точках системы, наблюдение за состоянием датчиков и возможность расширения системы.

Система сбора и обработки информации осуществляет сбор данных от технических средств СФЗ на объекте, представляет информацию оператору от системы телевизионного наблюдения и дает оператору возможность вводить команды управления на средства тревожного оповещения. Конечное предназначение системы сбора и обработки информации состоит в том, чтобы содействовать оперативной оценке ситуации на объекте с обнаружением причин подачи сигнала тревоги. Ниже будут рассмотрены устройства оповещения, взаимосвязь средств оповещения и средств телевизионного наблюдения, а также требования и рекомендации по их размещению на АРМ оператора СФЗ объекта. На рис. 5.1 приведено изображение типичного пульта управления СФЗ.

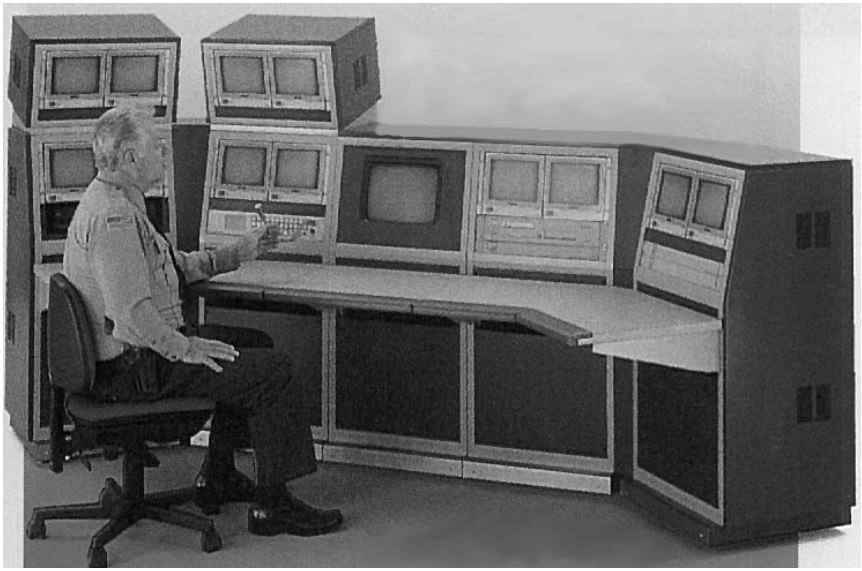


Рис. 5.1. Пульт системы сбора и обработки информации

5.2. Аппаратура сбора информации со средств обнаружения – контрольные панели

Современные системы физической защиты представляют собой совокупность совместно действующих технических средств обнаружения признаков появления несанкционированного проникновения нарушителя на защищаемый объект и (или) пожара на них, передачи, сбора, обработки и предоставления информации в заданном виде оператору системы. Сбор, обработку и частично представление информации выполняет аппаратура сбора информации от средств обнаружения, эти устройства также называются контрольными панелями (КП) (рис. 5.2). Номенклатура КП сегодня обширна, и их основные характеристики и возможности будут рассмотрены ниже.

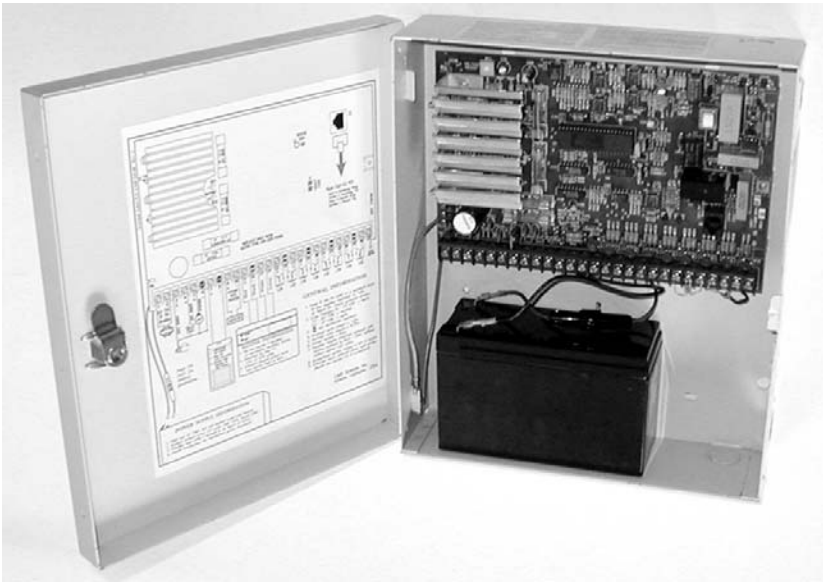


Рис. 5.2. Вид контрольной панели

Приемно-контрольные приборы (проще – контрольные панели) служат для приема сигналов от средств обнаружения, обработки их и передачи в удобном виде либо на центральный пульт управления (ЦПУ), либо на другую КП [5.1].

В зависимости от назначения КП для СФЗ подразделяются на охранные, охранно-пожарные, панели систем контроля и управления доступом (КУД) и комбинированные. Основными функциями КП являются:

- прием информации о состоянии СО и целостности линии связи (шлейфе сигнализации);
- запоминание и обработка принятой информации;
- управление световым и звуковым оповещателями;
- формирование и передача сигналов на центральный пункт управления или другую КП;

- обеспечение электропитания СО по шлейфу сигнализации (ШС) или по отдельной линии;
- обеспечение процедур взятия под охрану и снятия объекта с охраны.

Следует отметить, что не все контрольные панели выполняют полный набор перечисленных функций.

К дополнительным функциям КП относятся:

- возможность отключения отдельных ШС;
- программирование режимов работы КП и отдельных ШС;
- переключение ШС на прямой контроль системой передачи извещений при пропадании питания КП;
- самодиагностирование неисправностей функциональных узлов КП;
- встроенная и (или) выносная индикация режимов работы КП и состояния ШС.

Важными характеристиками контрольных панелей являются информативность, т.е. количество видов извещений (сигналов), отображаемых КП и передаваемых на ЦПУ, и информационная емкость, т.е. количество контролируемых ШС [5.1].

По информационной емкости КП подразделяют на:

- малой информационной емкости – до 5 шлейфов сигнализации;
- средней информационной емкости – от 6 до 50 шлейфов сигнализации;
- большой информационной емкости – свыше 50 шлейфов сигнализации.

На современном этапе развития средств ФЗ характерно модульное построение КП, а также фирменный подход, при котором разрабатываются и производятся серии приборов различной информационной емкости (например, «Аккорд», «ADEMCO», «Сигнал», «Аргус» и др.). Это позволяет комплектовать систему физической защи-

ты для различных объектов изделиями одной фирмы, что удобно для проектирующих и монтажных организаций.

По информативности КП подразделяют на:

- малой информативности – система контролирует до двух состояний ШС;
- средней информативности – от 3 до 5 состояний ШС;
- большой информативности – свыше 5 состояний ШС.

Повышение информативности – одно из главных направлений совершенствования КП. Контрольные панели ранних разработок имели, как правило, информативность, равную двум – состояния ШС «норма» и «тревога». Последние разработки позволяют передавать такие сигналы, как «норма», «неисправность», «проникновение», «пожар», «нападение» и др.

Основные элементы любой КП – это основная плата электроники и блок питания (БП), которые заключены в единый корпус. Типичный состав КП представлен на рис. 5.3.

На основной плате располагаются: процессор, модуль памяти (на рис. 5.3 это модуль управления), электроника БП (если это не отдельная плата), контакты для подключения СО, клавиатур управления, клавиатур и считывателей доступа, исполнительных устройств; защитная электроника (реле, предохранители), разъемы для подключения различных плат расширения и т.д. Блоки питания некоторых КП рассчитаны на организацию питания СО и считывателей.

В системах централизованной охраны контакты сигнальных реле КП подключаются к оконечным устройствам систем передачи извещений (СПИ), с помощью которых информация передается в ЦПУ по радиоканалу или, чаще всего, по проводным каналам связи, в качестве которых используются выделенные или занятые телефонные линии либо специальные линии. В некоторых КП предусмотрен узел переключения ШС на контроль непосредственно системой передачи

извещений при пропадании питания прибора. В последние годы получили распространение КП, питающиеся от линии ЦПУ.

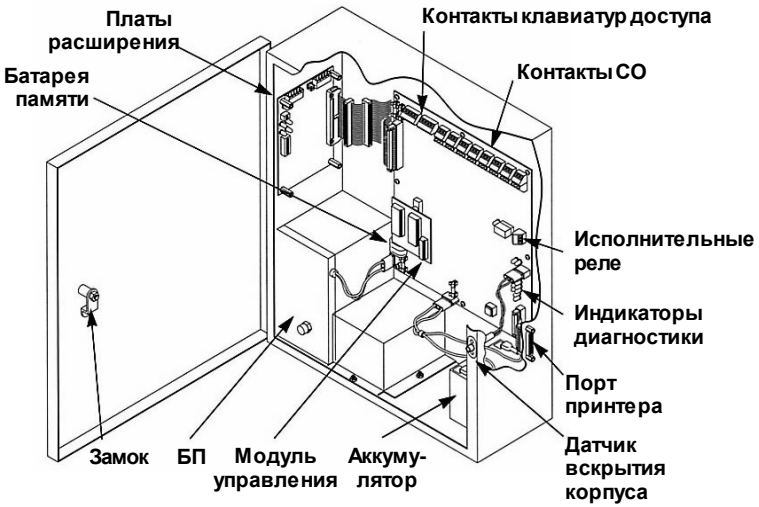


Рис. 5.3. Типичный состав контрольной панели

Выходы сигнальных реле нескольких КП могут подключаться к другой (объединяющей) КП. В автономных системах такая схема используется в основном для уменьшения количества оповещателей, а в системах централизованной охраны – из-за ограниченного количества линий связи с ЦПУ.

Область применения контрольных панелей

Одношлейфные КП в основном применяются для организации физической защиты одного помещения или небольшого объекта. Если на объекте нужно организовать не только шлейфы СО, но и

шлейфы пожарной и/или тревожной сигнализации, то для этих целей используются отдельные КП, работающие круглосуточно.

Контрольные панели с несколькими контролируемыми ШС используются для охраны небольших объектов или для организации многорубежной охраны. Эти приборы находят широкое применение, так как в своем большинстве позволяют одновременно контролировать охранные ШС в режиме «с правом отключения», а шлейфы пожарной и (или) тревожной сигнализации – в режиме «без права отключения» (круглосуточная работа). При этом в зависимости от предъявляемых требований назначение ШС и алгоритм работы прибора могут изменяться с помощью набора перемычек или программным путем.

Контрольные панели средней и большой информационной емкости применяются для физической защиты больших объектов и могут использоваться для объединения информации, приходящей из различных охраняемых зон, с целью передачи ее на ЦПУ, а также для управления в системах автономной сигнализации. Эти приборы также позволяют контролировать шлейфы пожарной и тревожной сигнализации.

Для отдельных видов объектов существуют также специальные типы КП, например: для охраны квартир, пожаро- и взрывоопасных помещений. Существуют контрольные панели, которые предназначены для эксплуатации в неотапливаемых помещениях.

Требования к монтажу контрольных панелей

Установка КП должна производиться в специально выделенном помещении (например, в служебном помещении или помещении внутренней охраны объекта), где КП защищена от механических повреждений и несанкционированного доступа посторонних лиц. Панели, имеющие настенное исполнение, устанавливаются на стене, на высоте не менее 1,5 м от уровня пола. Панели, выполненные в на-

стольно-настенном варианте, устанавливаются на столах или на других устойчивых горизонтальных поверхностях либо крепятся на стене, на высоте, обеспечивающей удобство доступа к органам управления.

При отсутствии специально выделенного помещения, КП устанавливаются на стенах на высоте не менее 2,2 м от уровня пола либо в металлических запираемых шкафах на высоте, удобной для технического обслуживания.

Не допускается установка приборов в сгораемых шкафах, а также на расстоянии менее 1 м от отопительных систем. Металлические корпуса приборов должны быть обязательно заземлены.

Подключение внешних цепей производится с помощью соединительных колодок, имеющихся в приборе.

Внешние световой и звуковой оповещатели должны устанавливаться в местах, удобных для визуального и слухового контроля. Рекомендуемая электрическая мощность оповещателей 25 Вт.

Не допускается производить разводку проводов шлейфов сигнализации и пультовых линий вблизи силовых электрических проводов и кабелей (в том числе и линий подключения оповещателей к КП). При прокладке шлейфов сигнализации и пультовых линий параллельно силовым цепям, расстояние между ними должно быть не менее 50 см, а их пересечение должно производиться под прямым углом.

Выносные элементы КП («шунтирующее» сопротивление) должны устанавливаться в конце ШС, скрытно, в местах, не доступных для посторонних лиц.

Запрещается монтаж ШС, а также его отдельных участков в виде наружных воздушных линий.

Ниже приведены характеристики и возможности одной КП. В лабораторном практикуме [5.2] можно ознакомиться более подробно с возможностями еще нескольких КП.

Контрольные панели большой информационной емкости

Контрольная панель Vista-101 фирмы ADEMCO (США) предназначена для организации автономной физической защиты средних и крупных объектов с возможностью передачи на ЦПУ обобщенных сигналов тревоги по четырем независимым выходам. Максимальное количество защищаемых зон (шлейфов сигнализации) – 36.

Изменяемая конфигурация прибора позволяет организовать:

- 6 радиальных проводных зон (шлейфов сигнализации). При использовании расширителя к ним можно добавить еще 8 проводных зон, доведя их количество до 14;
- до 30 программируемых зон с помощью адресуемых средств обнаружения или модулей расширителей по радиоканалу.

В КП Vista-101 реализованы следующие функции и режимы работы:

- резервирование основного питания;
- автоматизированная постановка объектов под охрану и снятие с охраны;
- автоматическая регистрация сообщений о состоянии объектов и служебной информации на цифропечатающем устройстве;
- антисаботажная защита;
- поддержка двух информационных телефонных каналов для связи с центральной станцией либо ЦПУ;
- программирование назначения и параметров ШС в зависимости от специфики объекта с помощью пульта управления или дистанционно по линии связи с помощью ЭВМ;
- сохранение запрограммированной конфигурации прибора при длительном отключении напряжения питания (энергонезависимая память);

- возможность группирования охраняемых зон в шесть независимых разделов с разными уровнями и персональными кодами доступа;
- отображение тревожной и служебной информации на жидкокристаллическом дисплее пульта управления;
- управление прибором с собственного пульта управления и/или с помощью клавиатуры по радиоканалу.

В ШС допускается включать охранные и пожарные извещатели фирмы ADEMCO либо их отечественные аналоги.

В состав системы на базе контрольной панели Vista-101 входят:

1) Адресуемые устройства, работающие по проводному каналу связи:
   - пульт управления и индикации установщика и пользователя;
   - релейный модуль на 4 реле;
   - расширитель на 8 ШС и 2 адресуемых выходных реле.
2) Адресуемые устройства, работающие по радиоканалу:
   - пульт управления и индикации пользователя двунаправленный;
   - пульты управления пользователя: 3-кнопочный; 12-клавишный;
   - радиоприемники: на 8 зон; на 16 зон; на 64 зоны (используется при организации более 16 радиозон);
   - радиопередатчик для работы с пультом управления и индикации;
   - детекторы: тревожный однокнопочный; охранный двухзонный; охранный трехзонный; охранный объемный оптико-электронный; пожарный дымовой оптико-электронный.
3) Оповещатели:
   - звуковой;
   - световой с красным светофильтром.

5.3. Технологии передачи данных от систем обнаружения

Основным критерием выбора оборудования для передачи информации от датчиков обнаружения на охраняемом объекте является географическое расположение датчиков (извещателей). Оптимальный метод передачи информации от датчиков обнаружения определяется их расположением на объекте.

Передача данных по схеме звезда

При передаче данных от датчиков обнаружения по схеме звезда используются отдельные проводные линии для каждого датчика (рис. 5.4). Если аппаратура сбора информации со средств обнаружения находится в центре охраняемой территории, то применяется данный метод передачи информации.

В такой схеме подключения каждая линия связи функционирует независимо и может прокладываться до аппаратуры сбора информации любым удобным маршрутом. Преимущество подключения датчиков по схеме «звезда» заключается в том, что при неисправности/обрыве одной линии связи вся остальная часть системы функционирует нормально. А из недостатков необходимо отметить то, что установка такой системы требует прокладки большого количества кабелей, и диапазон возможности расширения системы ограничен, если только не подключать на одну линию связи несколько датчиков, что приведет к уменьшению информативности системы.

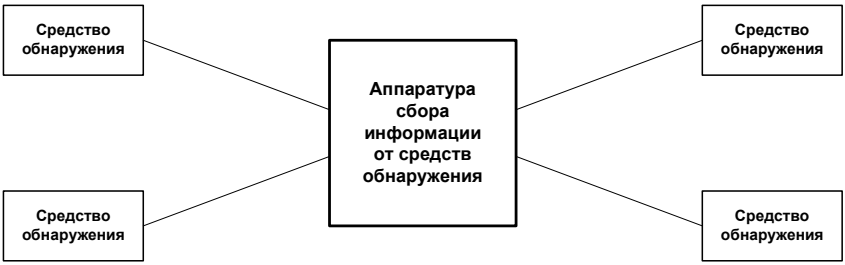


Рис. 5.4. Передача данных по схеме «звезда»

Передача данных по уплотненным линиям связи

Это система, в которой сигналы от нескольких датчиков передаются по одной линии связи (рис. 5.5). Также подобные системы еще называют системами с мультиплексной шиной. Уплотнение линии связи позволяет снизить стоимость систем.

Существует несколько методов уплотнения линий связи. Основное различие между этими методами состоит в том, каким образом осуществляется разделение каналов связи. Ниже рассматриваются преимущества и недостатки четырех методов уплотнения линий связи.

Уплотнение линий связи с временным разделением (временная модуляция). При использовании этого метода сигналы от различных датчиков обнаружения передаются по одному кабелю через определенные интервалы времени. Проблема идентификации датчиков решается путем выделения каждому из датчиков определенного промежутка времени. Недостаток такой системы заключается в том, что каждый сигнал должен ждать своей очереди. Например, сигнал тревоги от датчика не может мгновенно поступить на аппаратуру сбора информации. Основной характеристикой системы с временным разделением каналов связи является период синхронизации, т.е. количество времени, необходимое для передачи сигнала каждым из датчиков системы. Продолжительность периода синхронизации ог-

раничивается количеством датчиков обнаружения на одной линии связи, скоростью реагирования линии связи на изменения сигналов в линии.

Рис. 5.5. Система с передачей данных по уплотненной линии связи (система с мультиплексной шиной)

Уплотнение линии связи с частотным разделением (частотная модуляция). Уплотнение с частотным разделением каналов связи позволяет нескольким датчикам передавать сигналы по общей линии связи с выделением каждому датчику определенной полосы частот. Сигнал в линии связи позволяет идентифицировать датчик по частоте. При использовании подобной мультиплексной шины возникает проблема наложения двух и более сигналов, что может привести к полной потере важных сигналов от датчиков обнаружения. Решается эта проблема следующим образом. Сигналы от датчиков несколько раз дублируются через малый случайный интервал времени. Частотное разделение каналов связи позволяет избежать возникно-

вения проблем с запаздыванием сигналов и регулированием синхронизации, которые характерны для систем с временным разделением каналов.

Уплотнение с опросом. При уплотнении с опросом расположенное в центре системы устройство управляет использованием разделенных каналов связи, опрашивая датчики и определяя, передает ли какой-либо из них сигнал тревоги. Любой датчик может передать сигнал тревоги по линии связи только после того, как он будет опрошен центральным управляющим устройством. Если опрос датчиков производится последовательно, характеристики системы становятся сходными с характеристиками системы с временным разделением каналов связи. Характеристиками таких систем являются: максимальное время задержки подачи сигнала тревоги; максимальное количество датчиков, которые могут быть подсоединены к системе.

Уплотнение линии связи с кодированием сигналов (кодовая модуляция). Данный метод заключается в том, что каждому подключенному к линии связи устройству присваивается идентификационный номер. Для этого на каждом датчике имеется двухразрядный переключатель. В простейшем случае в линию связи от датчика обнаружения поступает сигнал в двоичном коде, который содержит номер датчика в линии и код его состояния (тревога, вскрытие и другие). Проблема наложения двух и более сигналов здесь решается так же, как при частотной модуляции. Данный метод наиболее широко применяется в современной аппаратуре охраны.

Уплотнение линий связи часто является экономичным методом передачи информации, даже если система содержит лишь несколько датчиков обнаружения, находящихся недалеко от пункта управления. Уплотнение линий связи позволяет повысить уровень секретности линии связи, так как затрудняет задачу нарушителя, пытающегося нейтрализовать датчик обнаружения. Системы с уплотнением линии связи могут иметь сложную конфигурацию; для ремонта оборудования и технического обслуживания таких систем требуются бо-

лее опытные технические специалисты, чем для ремонта и техобслуживания систем с прямой передачей данных.

Существенным недостатком систем с уплотнением линий связи является использование единого канала связи (мультиплексной шины). Неисправность уплотненной линии связи выводит из строя все датчики, подсоединенные к этой линии. Следует отметить, что и в системах без уплотнения линий связи, в случаях, когда провода, подсоединенные к нескольким датчикам, составляют один кабель или прокладываются по одному кабелепроводу, прерывание кабеля также вызовет отключение всех подсоединенных к нему датчиков обнаружения. С целью уменьшения вероятности случайного повреждения линий связи, их прокладывают в металлических трубах, металлических рукавах или специальных гофрированных пластиковых трубках. Там, где необходима высокая надежность линии связи, иногда необходимо прокладывать отдельный кабель к каждому из датчиков, чтобы снизить вероятность отключения целой группы датчиков.

Дублирование линий связи может способствовать повышению надежности системы связи. Одним из методов дублирования уплотненных линий связи является создание замкнутых (или кольцевых) контуров связи. При этом оба конца линии связи подключаются к аппаратуре сбора информации таким образом, что передача данных может осуществляться в обоих направлениях. Замкнутый контур обеспечивает существование двух линий связи для каждого датчика.

Передача данных по радиоканалу

В некоторых случаях становится нецелесообразно (по эстетическим или экономическим причинам) протягивать кабельные линии связи к каждому датчику обнаружения. Существует аппаратура, которая позволяет принимать информацию от датчиков обнаружения по радиоканалу. В этом случае в состав аппаратуры сбора информации входит радиоприемник, который принимает информацию с дат-

чиков на объекте; и каждый датчик подключен к радиопередатчику, который модулирует соответствующим образом поступающую на него информацию с датчика обнаружения.

Если рассматривать характеристики систем охраны, использующих для передачи информации радиоканал, то эти системы очень похожи на системы с уплотнением линии связи. При передаче информации по радиоканалу используются те же методы уплотнения (разделения) линии связи: временная модуляция сигнала, частотная модуляция и кодовая. Для уплотнения радиоканала методом опроса датчиков необходимо применение и приемника, и передатчика как составной части аппаратуры сбора информации, а также и передатчика, и приемника, подключенных к датчику обнаружения. Последний метод разделения каналов связи существенно увеличивает стоимость оборудования.

Современная аппаратура сбора информации позволяет использовать для связи с датчиками сразу все три известные линии связи. Например, существуют системы фирмы ADEMCO, к которым возможно подключить мультиплексную шину с кодовой модуляцией, радиоприемник (тоже кодовая модуляция сигналов датчиков) и прямые линии связи (6, 8, 12, 16 датчиков обнаружения). Необходимо также понимать, что для использования мультиплексной шины передачи информации с кодовой модуляцией нужны датчики обнаружения, поддерживающие данную технологию, или специальные согласующие устройства. Также для использования радиоканала применяются датчики обнаружения, в состав которых уже входит радиопередатчик (датчик и передатчик в одном корпусе), или отдельный согласующий радиопередатчик.

5.4. Контроль линии между контрольной панелью и средствами обнаружения

Обеспечение надежности связи

Система тревожного оповещения не может считаться эффективной, если случайное или намеренное повреждение линии связи приводит к невозможности передачи сигнала тревоги от датчика к станции наблюдения.

Используются несколько различных методов физической защиты в целях предотвращения или задержки доступа к линиям связи.

Один из методов защиты заключается в прокладке линий связи в металлических кабелепроводах. Если соединения таких кабелепроводов надежно сварены, уровень надежности повышается. Серьезную опасность кабельным линиям связи также представляют мелкие грызуны и другие животные. Металлические кабелепроводы и специальные пластиковые гофрированные трубки позволяют решить и эту проблему.

Другой метод защиты линий связи заключается в прокладке линий связи под землей. Для передачи информации на большие расстояния этот метод может оказаться дорогостоящим. При прокладке подземных кабелей необходимо предусматривать дополнительные линии связи на случай расширения системы.

Контроль состояния линии связи

С целью обеспечения надлежащего эксплуатационного состояния кабеля и предотвращения изменения данных в процессе их передачи осуществляется контроль состояния линии связи на всей ее протяженности.

Линии связи датчиков обнаружения и аппаратуры сбора информации подразделяются на две категории – пассивные и активные. По

пассивным линиям информация передается после вырабатывания сигнала тревоги. Прерывание пассивной линии связи сделает передачу сигналов тревоги невозможной, и обрыв линии нельзя будет обнаружить без проведения специальных испытаний. По активным линиям связи информация передается непрерывно, что позволяет немедленно обнаружить обрыв линии.

Некоторые методы передачи информации обеспечивают самозащиту линии связи, так как такие линии связи исключают возможность модификации передаваемой информации. Пример самозащищенной линии связи – волоконно-оптический кабель. Необходимо обратить внимание еще на одно преимущество волоконно-оптического кабеля – в линиях оптической связи не возникают ложные сигналы тревоги, вызываемые интерференцией электромагнитного поля, помехами от других линий связи или молниями.

Система контроля состояния линии связи может быть статической или динамической. В статических системах безопасное состояние линии связи определяется посредством передачи одного и того же сигнала. Характеристики этого служебного сигнала можно идентифицировать и дублировать.

В динамических системах контроля линии связи генерируется постоянно изменяющийся сигнал, оповещающий о состоянии линии связи. Определение характеристик сигнала и нейтрализация системы посредством передачи ложного сигнала в этом случае является трудной задачей для потенциального нарушителя.

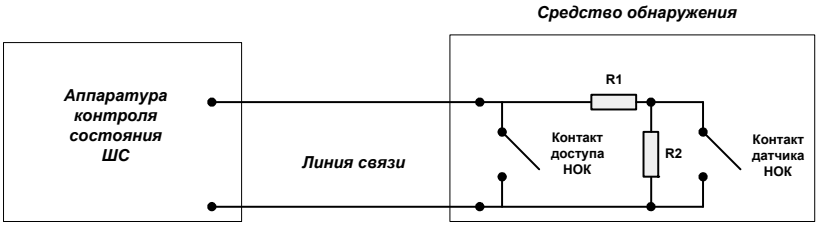
Ниже рассматриваются наиболее широко применяемые статические системы контроля состояния линии связи.

Контроль с подачей постоянного тока. В системах наблюдения за состоянием линий связи с подачей постоянного тока по проводам непрерывно протекает ток определенной силы. Аварийное состояние линии связи соответствует замкнутому или разомкнутому состоянию схемы наблюдения либо изменению значения силы протекающего тока. Любое отклонение от заданного значения силы тока

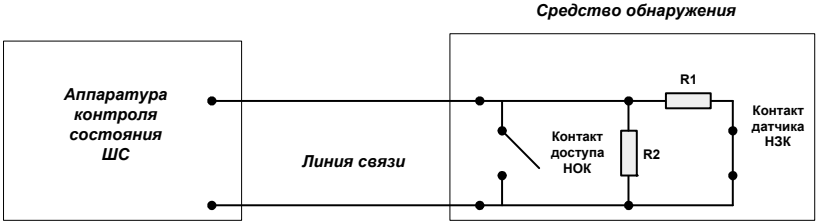
воспринимается системой как тревожный сигнал – нарушение безопасного состояния линии связи (рис. 5.6). В подобных системах идет одновременный контроль за состоянием СО и целостностью линии связи – контроль за состоянием шлейфа сигнализации (ШС).

На рис. 5.6 представлены варианты организации ШС при подключении к КП (рис. 5.6,а – при использовании НОК датчика обнаружения нарушителя; рис. 5.6,б – при использовании НЗК датчика обнаружения нарушителя; контакт доступа – контакт датчика вскрытия корпуса СО).

Значения сопротивлений $R1$ и $R2$ для каждой КП фиксированы и различны для панелей разных производителей и моделей. Любая подобная схема наблюдения за состоянием ШС характеризуется чувствительностью, т.е. для данной схемы – величиной, на которую сила протекающего тока может отклоняться от заданных значений, не вызывая срабатывания тревожной сигнализации. Чувствительность подобных схем наблюдения лежит в пределах от 2 % до 30 %. Может показаться, что система с чувствительностью, составляющей 2 %, обеспечивает большую надежность связи, чем система с чувствительностью 30 %, но это не совсем так. На самом деле нейтрализация системы с более высокой чувствительностью ненамного более затруднительна, но в то же время такая система обладает более высокой частотой возникновения ложных сигналов тревоги. Например, для медных проводов отклонения сопротивления при изменении температуры на 25,5 °С составляет 10 %.



а)



б)

Рис. 5.6. Контроль состояния линии связи с подачей постоянного тока

Для предложенных на рис. 5.6 вариантов построения ШС аппаратура контроля позволит распознавать четыре состояния ШС, значения сопротивления которых приведены в табл. 5.1.

Контроль методом уплотнения линии связи. Как отмечено ранее, данные, поступающие от нескольких датчиков, могут быть переданы по одной линии посредством уплотнения линии связи. Системы уплотнения линий связи сами по себе обеспечивают некоторую степень надежности и безопасности связи, так как затрудняют определение состояния каждого отдельного датчика и подмену подаваемых им сигналов.

Таблица 5.1 Состояния шлейфа сигнализации

Состояние ШС	Сопротивление ШС	Сигнал на КП
Используется НОК СО и НОК датчика вскрытия		
Нормальное состояние работы	R1+R2	«норма»
Тревога СО	R1	«тревога»
Обрыв ЛС	бесконечность	«обрыв»
Вскрытие СО	0 Ом	«вскрытие»
Используется НЗК СО и НОК датчика вскрытия		
Нормальное состояние работы	R1*R2/(R1+R2)	«норма»
Тревога СО	R2	«тревога»
Обрыв ЛС	бесконечность	«обрыв»
Вскрытие СО	0 Ом	«вскрытие»

Контроль методом шифрования сигналов. В последнее время применяются устройства шифрования передаваемой информации. Данный метод обеспечивает защиту линии связи и защиту данных. Шифрование/кодирование сигналов применяется в системах с мультиплексной шиной данных. В таких линиях связи наблюдение за состоянием самой линии связи (проводов) осуществляется с подачей постоянного тока.

Защита линии связи от попыток повреждения и модификации

Физическая защита линии и наблюдение за состоянием линии, рассмотренные выше, в основном обеспечивают надежность связи на всем протяжении линии связи, за исключением конечных точек соединения. Соединения линии с датчиками и в распределительных щитах, установленных на линии, и на входе оборудования сбора информации все еще не защищены от несанкционированного доступа. В таких местах дополнительная защита обеспечивается оснащением корпусов датчиков индикаторами доступа (датчик вскрытия прибора). Датчик вскрытия должен быть подключен как автономный дат-

чик, для того чтобы аппаратура контроля состояния ШС (например, КП) позволяла различать сигналы несанкционированного доступа к приборам от других сигналов тревоги. На рис. 5.6 представлен пример включения датчика вскрытия СО в линию связи.

5.5. Оборудование и выполняемые функции станции сбора и обработки данных

Оборудование системы сбора и обработки данных, устанавливаемое на пульте управления оператора, принимает поступающую от датчиков информацию. При проектировании пульта управления оператора необходимо ответить на следующие вопросы:

- какую информацию получает оператор;
- как представляется эта информация;
- какие устройства управления системой будут использоваться;
- как оптимально расположить оборудование на АРМ оператора.

К представляемой информации на АРМ оператора системы охраны, способствующей повышению уровня безопасности на объекте, относятся:

- состояния зоны наблюдения: разрешенный доступ, охрана, тревога, несанкционированный доступ, неисправность линии связи, неисправность датчика;
- географический план объекта с расположением на нем охраняемых участков;
- время поступления сигналов тревоги;
- информация об опасных условиях или опасных материалах на каждом наблюдаемом/охраняемом участке объекта;
- инструкции с описанием действий, которые необходимо предпринимать в той или иной тревожной ситуации.

Основная задача проектировщика системы сбора и обработки информации заключается в том, чтобы подробно определить все компоненты, обеспечивающие интерфейс оператора и системы. Например, необходимо определить тип используемого оборудования и характеристики представления визуальной информации. Ниже обсуждается аппаратура сбора и обработки информации.

Индикаторные панели – географическая карта территории объекта, на которой расположение световых индикаторов соответствует расположению датчиков. Такие индикаторные панели полезны в тех случаях, когда оператор одновременно наблюдает за дисплеем и за территорией объекта, например, оператор находится на вышке периметра объекта.

Недостатки индикаторных панелей:

- затруднена модернизация;
- занимают большое пространство на АРМ оператора.

Автоматические распечатывающие устройства. Аппаратура сбора и обработки данных с охраняемого объекта выводит информацию на принтер. Принтер не может являться основным средством оповещения, так как не способен предоставлять информацию о нескольких сигналах тревоги одновременно. В кризисной ситуации возможна перегрузка буферной памяти принтера из-за большого потока информации.

Монитор персонального компьютера. На мониторах ПК информация может быть представлена в виде текста (список событий в системе) и в графическом формате (план объекта), с использованием различных форматов и цветов. Мониторы не так дороги, как индикаторные панели, и не занимают большой площади на АРМ оператора системы безопасности.

К числу существенных факторов, которые определяют восприятие человеком информации, представленной на мониторах компьютера, можно отнести следующие.

- Выбор информации, т.е. отсеивание несущественной и предоставление оператору только информации, имеющей действительное значение.
- Выбор форматов представления информации, способствующих распознаванию информации оператором.
- Использование средств улучшения визуального представления информации.

Недостаток представления информации на мониторе ПК – ограниченная площадь экрана монитора. Разрешающей способности мониторов часто недостаточно для представления подробных планов всей территории объекта.

Одним из факторов, определяющих взаимодействие оператора с системой, является эргономичное использование АРМ оператора. Существуют три основных метода использования рабочего пространства вокруг оператора:

- вывод на дисплей различного рода информации в различное время;
- использование различных цветов для категорирования информации;
- использование нескольких мониторов.

Примером вывода на дисплей различных видов информации в различное время может служить отображение отдельной зоны охраняемой территории объекта, где сработал датчик обнаружения. В таких системах сообщение о поступлении сигнала тревоги заменяет на мониторе любые другие сообщения, если на экране нет места для нового сообщения. Система может быть организована таким образом, чтобы сообщения с определенных зон поступали на дисплей в первую очередь (приоритетное отображение зон объекта).

Использование нескольких мониторов позволяет экономично и главное эффективно использовать пространство АРМ оператора системы безопасности. Например, один из мониторов используется для

вывода информации о состоянии зон объекта (план-схема зоны или карта всей территории объекта), а другой монитор используется для вывода вспомогательной информации (протокол событий в системе).

Видеомониторы. Существует устоявшееся правило, что для вывода изображений, передаваемых камерами системы телевизионного наблюдения, можно использовать до шести видеомониторов. Использование более чем шести видеомониторов приведет к снижению остроты восприятия оператором информации. Систему можно запрограммировать таким образом, что на «первичные» мониторы автоматически (по сигналу тревоги) выводятся изображения тревожных зон объекта; также возможен выбор зон объекта вручную, с целью определения состояния той или иной зоны. «Второстепенные» мониторы могут быть использованы оператором по мере необходимости и обычно применяются в целях слежения за процессами, а не в целях оценки ситуации на объекте.

Оценка аварийной ситуации. В современных системах охраны применяется большое количество стационарных телекамер, позволяющих производить быструю дистанционную оценку ситуации с выяснением причин подачи сигнала тревоги. Аппаратура сбора и обработки информации должна автоматически управлять изображениями с телекамер таким образом, чтобы изображение с тревожной зоны немедленно появлялось на экране видеомонитора. Система также должна включать устройства для записи видеоинформации. В современных системах физической защиты эта координация осуществляется центральным компьютером системы и видеокоммутатором.

Логика обработки сигналов тревоги. Современные автоматизированные системы позволяют настроить любую логику работы системы обнаружения. Например, на участке объекта применяются одновременно два или даже три датчика обнаружения различных технологий. Логику работы системы (3 датчика) на выдачу сигнала тревоги с данного участка можно запрограммировать следующую: тревоги при срабатывании всех трех датчиков, тревога при срабаты-

вании двух из трех, тревоги при одном из трех. Теоретически система датчиков, работающая по логике «1 из 3», будет обладать большим количеством ложных тревог, а система «3 из 3» – большим значением вероятности необнаружения. Общего универсального алгоритма выбора логики работы системы датчиков на одном участке не существует, для каждого объекта или даже участка зоны объекта решение задачи выбора будет индивидуальным. Зависит оно, в первую очередь, от характеристик объекта и применяемых средств обнаружения. Для решения задачи выбора логики работы системы датчиков применяются вероятностные методы расчета характеристик системы.

Применение нескольких средств обнаружения на одном участке объекта (например, на периметре) и настройка времени запаздывания поступления сигналов тревоги от разных датчиков одного участка позволят судить о направлении движения нарушителя («на объект» или «с объекта»).

Расположение оборудования АРМ оператора системы безопасности. Рабочее место оператора должно быть спроектировано таким образом, чтобы обеспечить оптимальное выполнение оператором функций контроля, оценки и управления СФЗ.

Перед проектированием рабочего места оператора следует принять во внимание следующие факторы:

- какие объекты будут находиться в поле зрения оператора (люди, оборудование, мониторы, средства управления);
- какая информация будет восприниматься оператором (звуковые сигналы);
- какое оборудование должно быть доступно оператору (средства управления и средства связи).

Пространство АРМ оператора подразделяется на зоны различной видимости. Оператор, находящийся в нормальном рабочем положении, должен видеть все окружающие его мониторы и дисплеи.

Первичные мониторы (на которые выводится тревожная информация) должны быть расположены прямо перед оператором. Наблюдение за вторичными мониторами и дисплеями может потребовать отведения глаз в сторону. Вспомогательные мониторы и дисплеи (резервные индикаторные системы, индикаторы систем обеспечения) могут потребовать как отведения глаз в сторону, так и поворота головы оператора.

Важную роль играет обеспечение быстрого и правильного распознавания оператором средств управления, выполняющих те или иные функции. Распознавание обеспечивается многими способами, в том числе с помощью простых и четких надписей, цветовых кодов, а также посредством изготовления средств управления различной формы. Средство управления следует всегда располагать поблизости от соответствующего дисплея, чтобы свести к минимуму время поиска и количество движений оператора. Расположение оборудования АРМ должно определяться важностью выполняемых им функций и частотой их использования.

5.6. Дублирование/резервирование автоматизированного рабочего места оператора СФЗ

Дублирование пультов управления. Существуют СФЗ больших объектов, на которых имеется несколько локальных пунктов управления системой. Информация с этих пунктов дублируется на центральный пункт управления системой, что регламентируется Правилами по ФЗ. Дублирование оборудования позволяет повысить уровень надежности системы. В некоторых случаях создаются два пункта управления СФЗ, используемые с целью повышения

надежности персонала в соответствии с правилом, не разрешающим управление системой под наблюдением менее чем двух человек или позволяющим осуществлять операции с системой только при условии выполнения одних и тех же действий обоими операторами. Другой метод дублирования станции сбора и обработки информации предусматривает управление системой с одного, главного, пульта управления под наблюдением оператора, находящегося за вторым пультом управления, который может взять на себя функции управления в случае отказа оборудования или неспособности первого оператора выполнять свои функции.

Аварийная система электропитания. Бесперебойное функционирование систем с компьютерным управлением (всей СФЗ) зависит от электропитания с определенными характеристиками. Последнее время для этого широко применяются аккумуляторные системы непрерывного электропитания (UPS). Системы UPS сохраняют работоспособность СФЗ на тот промежуток времени, который необходим для запуска дизельной электростанции обеспечения СФЗ. При проектировании системы резервного электропитания надо внимательно подходить к выбору компонентов этой системы (UPS системы и дизельной установки). Также следует учесть, что надежность функционирования системы резервного электропитания зависит от правильности и своевременности ее технического обслуживания.

Резервные системы. В Правилах по ФЗ сказано: «Отказ или вывод из строя какого-либо элемента комплекса инженерно-

технических средств физической защиты не должен нарушать функционирование системы физической защиты в целом».

В любой автоматизированной системе может возникнуть та или иная неисправность. Особое внимание необходимо уделить выбору компонентов СФЗ, неисправность которых может привести к выходу из строя всей системы. Для предотвращения таких ситуаций устанавливается резервное оборудование и разрабатываются инструкции на случай выхода из строя того или иного оборудования. Резервное оборудование функционирует постоянно или одновременно с основной системой, или подключается автоматически либо вручную. Общий уровень защиты системы от неисправностей может быть повышен посредством увеличения количества обслуживающего систему персонала. Также на объекте должны быть разработаны и внедрены соответствующие инструкции, определяющие последовательность действий в случае выхода из строя компонентов СФЗ.

Вопросы для самоконтроля

1. Какие существуют методы передачи информации с датчиков обнаружения на аппаратуру сбора и обработки информации?
2. Опишите назначение контрольных панелей и выполняемые ими функции.
3. Какие существуют технологии передачи информации от СО к КП?
4. Какие существуют методы разделения каналов связи мультиплексной шины данных?
5. Как можно контролировать состояния шлейфа сигнализации?
6. Какие состояния средства обнаружения и линии связи контролируются контрольной панелью?
7. Какая аппаратура используется для оснащения АРМ оператора системы безопасности?
8. Какие требования предъявляются по организации АРМ оператора системы безопасности?
9. Какие требования предъявляются к повышению надежности АРМ оператора СФЗ и какие существуют методы и системы повышения надежности АРМ оператора СФЗ?

6. ПОДСИСТЕМА ЗАДЕРЖКИ

Подсистема задержки в системе физической защиты объекта выполняет функцию задержки продвижения нарушителей. В данном разделе будут рассмотрены вопросы, связанные с применением дополнительных элементов подсистемы задержки и укреплением конструкций зданий для защиты от проникновения [П.2, 6.1 – 6.8].

6.1. Назначение, задачи и состав подсистемы задержки

Эффективная система физической защиты должна предусматривать кроме обнаружения проникновения злоумышленника также и перехват злоумышленника силами ответного действия. Перехват злоумышленника должен быть при этом осуществлен до того, как злоумышленник выполнит свою задачу на объекте.

Непрерывное нахождение во всех помещениях объекта сотрудников охраны экономически нецелесообразно. Поэтому необходимо каким-либо образом задержать злоумышленника на время, необходимое силам ответного действия для прибытия из мест дислокации и развертывания. После того, как проникновение злоумышленников на территорию было обнаружено, в действие вступают пассивные или механизированные средства задержки.

Предназначение системы физической защиты состоит в том, чтобы гарантировать своевременное прибытие сил ответного действия и предотвращение выполнения злоумышленниками их задачи. Роль заграждений состоит в том, чтобы увеличить количество времени, необходимого злоумышленникам после их обнаружения, посредством создания препятствий в различных точках их маршрута. Некоторые заграждения способны существенно задерживать продвижение злоумышленников или даже остановить их.

Задачи подсистемы задержки

К основным задачам подсистемы задержки можно отнести следующие.

- Максимальное замедление продвижения нарушителя. Инженерные сооружения совместно с силами охраны в первую очередь должны обеспечивать задержку продвижения нарушителя к месту совершения диверсии или хищения ЯМ.
- Предупреждение несанкционированного доступа (НСД). Физические барьеры обозначают границы объекта и создают впечатление серьезной системы защиты.
- Обнаружение НСД. Большинство периметровых средств обнаружения могут эффективно функционировать только в комплексе с физическими барьерами. Периметр объекта должен представлять собой единую систему обнаружения и задержки.
- Пресечение НСД. Инженерные сооружения обеспечивают защиту сил охраны при выполнении ими своих основных задач и задерживают отступающего нарушителя.

Состав подсистемы задержки

К инженерным средствам физической защиты относят:

- физические барьеры;
- оборудование периметров (сигнальные заграждения СО; контрольно-следовая полоса (КСП); тропа нарядов (дорога охраны); наблюдательные вышки, постовые грибки, будки; указательные, разграничительные и предупредительные знаки; другое оборудование);
- оборудование КПП;
- защитно-оборонительные сооружения (пуленепробиваемые кабины для операторов КПП; укрепленные помещения для ре-

зервов караула; оборонительные сооружения (оборудованные позиции) для сил охраны; оборудование мест для часовых на транспорте).

6.2. Виды физических барьеров

Физический барьер – физическое препятствие, создающее задержку проникновению нарушителя в охраняемые зоны. К физическим барьерам относятся:

- Строительные конструкции:
  - стены;
  - перекрытия;
  - ворота, двери.
- Специальные конструкции:
  - заграждения (периметровые; конструкционные; механические; выпускаемые задерживающие материалы; быстро разворачиваемые устройства);
  - противотаранные устройства;
  - решетки;
  - контейнеры;
  - усиленные двери.
- Любые физические препятствия, задерживающие нарушителя.

Возможны ситуации, когда один физический барьер выполняет и функции исполнительного устройства СКУД и элемента задержки. В главе 3 было дано описание исполнительных устройств СКУД, а в данной главе будут представлены особенности применения устройств задержки.

К заграждениям периметра относятся: заборы, ограды, калитки, ворота, заграждения для транспорта.

Конструкционные заграждения включают: стены, окна, полы, крыши, усиления дверных проемов, решетки на технологических

каналах. Максимальная задержка осуществляется в заранее определенных точках. Чем больше конструкционных заграждений, тем эффективнее задержка.

Механические заграждения: двери, шлагбаумы, ворота, замки, задвижки. Такие заграждения оказывают минимальное воздействие на технологические процессы на объекте, безопасны для персонала, долговечны.

Наиболее часто используемые выпускаемые задерживающие материалы – это жидкий пенополиуретан, жидкий пеноматериал, химическая дымовая завеса, липкий термопластический пеноматериал (рис. 6.1). Эти средства дают хороший психологический эффект, но они требуют сложной техники, могут быть небезопасны для персонала, а в отдельных случаях могут серьезно нарушить технологический процесс на объекте.

Рис. 6.1. Липкий термопластический пеноматериал

Для усиления основной системы иногда применяют нетрадиционные меры задержки нарушителя, а именно: внезапный ослепительный свет; мощный звуковой сигнал; газ с сильным запахом; дымовую завесу; опускаемые (выдвигаемые) решетки; опускающиеся рулоны колючей проволоки; наполнители пространства. Эти средства бывают особенно эффективны, если нарушитель сталкивается с ними неожиданно.

Принципы построения подсистемы задержки

Основные принципы построения подсистемы задержки:

- Постоянная и бесперебойная работа всех средств задержки: физических барьеров, задерживающих материалов, сил охраны.
- Задержка эффективна только после обнаружения, так как только тогда нажинаются ответные действия сил реагирования.
- Сбалансированность (отсутствие слабых мест) и многорубежность системы задержки.
- Усиление средств задержки от периферии к центру объекта.
- Время, необходимое для обнаружения и развертывания сил охраны, должно быть меньше времени, необходимого злоумышленнику для выполнения его задачи.

6.3. Заграждения периметра

Заграждения периметра – первый рубеж системы физической защиты. Функция этих заграждений – предотвращать проникновение неуполномоченных лиц на территорию объекта. Стандартные ограждения из секций, обычно устанавливаемые в качестве периметра вокруг территории промышленных предприятий, не составляют серьезного препятствия для подготовленного злоумышленни-

ка. Заграждения такого типа можно проломить с помощью транспортного средства или перелезть, под них можно сделать подкоп, или пролезть через отверстие, проделанное в проволочной сетке – т.е. проникнуть на территорию в течение нескольких секунд. Усовершенствование такого заграждения с помощью нескольких валиков скрученной колючей проволоки или армированной колючей ленты (АКЛ) увеличит время задержки незначительно. Практически любое заграждение периметра высотой в несколько метров и шириной порядка 10 м может быть преодолено менее чем за минуту с помощью переносных раскладных лестниц.

Тем не менее, усовершенствование заграждений периметра может принести существенные выгоды. Во-первых, установка заграждений для транспортных средств и пеших злоумышленников в непосредственной близости к системе обнаружения проникновения через периметр с внутренней стороны позволяет задержать их на некоторое время в точке обнаружения, что способствует более успешной оценке аварийной ситуации. Во-вторых, если заграждения периметра обеспечивают сколько-нибудь существенную задержку злоумышленников, и силы ответного действия быстро реагируют на поступление общего сигнала тревоги после оценки аварийной ситуации, нарушители могут быть захвачены недалеко от точки, из которой поступил первый сигнал тревоги.

Должно быть уделено внимание возможности установки заграждений для транспортных средств вдоль всего периметра с внутренней стороны обычных заграждений с тем, чтобы принудить нарушителей передвигаться по территории объекта без помощи транспортных средств и нести с собой необходимые им инструменты и оружие.

Все заграждения в зависимости от назначения можно разделить на 4 типа:

- сигнализационные;

- сигнализационно-электризуемые (электрошоковые);
- строительные (технические);
- строительно-сигнализационные [П.1, 6.3, 6.4, 6.5].

Сигнализационные заграждения образовывают проводящие металлические конструкции, являющиеся чувствительным элементом периметрового средства обнаружения, которое называется заградительным. Например, в отечественном сигнализационном комплексе «С-175М», долгое время являвшемся базовым для охраны государственной границы, заграждение (высотой 210 см) образовывают перемежающиеся линии колючей проволоки (закрепленные на деревянных или бетонных столбах), включенные в два активных шлейфа, чувствительных к обрыву и короткому замыканию смежных линий, которые вызывает «нормальный» нарушитель. В другом современном заградительном электромеханическом СО DTR-2000 (фирма Magal, Израиль) физический барьер (высотой до 4 м) образовывают туго натянутые стальные проволоки, закрепленные на металлических столбах с помощью точечных датчиков натяжения, чувствительных к деформациям заграждения, вызванным нарушителем.

Сигнализационно-электризуемые заграждения представляют собой систему токоведущих проводов (изолированных от опор), по которой распространяются импульсы высокого напряжения (3-10 кВ), вызывающие болевой шок у нарушителя при касании. Действующие международные стандарты электробезопасности регламентируют энергию импульсов, не смертельную в обычном режиме. Появившись на мировом рынке более 20 лет назад, электризуемые заграждения к настоящему моменту времени приобрели сигнализационные качества детектора вторжения, позволяя контролировать не только свою целостность и структуру (обрыв, замыкание соседних проводников, заземление), но и локализовать (с точностью до нескольких десятков метров) место вторжения.

Строительные заграждения весьма разнообразны, их классификация дана на рис. 6.2 [6.1, 6.2]. Необходимо рассмотреть их с точки зрения охранно-сигнализационных качеств и эргономики. Особый тип образуют различные комбинации строительных и сигнализационных заграждений.

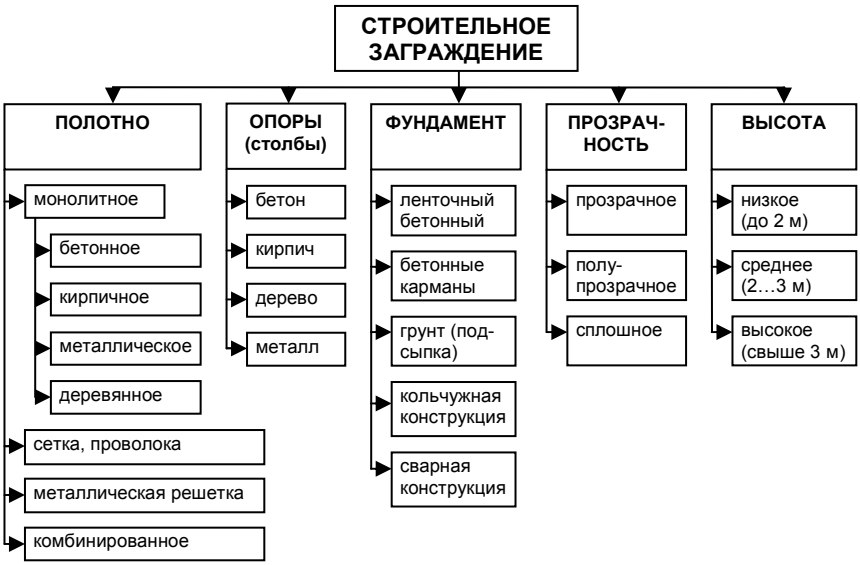


Рис. 6.2. Классификация строительных заграждений

Сегодня традиционно наиболее распространенными являются сплошные (непрозрачные) заграждения. К преимуществам таких заграждений можно отнести:

- возможность скрытного передвижения людей по объекту, особенно вблизи заграждения с внутренней стороны (например, реакция охраны на сигнал тревоги);
- скрытность установки средств обнаружения (СО) во внутренней части периметра;

- затруднение визуального сбора информации о характере производственной деятельности объекта, составе и тактике действия подразделения охраны.

Недостатками заграждения являются высокая стоимость и трудоемкость возведения, а также непрозрачность – для наблюдения изнутри за перемещениями или действиями людей с внешней стороны периметра.

Прозрачные заграждения (например, сеточные, решетчатые) относительно дешевле, трудоемкость их возведения значительно ниже, однако они не обеспечивают вышеописанной скрытности и достаточной прочности.

Эффективным заграждением являются «мягкие» заборы, выполненные из различных металлических сеток, проволоки или армированной колючей ленты (АКЛ). Любое воздействие на такой забор с целью преодоления (перелаз, разрушение полотна забора, подкоп) неизбежно приводит к колебаниям полотна заграждения. В настоящее время существует много вибрационных СО с кабельным чувствительным элементом, способных преобразовать эти колебания в сигнал тревоги (например, «Годограф-СМВ», «Дельфин-МП», «Гюрза-035», «Мультисенсор», «Гардвайр» и т. п.).

Что же касается железобетонных или кирпичных заборов, то как раз этот тип заграждений наиболее удобен для преодоления путем перелаза, особенно с применением различных вспомогательных средств (лестницы, стремянки и т.д.). Поэтому в большинстве случаев приходится дополнительно оборудовать монолитные («жесткие») заграждения различными козырьками в виде «мягких» заграждений из сетки или АКЛ.

Наиболее интересными свойствами обладают так называемые «полупрозрачные» заграждения, конструкция которых состоит из следующих элементов:

- непрозрачных элементов (например, кирпичное основание высотой 1,8–2 м) и прозрачных (например, сетка наверху), обес-

печивая относительную невидимость снаружи периметра (снизу, с высоты человеческого роста) и видимость изнутри (например, с крыши или чердака дома, пригорка);

- перемежающихся «косых» элементов, позволяющих видеть снаружи лишь отдельные части объекта, в то время как при перемещении охраны вдоль и внутри периметра, можно наблюдать за действиями людей снаружи (подобно жалюзи).

Эти и другие возможные композиционные конструкции могут обеспечить разумный компромисс между стоимостью, скрытностью и технической эстетикой.

Высота заграждения является важным параметром, который определяет его проходимость (путем перелаза), время преодоления, опасность падения, которой подвергает себя нарушитель наверху. В принципе, чем она больше, тем лучше, – по этой причине не рекомендуются заграждения высотой менее 1,5 м, которые могут быть преодолены прыжком. С другой стороны, заграждения высотой свыше 4 м (известны примеры высотой до 6 м), уже практически ничего не прибавляя с точки зрения охранных качеств, выглядят не эстетично, требуют дополнительного конструкционного усиления ввиду возрастания парусности. В целом, высота заграждения должна определяться разумным компромиссом между охранной функцией и эстетикой. Стоимость заграждения (материалы, работа) приблизительно пропорциональна его высоте, в то время как стоимость сигнализационного блокирования рубежа от его высоты (в рассматриваемых пределах) зависит в слабой степени.

Низкое заграждение высотой до 2 м позволяет просматривать часть территории объекта (например, с небольшого возвышения), использовать доступные и переносимые средства для облегчения вторжения, например, стремянку, не оказывающую механического воздействия на заграждение при его преодолении. Такое заграждение как бы провоцирует нарушителя на перелаз, что может использоваться при выборе и установке периметрового СО поверх него.

Заграждения высотой от 2 до 3 м являются наиболее распространенными. Преодоление такого заграждения путем перелаза возможно с помощью подручных средств, однако усиление его сверху дополнительной «колючей» объемной или плоской (желательно наклоненной наружу) конструкцией, например спиралью из армированной колючей ленты, значительно затрудняет перелаз.

Заграждение высотой от 3 до 4 м преодолеть путем перелаза (даже с помощью подручных средств) трудно, и более реальным становится его подкоп или разрушение. Такое заграждение ввиду большой высоты при условии ветровой нагрузки (расчет должен идти на порывы со скоростью до 30 м/с) требует дополнительного усиления фундамента и нижней части конструкции.

Фундамент (например, ленточный, по всему периметру), является практически обязательной частью заграждения, поскольку:

- обеспечивает меньшую подвижность заграждения при действии сильного ветра, который является существенным помеховым фактором для большинства периметровых СО, установленных на или вблизи заграждения;
- при глубине свыше 50–80 см он обеспечивает достаточно надежную противоподкопную защиту от действий нарушителя;
- способствует большей долговечности всего заграждения.

В случае невозможности установки ленточного, обеспечивается «точечный» фундамент под опоры заграждения (как правило, через 2,5-3 м), которые несут на себе основную нагрузку. Опыт показывает, что срок службы заграждения без фундамента составляет не более трех лет, после которых необходим либо капитальный ремонт, либо монтаж нового заграждения, с соответствующей переделкой сигнализационной части. Заграждение без фундамента резко ограничивает виды возможных к использованию СО, так как помехи, связанные с воздействием ветровых нагрузок, наиболее трудно компенсируемы.

Выбор полотна и опор заграждения определяется эстетическим расположением объекта, с учетом стоимости, строительной нагрузки и конструкции, а также выполняемой заграждением охранной функции:

- заграждения монолитного («закрытого») типа предназначены для обеспечения максимальной скрытности объекта и его обитателей, обладают наибольшей устойчивостью к разрушению (особенно металлические сварные), стоимость их, как правило, максимальная, а устойчивость к преодолению «с ходу» перелазом – минимальная;
- заграждения «открытого» типа (сетчатое, решетчатое), практически прозрачные для сквозного наблюдения, обладают невысокой устойчивостью к разрушению и последующему преодолению (перекус 5–8 проволок, отпиливание одной стойки решетки). Однако они наиболее приспособлены для использования средств периметровой охранной сигнализации;
- заграждения из стандартных и серийно выпускаемых комплектов армированной колючей ленты, преодоление которых как перелазом, так и разрушением заграждения затруднено (технология производства сертифицированной АКЛ обеспечивает устойчивость элементов ограждения от разрушения с помощью обычного инструмента: пассатижи, кусачки и т.п.);
- заграждения деревянные, представляющие собой наиболее уязвимые для преодоления конструкции (в том числе путем демонтажа, поджога), являющиеся, как правило, лишь красивым обрамлением территории – наиболее трудные с точки зрения использования средств обнаружения;
- заграждения комбинированные, у которых полотно представляет собой композицию двух или более типов заграждений.

Защитные ограждения с натянутыми по верхнему краю рядами колючей проволоки, с другими препятствиями из колючей проволоки общего назначения, не предотвращают проникновения на тер-

риторию. Тем не менее, размещение валиков колючей проволоки на стандартных ограждениях или около них может в какой-то степени повысить эффективность задержки злоумышленников. Возможности усовершенствования заграждения ограничены только длиной периметра и стоимостью средств усовершенствования заграждений.

Армированная колючая лента (АКЛ) изготавливается из стальной оцинкованной канатной проволоки диаметром 2,5 мм, путем обжатия ее плоской колючей лентой, штампуемой из рулонной оцинкованной стали толщиной 0,55 мм (рис. 6.3).

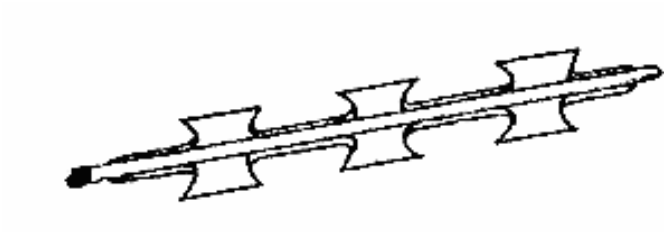


Рис. 6.3. Армированная колючая лента

Высокие механические характеристики материалов (прочность, твердость, упругость), используемых при производстве АКЛ, делают затруднительным ее перекусывание или разрезание без специальных технических средств. А защитный слой цинка на материалах обеспечивает АКЛ и изделиям из нее высокую стойкость против коррозии (срок службы — 20 лет).

Существует упрощенная конструкция АКЛ – армированная скрученная колючая лента (АСКЛ) (рис. 6.4), изготавливаемая вручную на станке «Самшит» и представляющая собой скрученные вместе проволоку и плоскую колючую ленту.

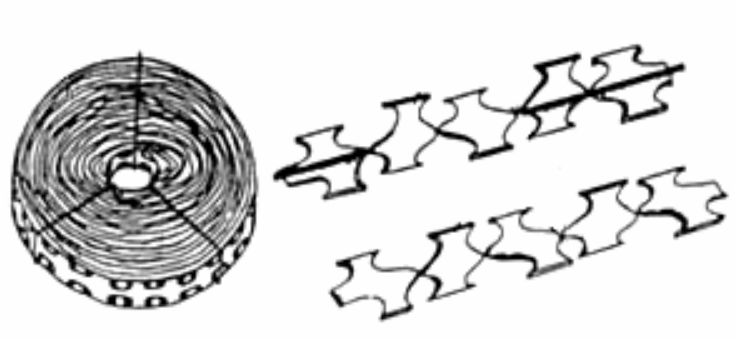


Рис. 6.4. Армированная скрученная колючая лента (АСКЛ)
и скрученная колючая лента (СКЛ)

АКЛ может устанавливаться в несколько рядов для создания эффективных заграждений или козырьков (рис. 6.5), а также используется для изготовления заграждения «Егоза», которое выпускается двух типов: в виде объемных или плоских спиралей, из которых устраиваются ограждения и заграждения различной конструкции и протяженности [6.9].

Спиральный барьер безопасности (СББ) «Егоза» представляет собой спираль, навитую из армированной колючей ленты. Соседние витки спирали связываются между собой особым образом, благодаря чему СББ «Егоза» приобретает свойства труднопреодолимой, пружинящей, пространственной конструкции (рис. 6.6).

Особенностью СББ «Егоза» является то, что его конструкция способна сохранять свою структуру после перекусывания в одном месте, однако если ее перекусить в нескольких местах, то она разъезжается в стороны, складываясь обратно в бухты. Для того чтобы СББ «Егоза» сохранял свою структуру после перекусывания в нескольких местах, необходимо каждый виток АКЛ прикреплять к заграждению, либо к опоясывающей АКЛ.

Рис. 6.5. Использование АКЛ для козырька

Рис. 6.6. Спиральный барьер безопасности «Егоза»

Плоский барьер безопасности (ПББ) «Егоза» (рис. 6.7) представляет собой плоскую, спиралевидную конструкцию из армированной колючей ленты, соседние витки которой, так же как и у СББ, скрепляются между собой особым образом.

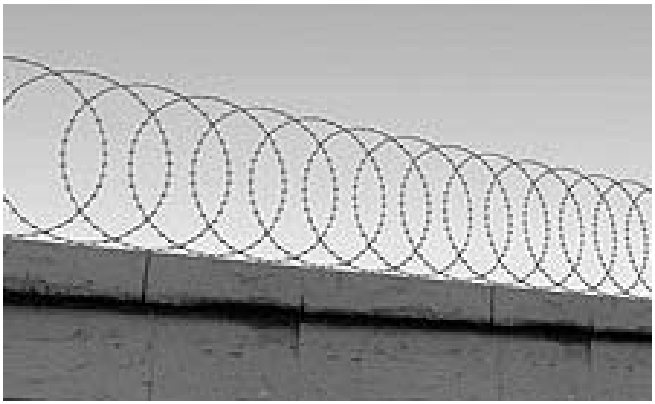


Рис. 6.7. Плоский барьер безопасности «Егоза»

Будучи плоской конструкцией, ПББ «Егоза» не выходит за габариты ограждения, имеет менее агрессивный внешний вид.

Колючая спираль «Ежевика» отличается от СББ «Егоза» другим типом используемой АКЛ, а также способом скрепления соседних витков АКЛ, которое позволяет наносить тяжелые колюще-режущие раны при попытке ее перекусить.

Варианты использования «Егозы» довольно разнообразны. Ранее уже упоминался вариант с установкой СББ и ПББ «Егоза» в качестве козырька заграждения (рис. 6.8, 6.9).

Однако возможно создание забора целиком из «Егозы», с использованием опор (рис. 6.10, 6.11) или даже без них (рис. 6.12, 6.13).

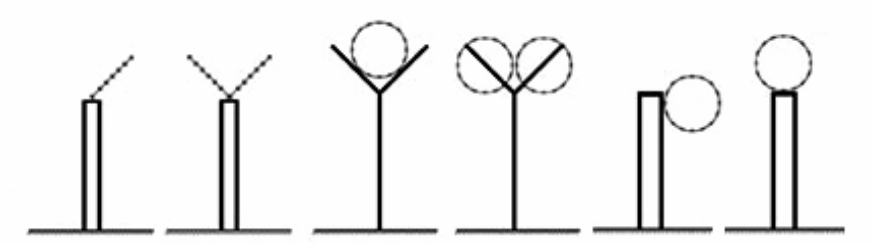


Рис. 6.8. Варианты использования «Егозы» для создания козырька заграждения

Рис. 6.9. Пример использования ПББ «Егоза» для создания козырька заграждения

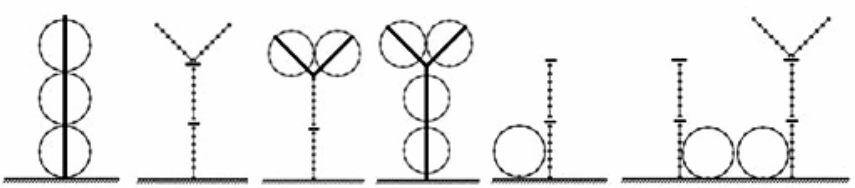


Рис. 6.10. Варианты использования СББ и ПББ «Егоза» с опорами

Рис. 6.11. Пример использования СББ «Егоза» с опорами

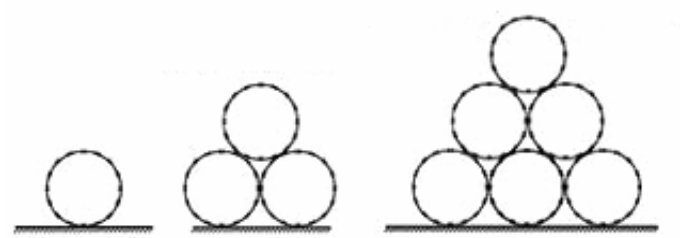


Рис. 6.12. Варианты использования СББ «Егоза» без опор

Малозаметная проволочная сеть «МЗП-1М» – предназначена для устройства мобильных противопехотных заграждений, позволяет предотвратить проникновение нарушителя на объект через забор и крышу, ограничить доступ на отдельных подходах к объекту, создать полосу отчуждения вдоль объекта. «МЗП-1М» является

препятствием для колесной и гусеничной техники и представляет собой проволочное плетение в виде пространственной четырехъярусной сети размерами 10х5х1 м, выполненной из 52 кольцевых гирлянд диаметром 0,5 м, соединенных между собой по длине и высоте скрутками из проволоки. «МЗП-1М» может устанавливаться на поверхности земли, на заборе, на стене здания или на крыше сооружения. Перед креплением к поверхности сеть растягивается, размеры ее могут быть 14х3х0,5 м.

Рис. 6.13. Пример использования СББ «Егоза» без опор

Ворота устанавливаются в определенных точках заграждений или стен для входа на территорию объекта или здания и выхода с нее. Функция ворот состоит в ограничении или предотвращении возможности перемещения пешеходов или транспортных средств и в обеспечении контроля над таким перемещением.

Про ворота как элемент СКУД было сказано ранее в главе 3. Здесь же рассмотрены некоторые особенности построения ворот как элемента подсистемы задержки.

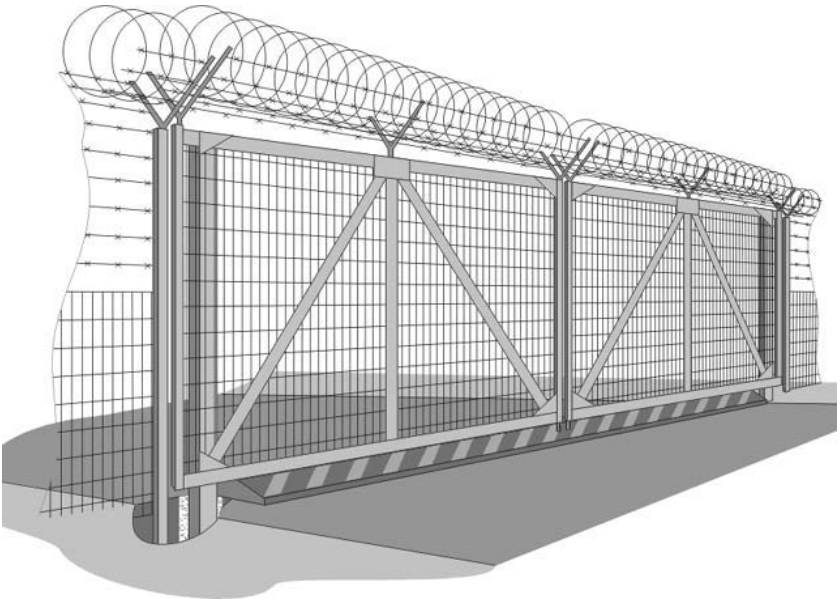


Рис. 6.14. Ворота строительного заграждения

Ворота и заграждения периметра должны быть одинаково эффективными средствами задержки (рис. 6.14). Петли, замки и засовы являются уязвимыми частями ворот ограждений. Кроме того, проезжая часть дороги для транспортных средств часто подходит непосредственно к воротам, что делает возможным разрушение ворот с помощью движущегося с высокой скоростью транспортного средства.

Расположение ворот под углом к проезжей части дороги для транспортных средств может уменьшить вероятность проламывания ворот с помощью транспортных средств. Множество поворотов

дороги перед воротами и за ними позволяют снизить скорость подъезжающих к воротам с обеих сторон транспортных средств.

Еще один метод усовершенствования заграждений проходных для транспортных средств заключается в установке множественных укрепленных ворот. Ворота должны быть организованы в виде шлюза – одни ворота должны быть закрыты и заблокированы перед тем, как открываются другие.

Заграждения для транспортных средств. Наземные транспортные средства могут быть использованы злоумышленниками в целях проникновения через заграждения периметра. Автомобили способны проломить большинство ограждений. С тем чтобы свести к минимуму вероятность проникновения транспортного средства на защищаемую территорию, в стратегических точках периметра должны быть установлены заграждения для транспортных средств, выбор которых необходимо осуществлять с учетом следующих факторов:

- вес, скорость и другие физические параметры транспортного средства;
- вероятные направления прорыва;
- особенности территории (рельеф грунта, расположение дорог на территории и за ее пределами, расположение зданий и стоянок для транспортных средств, климатические условия, особенности автомобильного движения в районе объекта).

Транспортное препятствие «ИЗП-1» – автомобильное транспортное препятствие, выполненное на основе стальной быстромонтируемой на полотне дороги конструкции «лежачего полицейского» и предназначенное для предотвращения слома ворот транспортным средством способом тарана (рис. 6.15).

Предусмотрен вариант исполнения «ИЗП-1-1» с проходным кабельным лотком для прокладки кабелей через полотно дороги без заглубления в грунт.

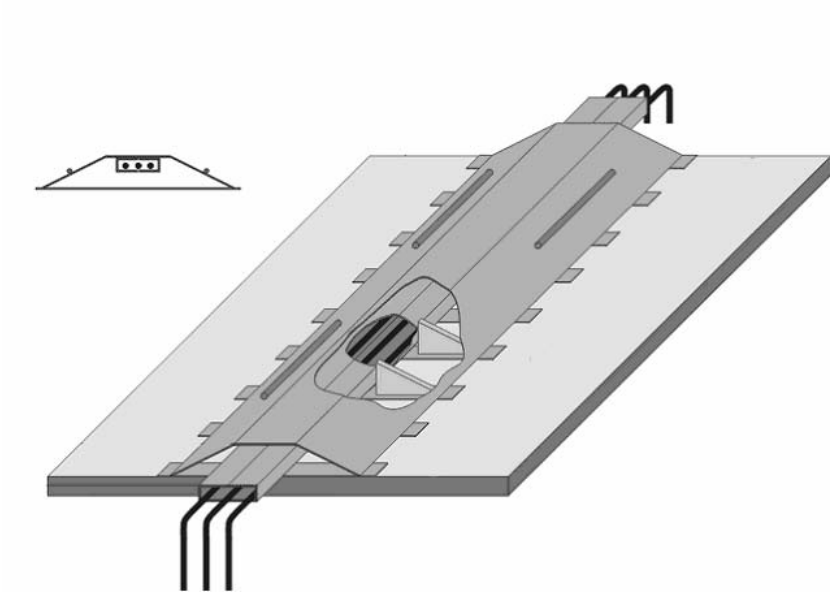


Рис. 6.15. Транспортное препятствие «ИЗП-1»

Фактор, учитываемый при выборе и установке заграждений для транспортных средств – высота, на которой происходит столкновение транспортного средства с заграждением. Оптимальный выбор высоты для любого заграждения зависит от конструкции заграждения и от характеристик транспортного средства, которым могут воспользоваться злоумышленники. Испытания показали, что высота столкновения на уровне 76 см соответствует характеристикам большинства транспортных средств.

Система заграждений должна обеспечивать полную остановку транспортных средств определенного заранее типа на определенном расстоянии от охраняемого участка независимо от того, в какой точке происходит нападение. Эффективность задержки транспортных средств с помощью стационарных и механизированных заграждений должна быть сбалансирована таким образом, чтобы в сис-

теме не было «слабых мест». В некоторых ситуациях может потребоваться защита от транспортных средств, передвигающихся в обоих направлениях, позволяющая предотвратить как проникновение транспортного средства на территорию объекта, так и его выезд с территории объекта.

Для того чтобы транспортное средство могло быть остановлено, должна быть рассеяна его кинетическая энергия (которая пропорциональна квадрату скорости и прямо пропорциональна массе).

Большинство применяемых в настоящее время систем заграждений для транспортных средств предусматривают использование одного или сочетания нескольких из следующих средств остановки движущегося транспортного средства:

- средства постепенной остановки – поглощают практически всю кинетическую энергию транспортного средства, оказывая небольшое или умеренное сопротивление передвижению, заставляющее транспортное средство постепенно остановиться, проехав довольно значительное расстояние. К таким средствам относятся балластные сетки с грузами, тянущимися за транспортным средством и постепенно накапливающимися по мере его продвижения, а также кучи песка;
- средства внезапной остановки – поглощают большую часть кинетической энергии транспортного средства, оказывая жесткое сопротивление передвижению, заставляющее транспортное средство остановиться на незначительном расстоянии. К таким средствам относятся наполненные жидкостью пластиковые контейнеры и решетки из пустотелых стальных перекладин, установленные на жестких подпорках;
- инерционные механизмы – устройства, обменивающиеся моментом и кинетической энергией в момент столкновения транспортного средства с заграждением. Такие устройства оказывают жесткое сопротивление передвижению, заставляющее транспортное средство остановиться на незначительном рас-

стоянии. К инерционным механизмам относятся бетонные блоки небольшого размера и заполненные песком незакрепленные бочки;

- жесткие средства остановки – оказывают очень жесткое сопротивление передвижению и останавливают транспортные средства на очень коротком расстоянии. При деформировании транспортного средства, столкнувшегося с заграждением, рассеивается практически вся его кинетическая энергия. К числу таких средств относятся массивные бетонные блоки и хорошо закрепленные стальные конструкции.

6.4. Объектовые заграждения

Стены. Стены зданий, хранилищ и других сооружений, как правило, считаются элементами, оказывающими большее сопротивление проникновению и менее привлекательными для лиц, замышляющих насильственное проникновение, чем двери, окна, вентиляционные отверстия и другие встречающиеся в обычных зданиях проходы. Тем не менее, стены из большинства существующих материалов могут быть преодолены с использованием надлежащих средств. Стена может быть оптимальным участком насильственного проникновения для злоумышленников. Взрывчатка позволяет очень быстро проделывать отверстия в стенах, достаточно широкие, чтобы через них можно было проникнуть внутрь. Укрепление существующих стен и возведение стен нового типа позволяют значительно увеличивать время задержки проникновения с помощью ручного инструмента, инструмента с приводом и термических резаков. Укрепление стен и увеличение их толщины позволяет в некоторой степени увеличить время проникновения с помощью взрывчатых веществ. Количество взрывчатки, необходимой для проникновения через стену, находится в экспоненциальной зависимости от толщи-

ны стены. Укрепление стен может также принудить нападающих выбрать более эффективные и сложные инструменты и изменить тактику проникновения.

Наиболее распространенные материалы для изготовления стен – железобетон, бетонные блоки, гипсовые плиты, литые бетонные секции с тавровыми балками, гофрированный асбест, стальные листы, деревянная рама с обшивкой.

Две или несколько стен, расположенных последовательно, обеспечивают большее время задержки, нежели одна стена, толщина которой равна совокупной толщине нескольких отдельных стен. Проникновение через несколько стен требует неоднократного приложения усилий и транспортировки инструментов и средств проникновения через отверстия, проделанные в уже преодоленных стенах.

Кирпичные или тонкие бетонные стены укрепляют металлическими решетками из сваренных арматур. Наиболее эффективное расположение такой решетки – между двумя стенами.

Двери. Ранее, в главе 3, была дана классификация дверей как исполнительных устройств СКУД. Ниже представлены особенности применения и приведена классификация дверей как устройств задержки. Принята следующая классификация дверей [П.1, П.2]:

- двери для персонала;
- бронированные и пуленепробиваемые двери;
- ворота для транспортных средств;
- двери хранилищ.

Двери являются одним из самых уязвимых участков конструкции, так как устройство двери и выбор материалов, из которых она изготовлена, зависят, прежде всего, от требований функционального характера. Например, вход во многие здания с толстыми бетонными стенами осуществляется через пустотелые стальные двери. Толстая бетонная стена является относительно эффективным пре-

пятствием, тогда как стандартные двери, дверные рамы и петли позволяют быстро проникать в помещение.

Следовательно, необходимо уделять особое внимание укреплению дверей и конструкциям рам, петель, шкворней и замков.

В последние годы несколько крупнейших изготовителей дверей начали выпускать бронированные и пуленепробиваемые двери. Правильная установка таких дверей иногда позволяет существенно увеличить эффективность задержки проникновения по сравнению с использованием стандартных промышленных дверей.

Стальные двери для пешеходов бывают одинарными (один лист металла) или двойными (два листа металла, между которыми может быть какой-либо наполнитель) и оснащаются самыми различными замковыми механизмами. Наружные двери, как правило, открываются наружу, независимо от выполняемой ими функции, и оборудованы встроенными замковыми механизмами. Петли скрепляются съемными или неразъемными шкворнями. Дополнительные двери устанавливаются на аварийных выходах, предусмотренных в соответствии с правилами противопожарной безопасности. Согласно требованиям по установке аварийных устройств выхода, все двери аварийных выходов должны беспрепятственно открываться изнутри наружу и, следовательно, могут выполнять функцию заграждения только при перемещении злоумышленников внутрь помещения.

Для проникновения через лицевую поверхность двери злоумышленниками могут быть использованы небольшие заряды, термические резаки, ручной инструмент с приводом.

Незащищенные замковые механизмы обычного типа могут быть открыты с помощью отмычки. Время, необходимое для открывания замка с помощью отмычки, зависит от типа и физического состояния замка, но в среднем занимает у опытного человека менее одной минуты. Взлом замка с засовом, заходящим в углубление, позволяет сократить продолжительность проникновения до нескольких секунд.

Устанавливаемые на наружных дверях петли обычно не защищены. Даже петли с неразъемными шкворнями могут быть без труда сорваны с помощью ручных инструментов. Термические резаки и взрывчатка также обеспечивают быстрое срывание петель. На проникновение через наружную дверь с повреждением петель уходит около одной минуты.

Для препятствования проникновению двери путем повреждения петель необходимо использовать торцевые крюки (анкерные штыри). Это металлические штыри, выступающие из того торца двери, который обращен к петлям, и входящие при закрывании двери в отверстия в коробке.

Ручной инструмент является эффективным средством проникновения через дверные жалюзи, окна или сетки. Достаточное для проникновения отверстие может быть проделано в листовом, закаленном или армированном стекле за 15 с. Жалюзи могут быть раздвинуты и стекло может быть разрезано примерно за 30 с.

Помимо окон и дверей, в стенах и потолках промышленных сооружений существует много неконтролируемых отверстий, таких, как выходы вентиляционных воздухопроводов, туннелей инфраструктур снабжения и туннелей для технического обслуживания оборудования, которые могут быть использованы в качестве маршрутов проникновения. Поэтому их следует оборудовать сигнализационными датчиками обнаружения.

Стекло. Обычное стекло чрезвычайно хрупко. Проникновение через обычное стекло с использованием ручного инструмента обычно занимает менее 20 с. Там, где необходимо обеспечить более высокий уровень безопасности, можно установить защитные стекла большой толщины. Кроме того, стандартные материалы для остекления окон могут быть защищены с помощью решеток, прочной стальной сетки и других металлических решетчатых структур.

Закаленное стекло изготовляется путем повторного нагревания и резкого охлаждения обычного стекла. Несмотря на то, что закали-

вание намного увеличивает механическую прочность стекла и улучшает его устойчивость к перепадам температур, закаленное стекло может быть без труда разбито с приложением умеренного усилия. Закаленное стекло можно разбить на небольшие осколки с помощью ручного молотка в течение менее чем 10 с.

Армированное стекло применяется в основном при изготовлении противопожарных дверей и окон. Армированное стекло толщиной 6 мм изготовляется с ромбическим, квадратным и шестиугольным рисунком проволочной арматуры. Проникновение через армированное стекло с помощью ручного инструмента занимает примерно 20 с.

Многослойное стекло изготовляется из двух или более слоев (дуплекса, триплекса и т.д.), листового стекла или витринного стекла, запрессованных в один или более слоев пластика шириной от 1 до 2 мм. Стекло толщиной 6 мм может быть преодолено за 30 с, тогда как проникновение через достаточно широкое отверстие в многослойном стекле толщиной 1 см требует постоянной работы ручным инструментом в течение 1,5 минут. Многослойное стекло не является прозрачной броней. Оно просто обладает большей сопротивляемостью к насильственному проникновению, нежели обычное стекло.

Прозрачным пластиком можно заменять большинство стекол: некоторые из таких пластиков, однако, легко воспламеняются, и их использование запрещено противопожарными правилами. Пластики толщиной до 2,5 см могут быть легко преодолены с помощью ручного инструмента менее чем за 10 с.

Крыши и полы. К числу средств проникновения через крыши и полы можно отнести ручной инструмент, ручной инструмент с приводом, термические резаки и взрывчатку, используемые по отдельности или в различных сочетаниях.

Строительные материалы и методы, используемые при возведении крыш и полов, сходны. Общая толщина строительных мате-

риалов, тип и количество стальной арматуры и прочность бетона, выдерживающего различные нагрузки, могут варьироваться в ограниченных пределах. В целом, полы обладают большей сопротивляемостью к проникновению, нежели крыши, так как они защищены фундаментом здания и рассчитаны на выдерживание больших нагрузок.

Крыши многих современных зданий изготовляются из следующих материалов: бетон с предварительно натянутой тавровой балкой, железобетон с металлической подложкой, легкий бетон с металлической обшивкой для крыш, металлическая обшивка с изоляцией, железобетонная плита с поперечными балками, деревянная обшивка с кровельным ковром.

Испытания на проникновение показали, что заграждения, установленные под крышей, иногда более эффективны, чем заграждения, установленные на крыше. Подкрышные заграждения могут быть установлены в некоторых существующих сооружениях без значительной модификации их конструкции. Оптимальное расстояние от крыши, определенное в ходе испытаний, составляет 25–30 см.

6.5. Механизированные заграждения

К механизированным заграждениям или устройствам относят электромеханические замки, турникеты, шлагбаумы, приводы ворот. Они могут управляться как оператором, так и автоматически, по сигналу от системы контроля доступа (СКУД).

Некоторые механизированные устройства задержки были описаны в главе «Подсистема контроля и управления доступом» как исполнительные устройства СКУД. В данной главе рассматриваются особенности применения и использования механизированных заграждений как элементов задержки.

Турникеты. Ниже описаны наиболее популярные типы конструкций турникетов.

«Трипод» – турникет с вращающимися преграждающими планками (рис. 6.16). «Трипод» является довольно популярным типом турникета. Это обусловлено невысокой стоимостью, компактностью, возможностью гармонично вписать в любой интерьер.

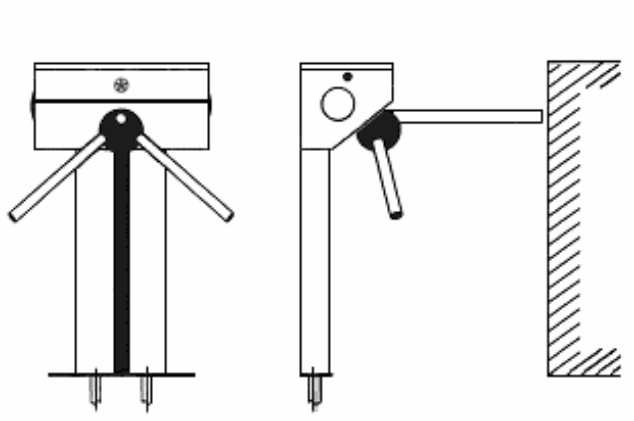


Рис. 6.16. Турникет типа «трипод»

Однако турникеты такого типа нельзя отнести к серьезным устройствам задержки, так как время, затрачиваемое подготовленным нарушителем на преодоление такого турникета, ничтожно мало. Нарушитель может как перепрыгнуть такой турникет, так и пролезть под преграждающей рамкой.

Полупрофильный турникет (рис. 6.17) – обеспечивает большую степень защищенности, чем «трипод», но требует большего пространства для установки. При использовании турникета данного типа нарушитель не сможет пройти под преграждающей планкой, но остается возможность перелезть через турникет сверху, несмотря на то, что такие турникеты выше «триподов».

Рис. 6.17. Турникет роторный полупрофильный PERCo-RTD-01

Калитка – турникет, выполненный в виде моторизованной или ручной калитки (рис. 6.18). Существуют двунаправленные электромеханические калитки с пультом дистанционного управления. После прохода человека створка калитки автоматически возвращается в закрытое состояние с помощью встроенного механического позиционирующего устройства и блокируется соленоидом. При пропадании напряжения питания калитка разблокируется, освобождая проход в обоих направлениях.

Калитки, также как «триподы» и полупрофильные турникеты, не относятся к серьезным устройствам задержки. Их можно рассматривать только как исполнительные устройства системы контроля и управления доступом и в случае, когда турникет оборудован дополнительными датчиками прохода как сигнализационное заграждение.

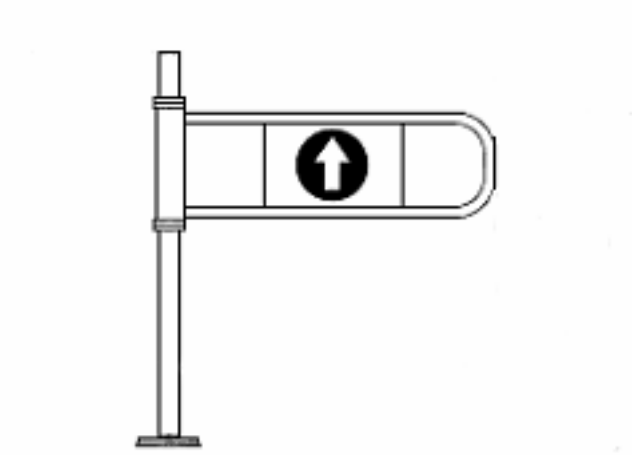


Рис. 6.18. Турникет в виде моторизованной или ручной калитки

Скоростные турникеты – обеспечивают наибольшую пропускную способность (рис. 6.19). Они могут иметь конструкцию как с дверцами небольшой высоты, так и с высокими створками (до 1,7 м).

Рис. 6.19. Скоростные турникеты

Раздвижные створки турникета расположены в середине корпуса и изготовлены из термоформованного полиуретана, а выступающие из стойки ограничивающие панели – из тонированного стекла толщиной 12 мм.

Такие турникеты по устойчивости к проникновению нарушителя могут приближаться к строительным заграждениям, только если они полностью перекрывают пространство для прохода.

Полнопрофильные турникеты – турникеты, обеспечивающие максимальную степень защиты. Они имеют конструкцию в полный рост человека, могут быть выполнены в виде вращающихся брусьев, вращающихся стеклянных створок и т.п. (рис. 6.20). Ряд моделей полнопрофильных турникетов предназначен для установки на улице для обеспечения контроля доступа на охраняемые территории.

Рис. 6.20. Полнопрофильный турникет

Часто при использовании таких турникетов внутри помещения над ними сооружаются дополнительные заграждения, по высоте достающие до потолка. В этом случае единственным способом проникновения является разрушение турникета или заграждения вокруг него.

При установке на улице полнопрофильные турникеты чаще всего встраиваются в заграждение периметра. В этом случае поверх турникета можно устанавливать тот же козырек (например, сигнализационный), что и поверх полотна забора периметра, либо дополнительный козырек из АКЛ (задерживающий). Турникеты данного типа являются довольно устойчивым заграждением при условии правильной их установки. Целостность турникета должна контролироваться, так же как и целостность основного заграждения периметра.

Шлагбаумы. Сам по себе шлагбаум не является серьезным заграждением, так как он не предназначен для задержки людей, а на автомобиле его легко разрушить. Поэтому для задержки автомобилей необходимо устанавливать дополнительные противотаранные устройства, которые уже были рассмотрены ранее в этой же главе.

Вопросы для самоконтроля

1. Каково основное назначение системы задержки?
2. Какие существуют основные принципы построения системы задержки?
3. Как классифицируются методы задержки?
4. Какие ограждения используются на протяженных периметрах?
5. Какие известны методы и способы применения АКЛ для повышения эффективности заграждений периметра?
6. Как организуется задержка в точках доступа в охраняемые зоны?
7. Перечислите методы задержки автотранспорта.
8. Какие способы укрепления дверей и окон зданий наиболее эффективны?
9. Какие существуют типы механизированных заграждений?
10. Опишите типы турникетов с точки зрения их применимости для подсистемы задержки.

7. ПОДСИСТЕМА ОТВЕТНОГО РЕАГИРОВАНИЯ

Подсистема ответного реагирования выполняет функцию ответного действия в системе физической защиты объекта, а также обеспечивает связь между персоналом СФЗ. В данную подсистему входят силы ответного реагирования, которые формируются из сотрудников службы безопасности объекта. В силы ответного реагирования также могут входить: милиция, вооруженные силы страны, отряды специального назначения и другие уполномоченные силы охраны объекта (например, ведомственная охрана предприятия). Силы ответного реагирования могут быть полностью или частично дислоцированы на территории объекта или за ее пределами.

Система связи является элементом подсистемы ответного реагирования, которая обеспечивает связь между персоналом СФЗ.

В данном разделе рассматриваются особенности сил ответного реагирования, методы построения и организации систем радиосвязи и особенности организации связи между персоналом системы физической защиты и силами ответного реагирования [П.2, 7.1, 7.2, 7.3].

7.1. Силы ответного реагирования

Цель сил ответного реагирования заключается в предотвращении действий нарушителей на объекте. Разнообразие применяемых методов выполнения этой функции находит отражение в квалификационных стандартах и требованиях по профессиональной подготовке личного состава отрядов ответного реагирования и в требованиях по выполнению отрядами перехвата и нейтрализации нарушителя. Две основные функции сил ответного реагирования – это перехват нарушителя и его нейтрализация.

Перехват определяется как успешное прибытие сил ответного реагирования на соответствующий участок с последующим предотвращением дальнейшего продвижения нарушителей. Осуществление

перехвата требует обеспечения надежной и оперативной связи между отдельными отрядами/группами сил охраны.

Характеристиками эффективности связи с отрядами ответного реагирования являются вероятность обеспечения надежной связи и время, необходимое для обеспечения связи с отрядами ответного действия. Успешное функционирование системы физической защиты требует организации оперативной и надежной сети связи отрядов сил ответного реагирования. Эта сеть связи должна быть устойчива к различным воздействиям со стороны нарушителей. Например, современные портативные радиостанции, не требующие большого количества электроэнергии, позволяют патрулям быстро передавать информацию в ходе патрулирования и осмотра территории объекта и обеспечить оперативное развертывание сил ответного реагирования при возникновении аварийной ситуации на объекте.

Возможна ситуация, когда нарушителям удастся завладеть оборудованием охраны. В этом случае необходимо предусмотреть оснащение личного состава сил охраны специальными средствами связи. Существуют несколько методов организации передачи сигнала тревоги в случае захвата нарушителями охранника или его оборудования, которые будут рассмотрены ниже.

Термин «развертывание сил ответного реагирования» означает предпринимаемые действия силами ответного реагирования с момента получения информации о возникновении чрезвычайной/нештатной ситуации на объекте до момента дислокации/расположения отрядов охраны на соответствующих участках и приведения отрядов охраны в состояние готовности к нейтрализации нарушителя. Характеристиками, определяющими эффективность развертывания сил ответного реагирования, являются вероятность успешного развертывания отрядов на заданном участке, и время, необходимое для развертывания сил охраны. Предотвращение выполнения нарушителями их задач требует выживания сил ответного реагирования. Для повышения вероятности успешной задержки и ней-

трализации нарушителя необходимо подготовить и проводить программы тактической подготовки личного состава сил ответного реагирования. Программа определения тактики развертывания сил ответного реагирования предусматривает:

- тактическое планирование;
- проведение тактической подготовки;
- проведение тактических учений.

Тактическое планирование должно осуществляться в рамках общего планирования размещения и развертывания сил ответного реагирования. Необходима разработка детально продуманных инструкций и планов, определяющих последовательность действий вооруженной охраны в случае возникновения действительной угрозы. Иерархия командного состава и порядок передачи полномочий в аварийной ситуации должны быть хорошо известны всему личному составу охраны. Готовятся подробные планы, в соответствии с которыми силы вооруженной охраны должны оснащаться оружием и аппаратурой, соответствующей уровню подготовки потенциальных нарушителей. Тактические планы (инструкции) должны содержать подробные описания действий, необходимых для успешного развертывания вооруженной охраны (например, описания маршрутов движения). Должна быть также спланирована стратегия действий сил охраны после прибытия на определенный участок (окружение и задержание нарушителей, нападение на нарушителей).

Тактическая подготовка. Личный состав сил ответного реагирования должен быть обучен выполнению всех инструкций, разработанных в ходе тактического планирования. Также личный состав должен уметь использовать тактические методы, увеличивающие вероятность своевременного развертывания и успешной нейтрализации нарушителя. К таким тактическим методам относится умение:

- использовать преимущества и недостатки сооружений и систем, расположенных на территории объекта;

- маскироваться и находить прикрытие;
- принимать меры предосторожности;
- выбирать наилучшие маршруты передвижения внутри зданий и на открытой территории объекта;
- принимать ответные меры в ночное время;
- организовывать развертывание сил ответного действия с использованием транспортных средств;
- координировать свои действия с другими членами группы вооруженной охраны.

Тактические учения. В дополнение к тактическому планированию и подготовке, важную роль играет проведение учений с развертыванием сил ответного действия на территории данного объекта; личный состав сил ответного действия должен знать, какие действия следует предпринимать в случае действительного проникновения нарушителей на территорию объекта. Практические учения используются также для того, чтобы подтвердить эффективность тактической подготовки и удостовериться в способности сил ответного реагирования выполнить свою задачу и в выполнимости тактического плана в целом.

Одно из испытаний эффективности развертывания сил ответного реагирования заключается в определении времени, проходящего с момента оповещения о необходимости перехвата нарушителей до момента прибытия отрядов охраны на соответствующий участок территории объекта. При испытаниях оценивается не только быстрота развертывания, но и навыки личного состава, что обеспечивается проведением проверочных учений по стрелковой подготовке, по физической подготовке, по использованию боевых навыков, по использованию средств подавления противника, по тактическому передвижению, по обеспечению надежной связи. Некоторые из этих навыков могут быть оценены в ходе моделирования ситуации. Другие испы-

тания могут проходить только на территории объекта или в сходной обстановке.

Нейтрализация – сочетание действий, останавливающих нарушителей перед тем, как они выполнят свою задачу. Характеристикой эффективности нейтрализации является эффективность функционирования сил ответного реагирования. Силы ответного реагирования должны быть достаточно многочисленными и должны оснащаться соответствующим возможной угрозе оборудованием и оружием. Кроме того, личный состав сил ответного реагирования должен находиться в хорошей физической форме и быть хорошо подготовленным к выполнению установленных процедур и обязанностей. В целях подтверждения способности сил ответного реагирования предотвращать успешное выполнение нарушителями своей задачи, проводятся практические занятия по поддержанию навыков личного состава сил охраны на специальных тренировочных площадках вне или на объекте.

Силы ответного реагирования должны располагать всем оборудованием и иметь возможность пользоваться всеми сооружениями, необходимыми для нейтрализации нарушителей. Техническое обслуживание и проверка оборудования проводятся для того, чтобы гарантировать его исправность при возникновении чрезвычайной ситуации на объекте. К применяемому и необходимому оборудованию сил охраны относятся:

- оружие;
- транспортные средства;
- средства связи (рации, телефоны, кнопки оповещения о нападении);
- средства личной защиты (противогазы, автономные дыхательные аппараты, каски, бронежилеты, бронетранспортеры);

- средства обеспечения выполнения поставленных задач в ночное время и в условиях недостаточной видимости (например, приборы ночного видения).

В ходе управления силами ответного действия основное внимание уделяется поддержанию необходимых навыков и надежности личного состава. Эти факторы имеют большое значение для успешного выполнения силами ответного реагирования поставленной задачи.

7.2. Связь сил ответного реагирования

Успешное функционирование системы физической защиты предполагает обеспечение надежной связи между отрядами сил ответного реагирования с помощью системы, которая защищена от попыток прослушивания линий связи, передачи ложных сообщений и глушения. Современными силами ответного реагирования широко применяются системы радиосвязи в дополнение к традиционным (проводным) средствам связи. Удобные в использовании средства радиосвязи являются неотъемлемым атрибутом сил охраны. Кодирование передачи речевых радиосигналов позволяет значительно затруднить прослушивание линий связи и попытки передачи ложных сообщений, но кодирование радиосигналов не обеспечивает защиты линий связи от глушения. Системы радиосвязи с распределенным спектром несущих частот (будут рассмотрены далее) обеспечивают высокую степень защищенности линий связи от прослушивания и глушения.

При использовании простых систем радиосвязи, потенциальные нарушители могут прослушивать переговоры, передавать ложные сообщения и просто создавать помехи в канале связи. Для решения обозначенных проблем применяются альтернативные средства связи. Таковыми являются телефоны, внутренние сети связи, системы об-

щего оповещения персонала охраны и другие средства (сигнальные ракеты, дымовые сигналы и др.). При организации системы связи отрядов сил ответного реагирования должны быть учтены такие характеристики, как сложность обращения с оборудованием и защищенность линий связи.

7.3. Современные системы радиосвязи

В данном разделе изложены основные концепции организации и построения современных систем радиосвязи. Раздел подготовлен по материалам фирмы «ТК Электорника-Дизайн», представленным на сайте фирмы.

Основы радиосвязи

Частотные диапазоны. Для организации сетей мобильной наземной радиосвязи на территории Российской Федерации выделены частотные диапазоны, указанные в табл. 7.1.

Разрешение использования радиочастот оформляются отделениями ФГУП Главный радиочастотный центр. Исключение составляют ведомственные системы связи: например, за силовыми структурами закреплены выделенные поддиапазоны частот. В любом случае для создания системы связи в указанных диапазонах обязательно выделение радиочастот.

Таблица 7.1. Частотные диапазоны, выделенные в России для организации мобильной наземной связи

Диапазон, МГц	**Метрическое обозначение**	**Условное обозначение**
30-50 и 136-174	Метровые волны	ОВЧ (VHF)
300-345 и 400-512	Дециметровые волны	УВЧ, УКВ (UHF)

Дальность радиосвязи. Дальность радиосвязи зависит от большого числа параметров (используемый частотный диапазон, рельеф местности, высота установки излучающей и принимающей антенн, окружающая электромагнитная обстановка) и может быть определена экспериментальным путем на местности.

Каждый из частотных диапазонов характеризуется специфическими условиями распространения радиосигнала. Сигналы в диапазоне коротких длин волн в наибольшей степени подвержены влиянию промышленных помех, помех от бытовых приборов, радиовещательных и телевизионных передатчиков. Применение оборудования данного диапазона оптимально в сельской местности, где уровень помех значительно ниже, чем в условиях плотной городской застройки. Диапазон характеризуется хорошим огибанием неровностей ландшафта и распространением за пределы прямой видимости.

Диапазон метровых волн (VHF) – один из самых универсальных диапазонов. Оборудование этого диапазона прекрасно работает как в сельской местности, так и в условиях городской застройки. Портативные станции работают достаточно успешно на открытой местности, но в условиях плотной городской застройки качество связи существенно снижается, поскольку отсутствуют переотражения сигнала передачи.

Диапазон дециметровых волн (UHF) – проявляет свои лучшие качества в условиях городской застройки. Выбор этого диапазона оптимален при необходимости получения устойчивой связи на небольших расстояниях, например, в черте города. Даже при использовании портативных радиостанций обеспечивается устойчивая связь с минимальным количеством мертвых зон. При использовании на открытой местности дециметровые радиоволны плохо огибают неровности рельефа и имеют сильное затухание в лесной местности.

Частотные каналы и режимы работы радиостанций. Подавляющее большинство современных радиостанций работает в симплексном или полудуплексном режиме. При этом прием и передача

информации одновременно невозможны. Включение передачи осуществляется нажатием тангенты (кнопки начала радиопередачи). При отпускании тангенты станция переходит в режим приема. Частоты передачи и приема образуют частотный канал и в общем случае могут быть различными.

Если частоты передачи и приема совпадают, то канал называется симплексным. Если частоты передачи и приема различны, то канал является дуплексным, а режим работы радиостанции полудуплексным. В режиме полного дуплекса (т.е. когда передача и прием осуществляются одновременно и тангенту нажимать не нужно) на дуплексном канале могут работать только полнодуплексные радиостанции, которые мало распространены из-за высокой стоимости.

В радиостанции могут быть запрограммированы параметры нескольких различных каналов связи. В зависимости от модели радиостанции число каналов варьируется от 1 до 100 и более.

Типы оборудования. Радиостанции, входящие в состав системы сухопутной подвижной радиосвязи, можно условно классифицировать следующим образом.

По условиям эксплуатации

Профессиональные радиостанции (например, фирмы MOTOROLA и VERTEX). Соответствуют требованиям военных стандартов по ударопрочности, воздействию вибрации и пылевлагозащищенности. Имеют минимум органов управления, параметры жестко программируются и не могут быть изменены пользователем. Рассчитаны на длительный срок службы в жестких условиях.

Коммерческие и любительские радиостанции (например, фирмы YAESU, ALNICO). Не рассчитаны на работу в экстремальных условиях. Параметры могут устанавливаться пользователем. Радиолюбительские станции имеют расширенный набор пользовательских функций.

По месту установки

Портативные (носимые) радиостанции. Выходная мощность 0,5 – 6 Вт, емкость аккумулятора 600 – 1550 мАч. Комплект поставки: приемопередатчик (радиостанция), антенна, аккумулятор, зарядное устройство.

Автомобильные радиостанции. Выходная мощность 10–60 Вт, питание от бортовой сети (13,8 В). Комплект поставки: приемопередатчик, монтажный комплект, кабель питания, автомобильный микрофон с креплением.

Стационарные радиостанции. Как правило, автомобильные станции имеют возможность стационарной установки. Дополнительное оборудование: блок питания от сети 220 В, стационарная антенна, антенный кабель. Для удобства работы может использоваться настольный диспетчерский микрофон.

Профессиональные, коммерческие и любительские станции, как правило, не отличаются по основным радиотехническим параметрам (частотные диапазоны, выходная мощность, чувствительность). Выбор того или иного типа оборудования определяется условиями эксплуатации и необходимым набором функций.

Традиционные системы радиосвязи

Выбор типа радиосети определяется имеющимся частотным ресурсом, количеством пользователей и спецификой их работы. В традиционных (conventional) диспетчерских системах радиосвязи за каждой группой закрепляется выделенный частотный канал.

Такой способ организации радиосвязи оказывается достаточно эффективным в тех случаях, когда общее число абонентов системы невелико, а необходимая зона радиопокрытия ограничена. Основным достоинством системы радиосвязи является простота и невысокая стоимость. К недостаткам относятся неэффективное использование частотного спектра и небольшой набор сервисных функций.

Симплексные радиосети. В простейшем случае радиосеть представляет собой группу радиостанций, работающих на одной частоте (на одном симплексном канале). Все пользователи радиостанций слышат друг друга и вызывают необходимого абонента голосом. При таком способе организации связи число радиостанций составляет 2 – 20. В радиосети могут использоваться портативные, автомобильные и стационарные радиостанции. Все они равнозначны. Дальность связи между автомобильными (стационарными) станциями выше. Модель симплексной радиосети представлена на рис. 7.1.

Группы абонентов в симплексной радиосети. Достаточно часто в системах радиосвязи необходимо разделить абонентов на группы. Самый простой вариант решения этой задачи – выделить каждой группе свою частоту, что в большинстве случаев невозможно из-за ограниченного частотного ресурса. Наиболее приемлемым решением является разделение групп по тональным или цифровым пилот-сигналам. Практически все современные радиостанции имеют функции тонального (TONE SQUELCH, GTCSS, PL) и/или цифрового (DIGITAL SQUELCH, DGS, DPL) управления шумоподавителем. Используя систему тонального или цифрового шумоподавления, можно разделить на группы пользователей, работающих на одной частоте. Каждой группе присваивается свой пилот-сигнал, и пользователи радиостанций будут слышать только членов своей группы. Несколько групп не могут вести переговоры одновременно. Одна и та же радиостанция может быть членом различных групп. При этом на различных каналах устанавливаются соответствующие пилот-сигналы. Несущая частота при таком разделении каналов одна для всех каналов.

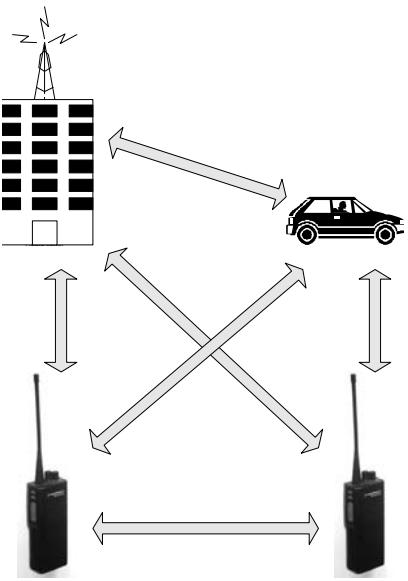


Рис. 7.1. Модель симплексной радиосети

Достаточно распространенным является вариант, когда одна из станций является диспетчерской (рис. 7.2).

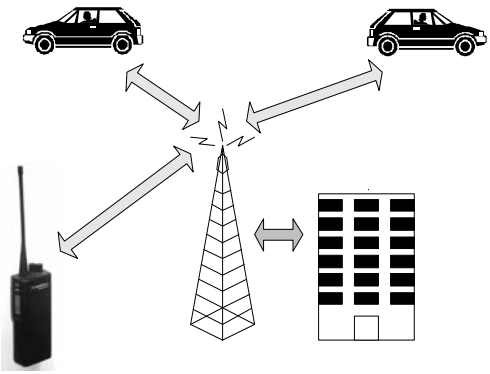


Рис. 7.2. Модель радиосети с диспетчерской станцией

Это, как правило, стационарная станция, имеющая антенну с большим коэффициентом усиления и достаточно высоко расположенную. При этом за счет правильного расположения и соответствующего типа антенны дальность связи с диспетчерской станцией может быть увеличена, и абоненты, не имеющие возможность связаться напрямую, могут передать сообщение через диспетчерскую станцию.

Выход в телефонную сеть. Даже при использовании одной симплексной частоты в радиосети можно организовать выход абонентов сети в телефонную сеть (например, ведомственную). Для этого должна быть установлена стационарная радиостанция с телефонным интерфейсом, а портативные и мобильные станции должны иметь Dual-Tone Multi-Frequency (DTMF) клавиатуру, аналогичную телефонной (рис. 7.3).

Радиостанции с клавиатурой DTMF имеют возможность передавать сигналы DTMF в эфир и выходить в телефонную сеть через телефонный интерфейс. Стационарная станция, оборудованная телефонным интерфейсом, принимает телефонный номер в системе DTMF, набираемый с абонентской станции, и передает его в телефонную сеть. Если в телефонной сети используется импульсный набор, то телефонный интерфейс преобразует DTMF в соответствующий номер в импульсивном виде. Как правило, при использовании простейших телефонных интерфейсов без селективного вызова, абоненты всех станций радиосети будут слышать все телефонные переговоры. Абонент телефонной сети, набравший номер телефонного интерфейса, также вызовет одновременно всех радиоабонентов.

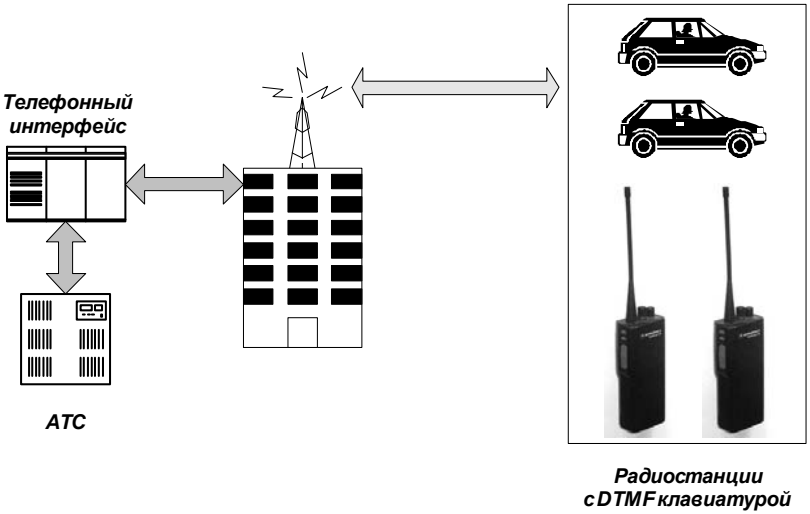


Рис. 7.3. Модель радиосети с выходом в телефонную сеть

Сигнальные системы избирательного вызова. Использование пилот-сигналов не предусматривает вызов конкретного абонента. Функции индивидуального и группового вызова, а также ряд дополнительных функций, таких как: сигнал тревоги, проверка наличия радиосвязи, передача идентификационных номеров радиостанций – возможно реализовать при использовании сигнальных систем.

Использование сигнальных систем позволяет реализовать указанные функции на уровне абонентских радиостанций без использования сложного и дорогостоящего оборудования.

Использование сигнальных систем ориентировано, в первую очередь, на решение профессиональных задач. В большинстве случаев возможность использования селективного вызова имеют только профессиональные радиостанции.

Радиосети с ретрансляторами. При наличии двух частот (дуплексной пары) возможна организация радиосети с использованием

ретранслятора, что позволяет значительно увеличить дальность радиосвязи.

Ретранслятор принимает сигнал на частоте $F1$, усиливает его и передает на частоту $F2$. Время, затрачиваемое на обработку сигнала, принято считать пренебрежимо малым. Ретранслятор является дуплексным устройством, т.е. прием и передача осуществляются одновременно. Частота передач всех абонентских станций, работающих через ретранслятор, равна $F1$, частота приема – $F2$. Абонентские радиостанции работают при этом в режиме двухчастотного симплекса (полудуплекса).

Для работы ретранслятора могут использоваться одна или две отдельные антенны для приема и передачи и дуплексный фильтр.

Дуплексным интервалом называется частота приема и передач. Для исключения взаимного влияния приемная и передающая антенны должны быть установлены на определенном расстоянии друг от друга. Величина пространственного разноса имеет обратную зависимость от величины дуплексного интервала. Далеко не всегда удается установить антенны таким образом, чтобы избежать взаимного влияния.

В большинстве случаев используется одна приемопередающая антенна и дуплексный фильтр – устройство, разделяющие полосы приема и передачи. Нормальным дуплексным интервалом для работы в полудуплексном режиме является интервал 4 – 5 МГц. При этом удается сделать дуплексный фильтр достаточно недорогим и компактным. В случае меньшего или большего дуплексного интервала конструкция дуплексного фильтра усложняется, а цена значительно возрастает.

При комплектации соответствующим контроллером ретранслятор может поддерживать различные режимы работы. Популярным являются контроллеры с селективным вызовом абонентов и выходом в телефонную сеть (рис. 7.4).

Ретранслятор с таким контроллером представляет собой одноканальную базовую станцию. Для пользователей системы связи возможны следующие типы вызовов:

- радиоабонент – радиоабонент (индивидуальный вызов);
- радиоабонент – группа;
- радиоабонент – абонент телефонной сети;
- абонент телефонной сети – радиоабонент (индивидуальный вызов);
- абонент телефонной сети – группа радиоабонентов.

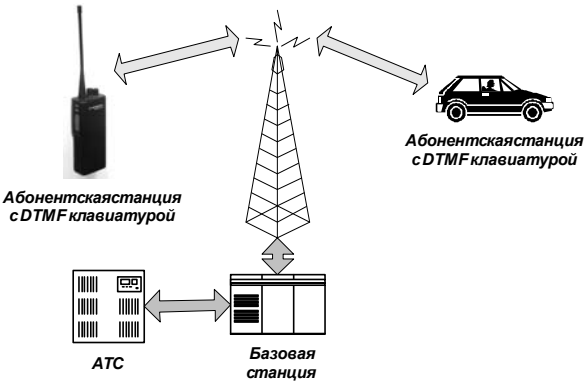


Рис. 7.4. Модель радиосети с ретранслятором и выходом в телефонную сеть

По набору функций подобные системы приближаются к транкинговым системам простейшего уровня.

Системы транкинговой радиосвязи

Системы традиционной радиосвязи обладают одним существенным недостатком – это неэффективное использование доступных радиочастот в системе (если таковых несколько).

Возможна ситуация, когда при использовании в системе традиционной радиосвязи нескольких каналов (частот) связи произойдет перегрузка одного канала (частоты) и «простаивание» (неэффективное использование) остальных. Система транкинговой радиосвязи (СТРС) – это система, в которой используется принцип равной доступности каналов для всех абонентов или групп абонентов. Этот принцип давно и повсеместно используется в телефонных сетях, откуда и происходит название «trunk» (пучок, или пучок равнодоступных каналов). Основой функцией оборудования СТРС является автоматическое предоставление свободного радиоканала по требованию абонента радиостанции и переключение на этот канал вызываемого абонента или группы абонентов.

Общие возможности транкинговых систем. Прежде всего, это увеличение радиуса действия системы, поскольку даже в простейшей СТРС связь радиостанций между собой осуществляется через ретрансляторы базовой станции (БСТ). Многозоновые СТРС имеют в своем составе несколько (от единиц до сотен) БСТ, каждая из которых обслуживает свою зону. При этом система установит соединение между радиостанциями независимо от их месторасположения.

Кроме вызова группы радиостанций (имеется во всех СТРС), почти все системы обеспечивают индивидуальный вызов конкретной радиостанции. При этом многие современные СТРС обеспечивают разделение всего парка радиостанций на отдельные отряды. Отряд – это совокупность радиостанций, принадлежащих одной группе пользователей (организации), внутри которой осуществим индивидуальный и групповой вызов. Вызовы между отрядами в большинстве случаев запрещены, хотя могут быть разрешены конкретным радиостанциям.

Как правило, СТРС обеспечивают связь радиостанции с абонентами городской и/или ведомственной телефонных сетей. Современные СТРС предоставляют также широкий спектр услуг по передаче данных между радиостанциями. Доступ к каждому виду услуг, пре-

доставляемых системой, обычно программируется индивидуально для каждого абонента. Кроме того, программируется предельное время разговора и приоритета абонента.

При работе радиостанции в СТРС могут возникнуть ситуации, в которых необходимо обойтись без ее услуг (связь с обычной радиостанцией, отказ БСТ, выход за зону действия всех БСТ системы). На этот случай все радиостанции, работающие в СТРС, имеют возможность переключения в режим обычной радиостанции.

Сравнительный обзор систем транкинговой радиосвязи. В настоящее время существует много различных типов СТРС, несовместимых между собой. Одни из них являются закрытыми, т.е. фирма-производитель не публикует протоколы их работы и сама производит все абонентское и базовое оборудование для таких систем. При этом потребитель оказывается в полной зависимости от фирмы-производителя. Другие СТРС являются открытыми, т.е. стандарты на них публикуются, и в рамках таких систем может совместно работать оборудование любых производителей, придерживающихся этих стандартов.

По способу передачи речевой информации СТРС можно разделить на аналоговые и цифровые. Цифровые системы в настоящее время предлагают для спецслужб некоторые фирмы, цифровым является и новый европейский стандарт TETRA.

Сканирующие СТРС. Подобные системы называют псевдотранкинговыми. В таких системах радиостанция при вызове сама ищет незанятый канал и занимает его. В дежурном режиме радиостанция непрерывно перебирает (сканирует) все каналы системы, проверяя, не вызывают ли ее на одном из них. К таким СТРС относятся некогда распространенная в СССР система «Алтай», а также система SMARTRUNK II.

Сканирующие СТРС просты и дешевы. В этих системах возможна полная независимость каналов БСТ друг от друга, поскольку их объединение в общую СТРС происходит на уровне абонентской

радиостанции. Это обуславливает высокую надежность и живучесть сканирующих СТРС.

Таким СТРС присущ ряд недостатков. С ростом количества каналов быстро возрастает длительность установления соединения в такой системе, так как она не может быть меньше длительности полного цикла сканирования. Реально к этому добавляется еще и длительность поиска свободного канала вызывающей радиостанции. Кроме того, в сканирующих СТРС затруднительна реализация многих современных требований, в числе которых многозоновость, гибкая и надежная система приоритетов, постановка на очередь при занятости системы или вызываемого абонента и так далее. Сканирующая СТРС идеально подходит в качестве небольшой (до 200 абонентов) однозоновой системы связи, к которой предъявляются минимальные требования.

СТРС с распределенным управляющим каналом. Такими являются распространенная в США система LTR, разработанная еще в конце семидесятых годов фирмой E. F. Johnson, и ее современная модификация ESAS, предлагаемая фирмой UNIDEN. В этих СТРС управляющая информация передается непрерывно по всем каналам, в том числе и по занятым. Это достигается использованием для ее передачи частот ниже 300 Гц. Каждый канал является управляющим для радиостанции, закрепленной за ним. В дежурном режиме радиостанция прослушивает свой управляющий канал. В этом канале БСТ непрерывно передает номер свободного канала, который радиостанция может использовать для передачи. Если же на каком-либо канале начинается передача, адресованная одной из радиостанций, то информация об этом передается на ее управляющем канале, в результате чего эта радиостанция переключается на канал, где происходит вызов.

Такие СТРС обладают рядом достоинств, присущих СТРС с управляющим каналом, не требуя в то же время выделения частот для него. В системе LTR установление соединения происходит на-

столько быстро, что оно осуществляется каждый раз при включении передатчика станции, т.е. в паузах разговора канал не занят.

Однако при выходе из строя какого-либо канала в системе LTR происходит отказ всех радиостанций, для которых он является управляющим. Кроме того, в таких СТРС скорость передачи управляющей информации крайне ограничена.

Это затрудняет реализацию многих требований, предъявляемых к современным СТРС, в том числе и многозоновости. Передача информации на частотах ниже 300 Гц одновременно с речью делает такие системы весьма критичными к точности регулировки. Все это привело к тому, что СТРС с распределенным управляющим каналом в настоящее время не разрабатываются. Исключение составляет лишь ESAS, в которой используется данный принцип ради совместимости с LTR.

СТРС с выделенным управляющим каналом. Для аналоговых систем речь идет о частотном канале, для цифровых – о временном разделении каналов. В таких СТРС радиостанция непрерывно прослушивает управляющий канал ближайшей к ней БСТ. При поступлении вызова БСТ передает информацию об этом по управляющему каналу, вызываемая радиостанция подтверждает прием вызова, после чего БСТ выделяет один из разговорных каналов для соединения и информирует об этом по управляющему каналу все участвующие в соединении радиостанции. После этого они переключаются на указанный канал и остаются на нем до окончания соединения. В то время, когда управляющий канал свободен, радиостанции могут передавать туда свои запросы на соединения. Некоторые типы вызовов (например, передача коротких пакетов данных между радиостанциями) могут осуществляться вообще без занятия разговорного канала.

СТРС с выделенным разговорным каналом в наибольшей степени отвечают современным требованиям. В них легко реализуется многозоновость (радиостанция выбирает БСТ с лучше всего принимаемым управляющим каналом) и другие функции. Среди них – по-

становка вызовов на очередь при занятости системы или вызываемого абонента. А это, в свою очередь, переводит такие СТРС из класса систем с отказом при занятости в класс систем с ожиданием. Тем самым не только повышается комфортность работы пользователя, но и, главное, увеличивается пропускная способность системы. В системах с отказом при занятости для обеспечения приемлемого качества сервиса в любой момент времени должен простаивать хотя бы один канал, чтобы абонент мог произвести вызов. В системе с ожиданием загружены могут быть все каналы. При этом, правда, вызывающему абоненту придется немного подождать в очереди.

Однако выделение отдельного управляющего канала имеет свои недостатки. Во-первых, это худшее использование частотного ресурса. В большинстве систем этот недостаток смягчается возможностью перевода управляющего канала в разговорный режим при перегрузке системы. Во-вторых, выделенный управляющий канал является уязвимым местом СТРС – при отсутствии специальных мер отказ оборудования БСТ для этого канала означает отказ всей БСТ. К тому же результату приводит и появление помехи на частоте приемника управляющего канала БСТ. По этой причине при разработке СТРС с выделенным управляющим каналом автоматическому контролю за работой оборудования БСТ уделяется особое внимание. При обнаружении отказа или длительной помехи на частоте приема БСТ делает управляющим другой исправный канал.

В главе 12 представлены требования по обеспечению информационной безопасности систем транкинговой радиосвязи при их использовании на ядерных объектах.

Системы радиосвязи с распределенным спектром частот

Наиболее высокую степень безопасности и помехоустойчивости обеспечивает технология передачи радиосигналов с распределенным спектром (широкополосный сигнал). Системы с распределенным

спектром применяются для связи в военных радиостанциях еще со времен второй мировой войны. Применение данной технологии для коммерческих нужд было разрешено с 1985 года. Сегодня технология распределенного спектра применяется в радиостанциях для связи сил охраны и в системах охранной сигнализации, в которых используется радиоканал для связи датчиков обнаружения с контрольными панелями. Применение данного метода для указанных выше целей является наиболее надежным и экономически выгодным решением проблемы безопасности радиоканалов связи.

Существует несколько технологий передачи информации с распределенным спектром частот. Одной из применяемых в системах связи для сил охраны является система со скачкообразным переключением несущей частоты.

В обычных системах радиосвязи с частотной модуляцией в узком диапазоне информация передается с использованием одной несущей частоты. В процессе передачи информации передатчик и приемник должны быть настроены на одну и ту же несущую частоту. Ширина полосы частот, используемых в таких системах, составляет 25 кГц.

Вместе с частотной модуляцией передаваемого сигнала система со скачкообразным переключением частоты распределяет передаваемые сигналы по полосе частот шириной 10 МГц. При использовании полосы частот шириной 10 МГц система создает, например, 400 дискретных радиочастотных каналов связи (400 отдельных несущих частот). Система передает модулированный сигнал информации, постоянно меняя несущую частоту передачи в заданном диапазоне рабочих частот в соответствии с псевдослучайным законом распределения. Для этого во всех компонентах системы связи имеются задающие генераторы. Все задающие генераторы радиостанций синхронизированы между собой. Продолжительность передачи сигнала на каждой из используемых несущих частот очень мала, и информация, передаваемая с использованием одной несущей частоты,

крайне мала. Для того чтобы заглушить сигнал подобной радиосистемы связи (400 разных несущих частот), потенциальным нарушителям понадобится 400 радиопередатчиков. Так как несущие частоты системы связи распределяются в соответствии с псевдослучайным законом, то отследить его и повторить с помощью одной радиостанции будет практически невозможно. На рис. 7.5 показаны спектр частот в традиционных системах радиосвязи с частотной модуляцией сигнала и спектр частот в системах связи со скачкообразным переключением несущей частоты.

Необходимо понимать, что спектр частот для системы связи со скачкообразным переключением несущей частоты приведен за некоторый интервал времени, т.е. сигнал не передается на всех несущих частотах одновременно.

Существующие системы радиосвязи со скачкообразным переключением несущей частоты имеют разное количество несущих частот, которое доходит до 2000.

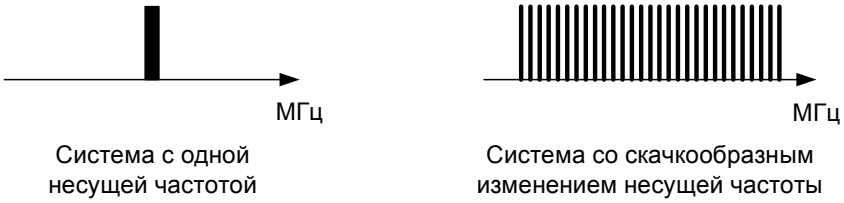


Рис. 7.5. Спектр частот узкополосной системы и системы со скачкообразным изменением частоты

7.4. Организация систем связи с использованием переносных радиостанций

Современные переносные радиостанции позволяют быстро передавать оперативные отчеты о результатах проверок в ходе патрулирования территории объекта и тем самым способствуют быстрому развертыванию сил ответного реагирования при обнаружении чрезвычайной ситуации на объекте. Типичная переносная радиостанция позволяет вести прием и передачу с использованием от одного до шести каналов связи (радиочастот). Максимальное расстояние, на котором обеспечивается надежная связь между двумя радиостанциями, составляет от 1 до 5 км на открытой местности. Применяются более мощные передатчики и более чувствительные приемники для установки в командном центре сил вооруженной охраны и на транспортных средствах. Такое оборудование позволяет обеспечить надежную связь на расстоянии 20 км и более.

Большинство используемых во всем мире систем радиосвязи представляют собой узкополосные радиосистемы открытой речевой связи с частотной модуляцией. Открытая речевая связь – передача речевых сигналов без кодирования или какой-либо иной защиты передаваемой информации. Нарушитель, располагающий приемником, настроенным на ту же частоту, может без труда прослушивать переговоры отрядов охраны, находясь в непосредственной близости от объекта. Для систем радиосвязи с частотной модуляцией характерны два существенных недостатка.

Переносные радиостанции имеют недостаточную дальность действия. Эта проблема решается либо установкой более мощных передатчиков на рациях, либо установкой радиоретрансляторов. Радиоретранслятор принимает сигналы, передаваемые переносными радиостанциями, и повторно передает их на другой частоте, на которую настроены приемники остальных элементов сети связи.

Если ретранслятор устанавливается на возвышенности, радиус действия радиостанций возрастает.

Второй недостаток радиосетей связи – большие здания и сооружения препятствуют прохождению радиосигнала. В этом случае непосредственно в здании устанавливается ретранслятор, соединенный кабельной линией связи с командным центром сил охраны. Подобная система связи позволяет существенно улучшить качество передаваемой информации, как от переносных радиостанций, так и от командного центра сил вооруженной охраны.

Современные радиосистемы связи на базе переносных радиостанций просто устроены, просты в обращении и достаточно эффективны. При условии соблюдения соответствующих инструкций использования систем радиосвязи, такие системы обеспечивают высококачественную передачу речевых сообщений и выполнение установленного периодического патрулирования территории объекта. Но, как было отмечено ранее, системы радиосвязи сил охраны могут подвергаться следующим «атакам» со стороны нарушителя: прослушивание сообщений, передача ложных сообщений и глушение радиосигнала.

Прослушивание и передача ложных сообщений. Применяемые в силах охраны каналы радиосвязи должны быть защищены от нарушителя, обладающего аппаратурой для несанкционированного прослушивания и использования радиочастот. Сообщения, передаваемые по простым каналам радиосвязи (амплитудная и частотная модуляция передаваемой информации), могут без труда приниматься нарушителем, пользующимся радиоприемником, настроенным на частоту сил охраны. Если частота канала связи неизвестна, то современные сканирующие приемники позволяют автоматически находить требуемую частоту за считанные минуты. Таким образом, при использовании простых каналов радиосвязи необходимо определить, какого рода информация может передаваться силами охраны в радиоэфир, и использовать этот канал связи, только если

это совершенно необходимо и важная информация не может быть передана с использованием более защищенных систем связи (например, по внутренней телефонной сети). Применение оборудования, защищающего системы радиосвязи от прослушивания, позволит решить и проблему передачи ложных сообщений на радиочастоте сил ответного реагирования. Если нарушители не могут понять закодированное цифровым оборудованием сообщение, то они не смогут передать ложное сообщение в нужной (закодированной) форме.

Защита радиоканала связи может быть обеспечена на различных уровнях и с использованием различных защитных технологий и систем. По мере повышения уровня защищенности системы, она становится все более сложной, требует все больших финансовых затрат, а также возрастает количество помех на линиях связи. Но даже при использовании самых современных и защищенных систем речевой радиосвязи следует учитывать возможность глушения передаваемого по радиоэфиру сигнала. Системы кодированной речевой радиосвязи не защищены от глушения.

Глушение – передача «пустых» (радиошум) сигналов на радиочастоте, которая используется для организации связи сил ответного реагирования, что приведет к смешиванию сигналов и блокированию канала связи. Глушение может осуществляться нарушителями с помощью передатчика, находящегося на значительном расстоянии от объекта. Используемые системой радиосвязи частоты могут быть определены нарушителями посредством прослушивания передач в непосредственной близости от объекта или ознакомления с широко распространенной и незасекреченной документацией по использованию подобных систем связи. Глушение не требует особых навыков или усилий – достаточно лишь настроить передатчик на соответствующую частоту. Если подавляющий сигнал обладает достаточной мощностью, прием истинного сигнала затрудняется до такой степени, что обеспечение надежной связи

становится чрезвычайно затруднительным или совсем невозможным. В самом простом случае глушение системы радиосвязи, в которой используются передающие на одной частоте переносные радиостанции, может быть осуществлено с помощью радиостанции такого же типа.

Сеть связи сил охраны будет устойчива к радиоглушению, если в распоряжении отрядов ответного реагирования имеются надежные альтернативные средства передачи информации, которыми можно быстро воспользоваться в любое время. При наличии дублирующих каналов связи и при эффективной отработке навыков их использования чувствительность системы связи к глушению будет существенно уменьшена.

В условиях глушения может произойти потеря радиосигналов, передаваемых с помощью маломощных (от 1 до 6 Вт) переносных радиостанций. Командный пост сил охраны можно оборудовать мощной стационарной передающей станцией (например, 100 Вт), что позволит без потери передавать информацию от командного поста к переносным радиостанциям. В этом случае будет поддерживаться односторонняя связь с отрядами охраны. Дежурный центральной станции должен понимать, что посылаемые им сообщения принимаются, и продолжать передачу важной информации. Для поддержки уже двухсторонней связи отряд ответного реагирования может использовать более мощную радиостанцию, установленную на автомобиле, либо использовать радиостанцию-ретранслятор, что позволит поддерживать связь с маломощными переносными радиостанциями отрядов сил охраны, находящихся на небольшом расстоянии от ретранслятора.

Проблему глушения используемой силами охраны радиочастоты можно решить переключением на другую частоту всех средств связи. Таким образом, формируется требование, что все используемые силами охраны средства радиосвязи должны иметь как минимум две рабочих частоты. Метод переключения радиочастот

наиболее прост и эффективен. Рекомендуется использовать оборудование, способное поддерживать связь на четырех и более радиочастотных каналах, хотя такое техническое решение не всегда целесообразно и оправдано на практике.

Личный состав сил охраны должен знать, когда и на каком радиочастотном канале будет поддерживаться связь, что четко регламентируется инструкциями. Наиболее эффективным способом оповещения личного состава о необходимости переключения на заданный канал радиосвязи является передача специальных кодовых сообщений.

В данной главе ранее было дано описание систем радиосвязи с распределенным спектром частот. Эти системы позволяют свести к минимуму возможность прослушивания, передачи ложных сообщений и глушения радиосигнала сил охраны нарушителем.

7.5. Системы радиосвязи, используемые на объектах ядерной отрасли

На предприятиях ядерной отрасли России системы и средства радиосвязи используются в системах комплексной безопасности стационарных и подвижных ядерно-опасных объектов, в том числе в системах физической защиты.

Порядок создания, развертывания и эксплуатации систем радиосвязи на предприятиях Министерства Российской Федерации по атомной энергии определен в «Положении о порядке использования систем радиосвязи на предприятиях Минатома России» (далее в пределах данной главы – Положение) [7.3].

Под системами радиосвязи в данном случае понимаются радиосистемы (транкинговой связи, спутниковой связи, навигации, сигнализации, пейджинговые, передачи данных) и радиоэлектрон-

ные средства (РЭС) (радиостанции, радиотелефоны, радиоудлинители, ретрансляторы, радиомодемы), а также комплекс организационно-технических мероприятий по использованию и поддержанию в требуемом состоянии этих радиосистем и РЭС.

Требования Положения являются обязательными для всех предприятий и закрытых административно-территориальных образований (ЗАТО) Минатома России, а также для дислоцированных на их территориях организаций и предприятий всех форм собственности, участвующих в обеспечении безопасности ЯО.

Положение разработано с учетом требований: законов Российской Федерации, постановлений Правительства Российской Федерации, положений Государственного Комитета по радиочастотам Российской Федерации (ГКРЧ) и решений Главного управления Государственного надзора за связью в Российской Федерации (Госсвязьнадзор России).

Использование на ЯО средств и систем радиосвязи предназначено для достижения следующих целей:

- повышение эффективности системы комплексной безопасности предприятий;
- усиление физической защиты стационарных и подвижных ядерно-опасных объектов;
- повышение эффективности оперативного управления и взаимодействия служб безопасности предприятия, сил охраны, а также подразделений, привлекаемых для выполнения совместных работ в случае возникновения нештатных ситуаций.

Указанные выше цели достигаются за счет:

- обеспечения радиосвязью служб безопасности, жизнеобеспечения и подразделений, привлекаемых к ликвидации нештатных ситуаций на объекте;

- обеспечения радиосвязью подразделений охраны ядерно-опасных объектов, осуществляющих также охрану спецпродукции в процессе ее транспортировки;
- обеспечения взаимодействия подразделений ведомств и структур, задействованных в обеспечении комплексной безопасности ядерно-опасных объектов, в том числе включая нештатные (аварийные) ситуации;
- передачи телеметрической информации по радиоканалу с объектов контроля;
- оповещения персонала при возникновении нештатных ситуаций и передачи по радиоканалу информации о нештатной ситуации при транспортировке специальных ядерных материалов.

Принятие положительного решения об организации на ЯО новой радиосвязи возможно только в тех случаях, когда на требуемом направлении отсутствуют средства проводной и радиосвязи общего назначения, или эти средства не обеспечивают потребности предприятия для решения поставленных задач.

Тактико-технические характеристики приобретаемых и используемых на ЯО систем радиосвязи и радиоэлектронных средств должны соответствовать требованиям действующих ГОСТов и нормативных документов ГКРЧ России и обеспечивать в зависимости от назначения:

- оперативную связь при произвольном перемещении абонентов по территории объекта;
- передачу речевых сообщений и выход в городские, местные и учрежденческие АТС;
- передачу данных;
- индивидуальный вызов, групповой вызов, экстренный вызов абонентов сети связи;

- оперативную модификацию параметров системы: подключение и отключение абонентов, изменение их прав доступа, разрешенная длительность связи, исключение утерянных или похищенных радиосредств;
- автоматизм вхождения и обеспечение связи при убытии транспортного средства с одного объекта следования, в пути следования, а также при прибытии в пункт назначения;
- учет использования абонентами эфирного времени, очередность обслуживания;
- возможность регистрации (контроля) ведущихся по радиосистемам переговоров;
- возможность сопряжения с аналогичными радиосистемами подразделений министерств и ведомств, привлекаемых для проведения совместных работ, включая аварийные (нештатные) ситуации.

Используемые в СФЗ радиоэлектронные средства должны иметь сертификаты соответствия Госкомсвязи России, а также должны быть сертифицированы по требованиям безопасности информации в системах сертификации средств защиты информации, функционирующих в России.

Приобретение, использование и эксплуатация систем радиосвязи должны осуществляться по согласованию с соответствующим органом исполнительной власти.

Согласование возможности применения средств радиосвязи на предприятиях отрасли, выделение необходимого частотного ресурса для радиосредств, разрешенных к использованию, организация ведомственного контроля за эксплуатацией радиосредств в отрасли осуществляются на отраслевом уровне.

Ответственность за организацию, развертывание, использование и эксплуатацию систем радиосвязи на ЯО возлагается на руководителей предприятий. При этом руководители предприятий, на которых внедряются или внедрены системы радиосвязи, обязаны обеспечить весь комплекс существующих требований в точном соответствии с назначением радиоэлектронных средств и условиями их эксплуатации. На предприятии должны быть назначены должностные лица, ответственные за регистрацию, хранение, установку и эксплуатацию РЭС. На каждом конкретном объекте должны быть разработаны и приняты к исполнению инструкции, конкретизирующие порядок использования радиосистем и радиосредств, с учетом конкретных особенностей функционирования этих объектов, условий размещения радиосредств и уровня конфиденциальности циркулирующей в них информации.

Порядок назначения и присвоения радиочастот к использованию радиоэлектронных средств на объектах Минатома определяется Положением.

Создание систем радиосвязи на ЯО должно представлять собой комплекс работ, включающих:

- предпроектное обследование;
- разработку технического задания (ТЗ);
- представление заявок на радиочастотные присвоения и получение конкретных радиочастот для создаваемых систем;
- выбор предприятий, осуществляющих проектные и монтажные работы;
- разработку организационно-распорядительной и рабочей (эксплуатационной) документации систем радиосвязи;
- приемку и аттестацию систем радиосвязи.

Предпроектное обследование условий развертывания планируемых систем радиосвязи включает в себя:

- определение задач, решаемых с использованием радиосистем;
- определение емкости проектируемой системы радиосвязи (максимальное число объектов, групп абонентов, каналов радиосвязи, зон, подключаемых каналов общего пользования);
- сравнительный анализ существующих радиосистем и протоколов связи;
- оценку электромагнитной обстановки на объекте;
- анализ возможности установления уверенной связи между абонентами независимо от их местонахождения, определение зон уверенного приема;
- анализ возможности комплексирования проектируемой системы с существующими каналами общего пользования и сетями передачи данных;
- анализ возможного проектируемого, предполагаемого графика радиосвязи;
- определение возможных мест размещения базового оборудования;
- определение необходимости обеспечения конфиденциальности связи;
- определение требований по времени установления соединений;
- определение требований по надежности и климатическим воздействиям на РЭС.

По результатам предпроектного обследования определяется архитектура построения системы радиосвязи, проводится выбор типа используемого оборудования и разрабатывается ТЗ на создание системы связи. При выборе оборудования должен отдаваться

приоритет отечественным средствам связи, а при их отсутствии – зарубежным средствам, которые включены в решения ГКРЧ для использования на ЯО и имеют соответствующие сертификаты.

Техническое задание на систему связи должно включать в себя:

- назначение и цели разработки;
- состав системы;
- перечень выполняемых функций и предоставляемых услуг;
- этапы и сроки разработки системы;
- требования по организации связи;
- требования к частотному обеспечению;
- требования по сопряжению с сетями общего пользования;
- требования по предотвращению несанкционированного доступа и защите информации в системе;
- требования к режиму приоритетной передачи информации и порядку работы системы радиосвязи в нештатных ситуациях;
- требования по обеспечению радиоконтроля за переговорами, по регистрации или документированию сообщений, передаваемых в системе;
- требования к системе по обеспечению взаимодействия радиосредств ведомств и структур, задействованных в обеспечении комплексной безопасности ЯО;
- требования по сертификации оборудования;
- требования к системе гарантированного электропитания;
- требования по надежности и эргономике;
- перечень нормативных документов, с учетом которых разработано ТЗ.

Техническое задание должно быть утверждено заказчиком системы радиосвязи и согласовано с исполнителями работ.

Проектные и монтажные работы по вводу радиоэлектронных средств в эксплуатацию должны осуществляться предприятиями и организациями, имеющими лицензию на данный вид деятельности, а для выполнения работ на ЯО – лицензию Госатомнадзора России на проведение работ на таких объектах и лицензию Федеральной службы безопасности на право проведения работ со сведениями, составляющими государственную тайну.

Организационно-распорядительная и рабочая (эксплуатационная) документация на систему радиосвязи предприятия (объекта) должна включать:

- инструкции по эксплуатации, включающие: порядок организации связи, режимные требования, регламент связи, требования по регистрации радиотрафика, порядок проведения регламентных работ;
- порядок использования радиосредств в аварийных и нештатных ситуациях;
- инструкции по программированию оборудования системы радиосвязи;
- приказ о назначении ответственных лиц и администратора системы;
- должностные инструкции ответственных лиц;
- перечень сведений, разрешенных к открытой передаче по каналам радиосвязи.

Эксплуатация систем радиосвязи и радиоэлектронных средств на предприятиях и в организациях должна осуществляться в строгом соответствии с требованиями нормативно-технической документации и требованиями Положения.

У лиц, ответственных за эксплуатацию систем радиосвязи, должна иметься следующая документация:

- Положение;
- разрешение на эксплуатацию радиостанции и радиосети предприятия, выданное Госсвязьнадзором России;
- список лиц, имеющих право ведения переговоров по радиоканалу, утвержденный руководителем предприятия.

Абоненты системы радиосвязи должны иметь при себе разрешение на эксплуатацию портативных индивидуальных радиостанций при использовании их вне территории объекта.

При пользовании радиосвязью категорически запрещается передача сведений, не разрешенных к передаче открытым текстом, по каналам радиосвязи через радиостанции всех назначений, не оснащенные соответствующей защитной аппаратурой.

В случае хищения или утраты средств радиосвязи пользователь обязан немедленно сообщить об этом лицу, ответственному за регистрацию, хранение, установку и эксплуатацию РЭС. Ответственный за эксплуатацию системы должен принять необходимые меры для исключения негативных последствий.

Вопросы для самоконтроля

1. Какие функции выполняют силы ответного реагирования?
2. Какие тактические методы успешного выполнения задач силами ответного реагирования Вам известны?
3. Как обеспечивается связь сил ответного реагирования?
4. Какие существуют проблемы организации радиосвязи сил ответного реагирования?

5. Какие существуют методы построения систем радиосвязи?

6. Каковы особенности и возможности использования систем транкинговой радиосвязи?

7. Объясните принцип работы систем радиосвязи со скачкообразным изменением несущей частоты.

8. Каковы преимущества использования систем радиосвязи со скачкообразным изменением несущей частоты относительно традиционных (с частотной модуляцией) систем радиосвязи?

9. Каковы цели создания и назначение систем радиосвязи на предприятиях ядерной отрасли?

10. Опишите комплекс мероприятий по созданию систем радиосвязи на ЯО.

11. Какие существуют особенности эксплуатации систем радиосвязи на ЯО?

8. ОСОБЕННОСТИ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ

С точки зрения безопасности объекта, ядерный объект (ЯО) имеет определенную специфику, обусловленную, прежде всего, наличием ядерных материалов (ЯМ), ядерных энергетических установок (ЯЭУ) и различных технологических процессов с ЯМ.

В данном случае необходимо определить нормативно-правовую основу обеспечения физической защиты ЯО, уточнить термины и определения, сформулировать цели и задачи СФЗ ЯО и общие принципы создания таких систем, выявить специфику угроз и особенности модели потенциального нарушителя, определить порядок создания и совершенствования СФЗ ЯО, дифференцировать требования по физической защите ЯО, определить организационные мероприятия по обеспечению физической защиты и рассмотреть типовые структуры СФЗ ЯО. В данной главе будут рассмотрены указанные выше вопросы [П.1, П.2, 8.1-8.3].

8.1. Нормативно-правовые основы обеспечения физической защиты ядерных объектов

Физическая защита ядерных объектов (ядерных материалов, ядерных установок и пунктов хранения ядерных материалов) – вид деятельности в области использования атомной энергии, осуществляемый с целью предотвращения несанкционированных действий в отношении ядерных материалов, ядерных установок и пунктов хранения ядерных материалов.

Нормативное и правовое обеспечение физической защиты ядерных объектов формируют две группы документов: федерального и отраслевого уровня.

В первую группу входят следующие документы:

1.Федеральный закон Российской Федерации «Об использовании атомной энергии» от 21.11.95 № 170-ФЗ.

2.Закон Российской Федерации «О государственной тайне» от 21.07.93 № 5485-1.

3.Федеральный закон Российской Федерации «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ.

4.Закон Российской Федерации «О сертификации продукции и услуг» от 10.06.93 № 5151-1 и Федеральный закон Российской Федерации «О внесении изменений и дополнений в Закон Российской Федерации «О сертификации продукции и услуг» от 31.07.98 № 154-ФЗ.

5.Федеральный закон Российской Федерации «О ведомственной охране» от 14.04.99 № 77-ФЗ.

6.Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов. Утверждены постановлением Правительства Российской Федерации от 19.07.2007 № 456.

7.Положение о Министерстве Российской Федерации по атомной энергии. Утверждено постановлением Правительства Российской Федерации от 05.04.97 № 392.

Во вторую группу входят нормативные документы, ранее (до 2004 г.) разработанные в Министерстве Российской Федерации по атомной энергии (Минатом России) и в Федеральном надзоре России по ядерной и радиационной безопасности (ГАН — Госатомнадзор России), и документы, которые разрабатываются и будут приняты Федеральным агентством Российской Федерации по атомной энергии и Федеральной службой Российской Федерации по атомному надзору.

Особо важно отметить, что любые требования ведомственных нормативных актов должны быть не ниже требований, установленных нормативными актами федерального уровня.

Дальнейшее рассмотрение особенностей систем физической защиты ЯО базируется на документе «Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» (далее — Правила), утвержденном постановлением Правительства Российской Федерации.

Правила разработаны на основе законодательства Российской Федерации в области обеспечения безопасности при осуществлении ядерной деятельности и с учетом международных обязательств Российской Федерации и рекомендаций МАГАТЭ по физической защите ядерных материалов и ядерных установок.

Правила устанавливают требования к организации и обеспечению физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов на всей территории Российской Федерации, обязательные для выполнения всеми юридическими лицами, осуществляющими ядерную деятельность, независимо от форм собственности, источников финансирования и ведомственной принадлежности, федеральными органами исполнительной власти, обеспечивающими, координирующими и контролирующими ядерную деятельность, а также осуществляющими надзор за этой деятельностью.

Правила регулируют отношения, возникающие в процессе организации и обеспечения физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов, и распространяются на организацию и обеспечение физической защиты ядерных материалов, изделий на их основе, ядерных установок и пунктов хранения ядерных материалов как мирного, так и военного назначения.

В соответствии с Правилами устанавливаются следующие требования.

•Обеспечение физической защиты должно быть предусмотрено и осуществляться на всех этапах жизненного цикла ядерной

установки и пункта хранения ядерных материалов: при их создании, эксплуатации и выводе из эксплуатации, при обращении с ядерными материалами, а также при их транспортировке.

•Ядерная деятельность без обеспечения физической защиты в соответствии с требованиями настоящих Правил запрещается.

8.2. Термины и определения

В Правилах даны определения следующих понятий:

«анализ уязвимости» — осуществляемый на ядерном объекте процесс выявления уязвимых мест ядерной установки, пункта хранения ядерных материалов и технологических процессов использования и хранения ядерных материалов, исходя из принятых угроз, а также определения вероятных способов осуществления угроз и моделей нарушителей;

«диверсия» — преднамеренное действие в отношении ядерных материалов, ядерных установок, пунктов хранения ядерных материалов или транспортных средств, перевозящих ядерные материалы и ядерные установки, способное привести к аварийной ситуации и создать угрозу здоровью или жизни людей в результате воздействия радиации или привести к радиоактивному загрязнению окружающей среды;

«допуск» — оформленное в установленном порядке разрешение на проведение определенной работы или на получение определенных документов и сведений;

«зона ограниченного доступа» — зона, не содержащая ядерных материалов I – III категории и ядерных установок, доступ в которую ограничен и контролируется, в которой могут размещаться элементы и системы, обеспечивающие безопасность ядерного объекта или его системы физической защиты;

«инженерно-технические средства физической защиты» — совокупность инженерных и технических средств, предназначенных для решения задач физической защиты;

«контрольно-пропускной пункт (пост)» — специально оборудованное на границе охраняемой зоны место для осуществления контроля и управления проходом людей и проездом транспортных средств в порядке, установленном пропускным режимом;

«международная транспортировка ядерных материалов» — транспортировка ядерных материалов любыми видами транспортных средств, связанная с пересечением границы государства-грузоотправителя, в том числе, транзит по территории других государств;

«модель нарушителя» — формализованные сведения о численности, оснащенности, подготовленности, осведомленности и тактике действий 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 несанкционированное действие, а также лицо, оказывающее ему содействие в этом;

«нейтрализация нарушителя» — реализация совокупности действий системы физической защиты по отношению к нарушителю, в результате чего он лишается возможности продолжать несанкционированные действия;

«несанкционированное действие» — совершение или попытка совершения диверсии, хищения ядерных материалов, несанкционированного доступа, проноса (провоза) запрещенных предметов, вывода из строя или нарушения функционирования отдельных элементов системы физической защиты;

«несанкционированный доступ» — проникновение в охраняемые зоны, здания, сооружения, помещения или в грузовые

отсеки транспортных средств, перевозящих ядерные материалы, лиц, не имеющих на это права, или с нарушением установленного порядка;

«охраняемая зона» — территория ядерного объекта или ее часть, оборудованная инженерно-техническими средствами физической защиты, находящаяся под охраной, доступ в которую ограничен и контролируется;

«периметр» — граница охраняемой зоны, оборудованная инженерно-техническими средствами физической защиты и контрольно-пропускными пунктами (постами);

«персонал физической защиты» — лица, в должностные обязанности которых входит выполнение функций по обеспечению физической защиты на конкретном ядерном объекте;

«правило двух (трех) лиц» — принцип групповой работы, основанный на требовании одновременного присутствия на одном рабочем месте не менее двух (трех) человек, обладающих соответствующими полномочиями, для снижения возможности несанкционированных действий;

«пропускной режим» — совокупность организационных и технических мероприятий, установленных правил, направленных на недопущение бесконтрольного доступа людей (персонала, посетителей, командированных лиц и т.д.) и пропуска транспортных средств, а также перемещения предметов, материалов и документов через контрольно-пропускные пункты (посты) в охраняемые зоны (в том числе, здания, сооружения, помещения) и обратно;

«противотаранное устройство» — заграждение, предназначенное для принудительной остановки транспортного средства;

«пункт хранения ядерных материалов» — не относящиеся к ядерным установкам стационарный объект или сооружение, предназначенные для хранения ядерных материалов;

«пункт управления системы физической защиты» — специально оборудованное и оснащенное техническими средствами помещение (место), с которого специально назначенный персонал физической защиты в полном объеме или частично осуществляет управление инженерно-техническими средствами физической защиты в штатных и чрезвычайных ситуациях;

«санкционированный доступ» — проход (проезд) в охраняемые зоны, здания, сооружения, помещения ядерного объекта в порядке, установленном пропускным режимом (далее — доступ);

«сертификат-разрешение» — документ, выдаваемый государственным компетентным органом по ядерной и радиационной безопасности при перевозках ядерных материалов, радиоактивных веществ и изделий из них для подтверждения соответствия транспортного упаковочного комплекта и условий транспортирования установленным требованиям по безопасности;

«система физической защиты» — совокупность персонала физической защиты, осуществляемых им организационно-технических мероприятий, действий и инженерно-технических средств, предназначенная для реализации физической защиты на ядерном объекте;

«служба безопасности» — структурное подразделение ядерного объекта, предназначенное для организации и контроля за выполнением мероприятий по обеспечению физической защиты и иных функций, определенных федеральными и ведомственными нормативными документами;

«транспортное защитное устройство» — устройство, предназначенное для размещения, закрепления и транспортирования в нем упакованного ядерного материала с обеспечением его защиты от внешних, в том числе и аварийных поражающих воздействий заданного уровня при транспортировке;

«угроза» — совокупность условий и факторов, создающих возможность совершения хищения ядерного материала или диверсии;

«уязвимые места» — элементы систем (оборудование или устройства) ядерной установки или пункта хранения ядерных материалов, несанкционированные действия, в отношении которых могут привести к хищению ядерных материалов или создать угрозу здоровью или жизни людей;

«физический барьер» — физическое препятствие, создающее задержку проникновению нарушителя в охраняемые зоны или к уязвимым местам;

«ядерная деятельность» — деятельность, связанная с производством, использованием, хранением, утилизацией и транспортировкой ядерных материалов, вводом в эксплуатацию, эксплуатацией и выводом из эксплуатации ядерных установок и пунктов хранения ядерных материалов;

«ядерная установка» — содержащие ядерные материалы: сооружение, комплекс, устройство, предназначенные для проведения испытаний (исследований), производства, использования и переработки ядерных материалов, производства или использования атомной энергии;

«ядерный объект» — предприятие (организация, воинская часть), на территории которого используется или хранится ядерный материал либо размещается и (или) эксплуатируется ядерная установка или пункт хранения ядерных материалов, в том числе используемые, хранимые или размещаемые на отдельных территориях (площадках);

«ядерный материал» — материал, содержащий или способный воспроизвести делящиеся (расщепляющиеся) ядерные вещества.

8.3. Цели и задачи системы физической защиты ядерного объекта

Система физической защиты создается на ЯО для обеспечения защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов. При этом задачами физической защиты являются:

- предупреждение несанкционированных действий;
- своевременное обнаружение несанкционированного действия;
- задержка (замедление) проникновения (продвижения) нарушителя;
- реагирование на несанкционированные действия и нейтрализация нарушителей для пресечения несанкционированных действий.

Предупреждение несанкционированных действий и обеспечение санкционированного доступа достигается путем информирования местного населения и персонала ЯО о степени безопасности функционирования ЯО, эффективности его СФЗ, ответственности за несанкционированные действия по отношению к ЯМ, ЯУ и другим предметам физической защиты в соответствии с законодательством Российской Федерации; организации пропускного режима на ЯО и допуска на него персонала, командированных лиц и посетителей; организации оборудования периметров охраняемых зон инженерно-техническими средствами физической защиты; выявления лиц, причастных к подготовке диверсий или хищений ЯМ, а также несанкционированных действий по отношению к другим предметам физической защиты (совместно с органами ФСБ России и МВД России).

Своевременное обнаружение несанкционированных действий или попытки совершения диверсии, хищения ЯМ, несанкционированного доступа, проноса (провоза) запрещенных

предметов, вывода из строя средств физической защиты достигается путем организации охраны периметров охраняемых зон, контрольно-пропускных пунктов и отдельных объектов; применения систем охранной сигнализации и систем оптико-электронного наблюдения; досмотра персонала, командированных лиц, посетителей и их вещей, в том числе с применением средств обнаружения проноса ЯМ, взрывчатых веществ и предметов из металла; своевременного выявления умышленного вывода из строя инженерно-технических средств СФЗ; обеспечения пропускного и внутриобъектового режима на ЯОО; монтажа и эксплуатации инженерно-технических средств СФЗ в строгом соответствии с проектной и эксплуатационной документацией; контроля их состояния и работоспособности; проведения учебы, разъяснительной работы и профилактики по обнаружению несанкционированных действий и оповещению сил реагирования СФЗ персоналом ЯО.

Задержка (замедление) проникновения (продвижения) нарушителя к месту совершения диверсии или хищения ЯМ достигается путем установки физических барьеров на возможных маршрутах проникновения нарушителя к местам совершения диверсий или хищения ЯМ, позволяющих задержать нарушителя на время, достаточное для прибытия сил охраны; выполнения подразделениями охраны и службы безопасности ЯО действий по задержке продвижения нарушителей к месту совершения диверсии или хищения ЯМ.

Реагирование на несанкционированные действия и нейтрализация нарушителей для пресечения несанкционированных действий достигается путем действий подразделений охраны и безопасности, а также, в случае необходимости, внешних сил реагирования (региональных, федеральных) по предотвращению несанкционированного доступа в охраняемые зоны и нейтрализации нарушителей, проникших в охраняемые зоны;

применения в установленных законодательством случаях средств нелетального воздействия на нарушителей в целях временного вывода их из строя; задержания лиц, причастных к подготовке или совершению диверсии или хищения ЯМ; взаимодействия администрации, службы безопасности и подразделений охраны ЯО с органами ФСБ России и МВД России в целях задержания нарушителей.

В дополнение к основным задачам в рамках СФЗ в целях их эффективного решения должны выполняться обеспечивающие задачи по разработке правового и нормативного обеспечения СФЗ; анализу уязвимости ЯО и оценке эффективности СФЗ, подготовке на их основе предложений по совершенствованию СФЗ; защите информации в СФЗ; обеспечению подготовки персонала СФЗ к решению задач по физической защите ЯО; эксплуатации инженерно-технических средств.

Физической защите подлежат следующие элементы (предметы физической защиты — ПФЗ):

- ядерные материалы, в том числе изделия на их основе;
- ядерные установки и/или их уязвимые элементы, выявленные в процессе анализа уязвимости ядерного объекта;
- пункты хранения ядерных материалов и/или их уязвимые элементы, выявленные в процессе анализа уязвимости ядерного объекта.

Кроме этого на ЯО должна быть обеспечена защита систем, элементов и коммуникаций ядерного объекта, не относящихся к ядерной установке или пункту хранения, в отношении которых в процессе анализа уязвимости выявлена необходимость предотвращения несанкционированных действий.

В самой системе физической защиты должна быть обеспечена защита информации, в том числе секретность (конфиденциальность) информации об организации, составе и

функционировании системы физической защиты, ее целостность и санкционированная доступность, нарушение которых может привести к снижению эффективности функционирования системы физической защиты в целом или ее отдельных элементов. Вопросам обеспечения информационной безопасности систем физической защиты ЯО будет посвящена отдельная глава учебника.

Для выполнения задач физической защиты администрация ядерного объекта обеспечивает с привлечением специализированных организаций создание, совершенствование и функционирование системы физической защиты, в том числе:

- проведение анализа уязвимости ядерного объекта;
- оценку последствий несанкционированных действий в отношении предметов физической защиты;
- категорирование предметов физической защиты, помещений (а при необходимости — зданий, сооружений) и ядерного объекта в целом;
- выделение охраняемых зон, зон ограниченного доступа и определение мест размещения предметов физической защиты в соответствующей зоне (здании, сооружении, помещении);
- определение и создание системы охраны ядерного объекта;
- оценку эффективности системы физической защиты и определение путей ее совершенствования;
- формирование и задание конкретных требований к системе физической защиты на основании требований настоящих Правил, федеральных норм и правил и ведомственных нормативных актов;
- разработку документов объектового уровня;
- планирование и организацию функционирования системы физической защиты, в том числе эксплуатацию инженерно-технических средств физической защиты;

•проведение контроля за соблюдением требований по физической защите.

8.4. Общие принципы создания системы физической защиты ядерного объекта

Принципы построения СФЗ направлены на достижение ее эффективности, которая определяется способностью СФЗ противостоять действиям нарушителей в отношении ЯМ, ЯУ и других ПФЗ с учетом перечня угроз и моделей нарушителей для конкретного ЯО, определенных на этапе проведения анализа уязвимости.

При построении СФЗ необходимо руководствоваться следующими принципами:

•зонального построения;

•равнопрочности;

•обеспечения надежности и живучести;

•адаптивности;

•регулярности контроля функционирования;

•адекватности.

Принцип зонального построения СФЗ предусматривает организацию и создание охраняемых зон, обеспечивающих «эшелонированную» защиту ПФЗ. На ЯО следует выделять защищенную (ЗЗ), внутреннюю (ВЗ) и особо важную (ОВЗ) зоны, в которых размещаются или хранятся ЯМ или проводятся работы с ними, а также зоны ограниченного доступа (ЗОД), доступ в которые ограничивается из-за расположения в них жизненно важных для объекта и его систем безопасности элементов, но в которых ЯМ и ЯУ отсутствуют.

Принцип равнопрочности обеспечивает при его реализации требуемый уровень эффективности СФЗ для всех выявленных в процессе анализа уязвимости типов нарушителей, способов совершения несанкционированных действий и маршрутов движения. Равнопрочность СФЗ должна обеспечиваться с точки зрения предотвращения несанкционированного доступа; обнаружения попытки совершения несанкционированных действий; пресечения несанкционированных действий и задержания нарушителей для различных ситуаций; утечки информации. Требуемый уровень эффективности СФЗ должен уточняться при создании и совершенствовании СФЗ с учетом категории ЯО и критерия «эффективность — стоимость». Равнопрочность СФЗ должна обеспечиваться по всему периметру охраняемой зоны (для заданного категорированного помещения или группы помещений), включая контролируемые проходы и/или контрольно-пропускные пункты.

Принцип обеспечения надежности и живучести отражает способность СФЗ выполнять задачи в штатных и чрезвычайных ситуациях, в том числе в условиях аварийной ситуации на ЯО в пределах проектной аварии и ликвидации ее последствий.

Нарушение функционирования отдельных элементов СФЗ не должно приводить к нарушениям функционирования СФЗ в целом. Для повышения надежности и живучести СФЗ должны использоваться соответствующие технические решения и организационные меры. Должно быть обеспечено резервирование

элементов СФЗ. Резервирование отдельных функций может осуществляться за счет компенсационных мероприятий (с использованием персонала, технических и организационных мер). Для связи и передачи данных должны предусматриваться резервные каналы, в том числе с использованием альтернативных (носимых, световых, звуковых и т.п.) средств передачи информации. СФЗ следует строить на базе унифицированных модулей, обеспечивающих их структурную, конструктивную, логическую, информационную и электромагнитную совместимость при функционировании СФЗ. Организация эксплуатации инженерно-технических средств должна предусматривать реализацию системы планово-предупредительного технического обслуживания. Должны проводиться отбор и проверка благонадежности персонала ЯО, обучение, подготовка персонала службы безопасности ЯО и личного состава подразделений охраны к действиям в штатных и чрезвычайных ситуациях.

Принцип адаптивности обозначает возможность СФЗ адаптироваться к изменениям угроз и моделей нарушителей, в конфигурации объекта и границ охраняемых зон, видов и способов охраны, размещения ПФЗ. Система физической защиты должна иметь возможность образовывать дополнительные рубежи физической защиты. При этом должны сочетаться различные способы постановки/снятия периметров, зданий, сооружений, помещений под охрану как в автоматическом, так и в ручном режимах. СФЗ не должна создавать препятствий функционированию ЯО и должна адаптироваться к

технологическим особенностям работы ЯО, в том числе в чрезвычайных ситуациях с учетом принятых на нем мер ядерной, радиационной, технологической и пожарной безопасности.

Принцип регулярности контроля функционирования СФЗ реализуется на ведомственном уровне и на уровне ЯО. С целью определения эффективности СФЗ и отработки вопросов взаимодействия периодически должны проводиться учения, а также проводиться оценка эффективности СФЗ аналитическим и другими методами. Результаты оценки эффективности должны использоваться для совершенствования СФЗ. Комплекс ТСФЗ должен иметь в своем составе компоненты и встроенные элементы, позволяющие осуществлять постоянный дистанционный контроль состояния и работоспособности ТСФЗ и функционирования СФЗ в целом.

Принцип адекватности отвечает за то, чтобы принятые на ЯО организационные и административные меры, технические способы реализации физической защиты соответствовали бы принятым угрозам и моделям нарушителей. Реализация принципа адекватности обеспечивается путем проведения анализа уязвимости ЯО, категорирования ЯО, ПФЗ и мест их хранения и использования, выбора структуры и состава ИТСФЗ, определения способов охраны ЯО, оценки эффективности СФЗ, использования при создании и совершенствовании СФЗ критерия «эффективность — стоимость» и возможности применения компенсационных мер.

На основании указанных принципов устанавливаются требования к созданию и организации функционирования СФЗ. Однако перед тем, как сформулировать эти требования, необходимо уточнить перечень угроз и модель нарушителя безопасности ЯО.

8.5. Специфика угроз безопасности ядерного объекта

Наличие на объекте ядерных материалов приводит к появлению серьезных дополнительных специфических угроз безопасности ЯО и естественным образом определяет повышенные требования к защищенности ЯО. Предотвращение реализации именно этих угроз и является основной целью и задачей систем физической защиты ЯО.

В виду того, что неправильное обращение с ЯМ, вмешательство в работу ЯЭУ или нарушение технологических процессов с ЯМ может привести к очень серьезным последствиям, связанным с угрозой жизни и здоровью большого количества людей и экологической катастрофе, ЯО становятся привлекательной целью для различных экстремистских и террористических организаций или просто психически неуравновешенных людей. Тот же самый результат можно получить несанкционированным вмешательством (может даже непреднамеренным) неквалифицированного сотрудника ЯО в некий технологический процесс, следовательно, на территории ЯО должна четко и бесперебойно действовать система контроля и управления доступом, система обнаружения и т.д. Кроме того, ЯМ являются необходимым сырьем для производства ядерного оружия, которое для достижения своих политических целей хотели бы иметь многие страны третьего мира и международные террористические организации. Однако организация процесса производства ЯМ, готовых к применению в ядерном оружии, требует реализации сложных наукоемких технологий, больших экономических затрат и кроме того, это не пройдет не замечено для других стран. Поэтому возможность спланированного и организованного кем-то нападения на ЯО, с целью хищения уже готовых ЯМ, представляет определенную угрозу. Также хищение

ЯМ может производиться сотрудниками ЯО для продажи с целью обогащения.

Поэтому основными угрозами безопасности ЯО являются:

- вооруженное нападение на ЯО;
- тайное проникновение нарушителей на ЯО или его отдельные зоны;
- организация диверсий и террористических актов на ЯО;
- хищение ЯМ;
- подкуп или шантаж сотрудников ЯО для получения их помощи в хищении ЯМ или проникновении на ЯО.

Таким образом, функционирование СФЗ ЯО направлено на предотвращение проникновения нарушителей на ЯО, хищений ЯМ, а также несанкционированных действий в отношении ЯМ, ядерно-опасных изделий, установок или транспортных средств, перевозящих ЯМ.

При составлении списка возможных угроз реальному ЯО особую проблему, связанную с тем, что количество уже имевших место серьезных случаев преступных или враждебных действий на атомных объектах относительно невелико, представляет сбор необходимой информации. В данном случае необходимо накопить как можно больше информации, поступающей из различных источников. Рассмотрим некоторые из них.

Условия местной среды позволяют получить информацию об опасности, угрожающей тому или иному индивидуальному объекту. Следует учитывать как условия, существующие за пределами объекта, так и характеристики самого объекта. Внешние условия — например, общие настроения населения окружающего объект района, характер окружающей местности (густонаселенный, городской или малонаселенный, сельский), а также наличие в окружающем объект районе определенных организованных групп — могут послужить источником

информации о существующей угрозе. Условия на территории самого объекта — такие, как состав рабочей силы, характер трудовых отношений, правила взаимодействия с другими предприятиями, принципы взаимоотношений с представителями общественности, сознательность в том, что относится к обеспечению безопасности и охране объекта, наличие программ проверки и повышения надежности персонала — могут повлиять на характеристики возможной угрозы.

Изучение и определение характеристик местного и общенационального состава населения могут быть полезны при определении возможной угрозы определенному атомному объекту. Любая неудовлетворенная или враждебно настроенная существенная фракция населения должна быть изучена отдельно. При изучении такой фракции населения особое внимание следует уделять имеющим боевой опыт ветеранам вооруженных сил, опытным техническим специалистам, политическим экстремистам и людям, имевшим ранее доступ на территорию атомных объектов.

Можно указать некоторые характеристики объекта, более или менее привлекательные для нарушителя, который стремится использовать их в свою пользу. К ним относятся географические или конструкционные особенности объекта, привлекательность находящихся на территории объекта определенных целей, представление диверсанта об эффективности системы физической защиты.

В связи с существованием известных международных террористических организаций необходимо собирать информацию об угрозах как местного, так и национального и международного масштаба. К источникам такой информации относятся:

- разведывательные организации;
- криминологические исследования;
- профессиональные организации;

•публикуемая литература.

Разведывательные организации могут предоставить подробную информацию о текущей деятельности групп, способных представлять угрозу атомным объектам. Важно получать и изучать такую текущую информацию постоянно.

Криминологические исследования. Изучение преступлений, совершенных в районе атомного объекта, в национальном и в международном масштабе в прошлом и в недавнее время, часто позволяет извлечь полезную информацию, характеризующую потенциальные виды угрозы.

Профессиональные организации. Неправительственные структуры обмена информацией позволяют получить сведения, полезные при оценке существующей угрозы. Ученые, исследователи и промышленные специалисты встречаются, чтобы обсудить проблемы и технологические достижения. Часто обсуждаются также вопросы и проблемы, связанные с обеспечением безопасности. Может быть создана структура информационного обмена в области обсуждения проблем, угрожающих безопасности предприятия на местном, национальном и международном уровне.

Публикуемая литература. Тщательное изучение доступной текущей литературы может привести к накоплению информации, относящейся к оценке существующей угрозы. Такую информацию можно получить из общедоступных источников, из библиотек и от исследовательских организаций. К общедоступным источникам текущей литературы относятся бюллетени национальных информационных агентств и периодические издания, передаваемые по радио и телевидению новости, труды, посвященные определенным вопросам. Важно сравнивать получаемую информацию со сведениями о других странах. В библиотеках и у исследовательских организаций имеются электронные базы

данных, коллекции микрофильмов с выдержками из газет на определенные темы, справочные материалы по различным вопросам, значительно облегчающие поиск информации, имеющей отношение к потенциальной угрозе объекту.

8.6. Особенности модели нарушителя для систем физической защиты ядерного объекта

В качестве вероятных нарушителей могут выступать внешние и внутренние нарушители, а также внешние нарушители в сговоре с внутренними.

К внешним нарушителям относятся лица, не имеющие права доступа в защищаемую зону, действия которых направлены на проникновение на ядерно-опасный объект, хищение ядерных материалов, совершение диверсии в отношении ЯО и ЯМ или сбор разведданных о ЯО.

В качестве внутреннего нарушителя могут выступать лица из числа персонала СФЗ и посторонние лица, в том числе сотрудники подразделений ЯО, работающие в пределах ЯО, а также разработчики различных технологических и охранных систем, а также различные специалисты, привлекаемые для оказания услуг.

Все они имеют разного уровня допуск на территорию ЯО и возможность реализации угроз безопасности ЯО, в том числе с помощью технических средств.

Каждый из этих нарушителей отличается друг от друга уровнем осведомленности о функционировании основных жизнеобеспечивающих систем ЯО и его СФЗ, возможности, подготовленности и оснащенности к преодолению СФЗ в противоправных целях.

Внешние нарушители разделяются на силовую группу и одиночных нарушителей.

К внутренним нарушителям можно отнести:

•вспомогательных работников ЯО (дворники, сантехники и др.), имеющих ограниченный допуск в охраняемые зоны;

•основной персонал ЯО, допущенный в охраняемые зоны и к ПФЗ;

•персонал охраны и службы безопасности.

Нарушители каждой категории имеют свои сильные и слабые стороны. Например, нарушители из числа основного персонала ЯО не имеют оружия, не могут адекватно противостоять силам охраны, но допущены к предметам физической защиты, имеют высокую осведомленность. В качестве другого примера потенциальных нарушителей можно привести силы охраны, которые, хотя и имеют ограниченный санкционированный доступ в охраняемые зоны (например, в помещения), но вооружены и могут противостоять силам реагирования при обострении обстановки.

Как же формировать модель нарушителя в процессе работ на предпроектной стадии, в частности, при концептуальном проектировании?

На практике заполняется специальная анкета «Модель нарушителя и задачи охраны» по каждому помещению, принадлежащему определенной зоне ЯО. Анкета заполняется на объекте экспертной группой, в состав которой входят представители ЯО (служба безопасности, технологи, строители и т.п.), войсковых формирований, охраняющих ЯО, специализированной организации (аналитики), под методическим руководством которых и проводится данная работа.

Модель нарушителя разрабатывается с учетом расположения и функционирования конкретного ЯО для каждой защищаемой зоны, утверждается заказчиком и является основополагающим документом для оценки эффективности СФЗ объекта.

При разработке модели нарушителя учитываются:

- тип нарушителя;
- характер угроз;
- численность вероятного нарушителя, его вооружение и оснащенность;
- возможные способы преодоления рубежей и контроля доступа;
- решаемые нарушителем задачи;
- возможность доступа в жизненно-важные объекты СФЗ (пункты управления, «серверные», хранилища информации, узлы связи, к коммуникациям и к системе электропитания), к средствам защиты и техническим средствам СФЗ;
- полномочия внутреннего нарушителя;
- возможность совместных действий нарушителей различных типов.

В своей противоправной деятельности вероятный нарушитель может использовать средства воздействия на технические средства СФЗ и средства информатизации, финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей. В данном случае целесообразно выявить возможные мотивы нарушителей.

Мотивы, движущие потенциальными диверсантами, предпринимающими преступные действия по отношению к

атомным объектам, можно отнести к трем обобщенным категориям: идеологические мотивы, экономические мотивы, личные мотивы.

Идеологические мотивы непосредственно связаны с системами политических или философских убеждений. К руководствующимся политическими мотивами диверсантам можно отнести политических террористов, протестующих против атомной промышленности экстремистов, а также определенные группы философствующих или религиозных фанатиков. Такие идеологические диверсанты могут избрать своей целью атомный объект:

- в надежде повлиять на политику правительства в области использования атомной энергии или разработки ядерных вооружений;
- стремясь принудить правительство к изменению политики в других (не имеющих отношения к атомной энергетике или ядерному оружию) областях;
- стремясь подорвать доверие общественности к правительству и расшатать политические устои общества.

К экономическим мотивам относится стремление к обогащению. Преступники могут рассматривать хищение ядерных материалов или ядерного оружия как привлекательное средство получения выкупа, как ценный и редкий товар или как средство вымогательства.

Личные мотивы зависят от индивидуальных ситуаций, в которых оказываются те или иные люди. Личные мотивы к совершению преступления, связанного с ядерными материалами, могут быть самыми различными — от враждебного отношения служащего к своему нанимателю до непредсказуемых побуждений психически ненормального человека.

8.7. Требования к порядку создания и совершенствования систем физической защиты

Порядок создания и совершенствования систем физической защиты устанавливается федеральными нормами и правилами и (или) ведомственными нормативными актами.

Требования к системе физической защиты должны основываться на утвержденном перечне угроз и модели нарушителя, результатах анализа уязвимости ядерного объекта, оценки эффективности вариантов построения системы физической защиты и конкретизироваться в техническом задании на создание (совершенствование) системы физической защиты и задании на проектирование системы физической защиты.

Качество создания и функционирования системы физической защиты должно подтверждаться оценкой ее эффективности. Результаты оценки эффективности системы физической защиты должны использоваться для определения путей совершенствования системы физической защиты. Порядок (методика) проведения оценки эффективности системы физической защиты определяется ведомственными нормативными актами.

Создание, обеспечение функционирования системы физической защиты и ее совершенствование должны проводиться на основании единой системы планирования, координации, реализации и контроля комплекса организационных и технических мер, а также действий персонала физической защиты на ядерном объекте.

При создании (совершенствовании) системы физической защиты на ядерном объекте необходимо:

•учитывать особенности объекта и действующие на нем меры ядерной, радиационной, экологической, пожарной, технической, информационной и иных видов безопасности;

•ограничивать число лиц, имеющих доступ к ядерным материалам, ядерным установкам, к элементам и системам, важным для обеспечения безопасности ядерного объекта или его системы физической защиты, к информации об организации, составе и функционировании системы физической защиты;

•обеспечивать соответствие физической защиты принятым угрозам и моделям нарушителей;

•дифференцировать требования к организационно-техническим мерам обеспечения физической защиты в зависимости от категории предметов физической защиты.

8.8. Дифференциация требования по физической защите ядерного объекта

В целях дифференциации требований по физической защите и обеспечения адекватности системы физической защиты принятым угрозам и моделям нарушителей проводится категорирование предметов физической защиты и ядерного объекта в целом.

Категорирование представляет собой установленный порядок распределения предметов физической защиты по категориям, а ядерных объектов в целом — по типам и категориям.

В качестве критериев категорирования предметов физической защиты должны рассматриваться:

•категория ядерных материалов;

•степень секретности ядерных материалов, изделий на их основе и ядерных установок, определяемая в соответствии с ведомственными перечнями сведений, подлежащих засекречиванию;

•возможные последствия несанкционированных действий в отношении предметов физической защиты.

Категория ядерных материалов определяется видом, степенью облучения и массой ядерных материалов в соответствии с принятой классификацией.

Категорирование предметов физической защиты и оценка в отношении каждого из них последствий несанкционированных действий при реализации угроз проводятся на основе результатов анализа уязвимости ядерного объекта.

Порядок (методика) проведения анализа уязвимости ядерного объекта и проведения категорирования предметов физической защиты определяются ведомственными нормативными актами.

Порядок (методика) оценки последствий несанкционированных действий в отношении предметов физической защиты и категорирования ядерных установок по их потенциальной опасности определяется федеральными нормами и правилами в области использования атомной энергии и (или) ведомственными нормативными актами.

С учетом технологических и других особенностей использования, производства, переработки, хранения ядерных материалов и эксплуатации ядерных установок ядерные объекты относятся к следующим типам:

•объекты ядерно-оружейного комплекса;

•объекты атомной энергетики;

•объекты ядерно-топливного цикла;

•объекты атомной науки;

•судостроительные и судоремонтные заводы, на которых строятся и ремонтируются суда с ядерными энергетическими установками;

•объекты утилизации ядерных материалов и ядерных установок;

•пункты хранения ядерных материалов.

Один и тот же ядерный объект может относиться к различным типам.

Категорирование ядерного объекта проводится на основе категорирования предметов физической защиты, имеющихся на ядерном объекте, и отнесения ядерного объекта к соответствующему типу. Если ядерный объект может быть отнесен к нескольким типам, то при категорировании ядерного объекта принимается тип ядерного объекта, определяющий более высокую категорию ядерного объекта. Порядок (методика) проведения категорирования ядерного объекта определяется федеральными нормами и правилами и (или) ведомственными нормативными актами.

На ядерном объекте должно проводиться категорирование помещений, в которых размещаются предметы физической защиты, а при необходимости, категорирование зданий и сооружений. Категория помещения, здания, сооружения определяется как максимальная категория присутствующих в нем предметов физической защиты.

В зависимости от категории предметов физической защиты, особенностей ядерной установки и пункта хранения ядерных материалов на ядерном объекте выделяются и документально оформляются соответствующие охраняемые зоны (защищенные, внутренние и особо важные) и зоны ограниченного доступа.

8.9. Организационные мероприятия по обеспечению физической защиты ядерного объекта

Организационные мероприятия в рамках обеспечения физической защиты должны включать в себя комплекс мер, осуществляемых администрацией ЯО, и регламентирующие эти меры нормативные акты и организационно-распорядительные документы.

В рамках выполнения организационных мероприятий администрация ЯО обеспечивает разработку и утверждение в установленном порядке следующих документов объектового уровня:

- положения о разрешительной системе допуска и доступа к ядерным материалам, ядерным установкам и пунктам хранения ядерных материалов, к информации о функционировании системы физической защиты;
- инструкции о пропускном режиме;
- положения о внутриобъектовом режиме;
- положения о службе безопасности;
- положения о подразделении ведомственной охраны;
- плана охраны ядерного объекта;
- плана действий персонала физической защиты и персонала ядерного объекта в штатных и чрезвычайных ситуациях;
- плана взаимодействия администрации ядерного объекта, воинских частей (подразделений) внутренних войск МВД России с органами внутренних дел МВД России и органами ФСБ России в штатных и чрезвычайных ситуациях;
- плана проверки технического состояния и работоспособности инженерно-технических средств физической защиты.

Допускается объединение ряда документов в один документ с общим наименованием, разделы которого по составу и содержанию должны соответствовать приведенным в перечне документам.

Документы объектового уровня должны конкретизировать требования федеральных и ведомственных нормативных правовых актов по физической защите с учетом организационной структуры и особенностей функционирования ядерного объекта и не должны противоречить им.

8.10. Требования к инженерно-техническим средствам системы физической защиты ядерного объекта

Комплекс инженерно-технических средств СФЗ включает в себя инженерные и технические средства физической защиты.

К инженерным средствам физической защиты относятся физические барьеры, инженерное оборудование периметров охраняемых зон и постов охраны. Физическими барьерами являются строительные конструкции ядерного объекта (стены, перекрытия, ворота, двери), специально разработанные конструкции (заграждения, противотаранные устройства, решетки, усиленные двери, контейнеры) и другие физические, в том числе естественные, препятствия.

Комплекс технических средств физической защиты должен включать следующие основные функциональные системы:

- охранной сигнализации;
- тревожно-вызывной сигнализации;
- контроля и управления доступом;
- наблюдения и оценки ситуации;
- оперативной связи и оповещения;
- защиты информации;

•обеспечения (электропитания, освещения).

Устройства, используемые в составе комплекса технических средств физической защиты, могут обеспечивать реализацию требований, предъявляемых к одной или к нескольким функциональным системам (интегрированные системы и устройства).

Отказ или вывод из строя какого-либо элемента комплекса инженерно-технических средств физической защиты не должен нарушать функционирование системы физической защиты в целом. С этой целью должно быть предусмотрено резервирование элементов и функций комплекса инженерно-технических средств физической защиты.

Должна быть обеспечена бесперебойная работа технических средств физической защиты в случае отключения основного электропитания за счет автоматического переключения на резервные источники.

Требования к инженерным и техническим средствам физической защиты устанавливаются государственными и отраслевыми стандартами, а также ведомственными нормативными документами.

Периметр охраняемой зоны должен быть оснащен инженерно-техническими средствами физической защиты, обеспечивающими обнаружение несанкционированных действий, экстренный вызов сил реагирования, представление информации для оценки ситуации и задерживающими продвижение нарушителя к предметам физической защиты.

На путях наиболее вероятного прорыва нарушителя через периметр охраняемой зоны с использованием транспортных средств должны устанавливаться противотаранные устройства или приниматься другие меры, исключающие или существенно затрудняющие такой прорыв.

Для организации прохода людей и проезда транспортных средств на периметре охраняемой зоны должны оборудоваться контрольно-пропускные пункты (посты). Контрольно-пропускные пункты (посты) должны располагаться с учетом организации движения транспорта и прохода людей и обеспечивать требуемую пропускную способность.

На контрольно-пропускных пунктах (постах) должен осуществляться контроль правомочности прохода (проезда) и подтверждение подлинности проходящих лиц (проезжающих транспортных средств), обеспечиваться санкционированный доступ персонала ядерного объекта, посетителей и командированных лиц, и задержание нарушителей. Должны быть приняты меры по предотвращению несанкционированного проноса (провоза) ядерных материалов, взрывчатых веществ, холодного и огнестрельного оружия, других запрещенных предметов.

Контрольно-пропускные пункты (посты) должны быть оборудованы и (или) оснащены средствами защиты лиц, осуществляющих выполнение контрольных и пропускных функций, от поражения стрелковым оружием. Транспортные контрольно-пропускные пункты защищенной зоны должны оборудоваться противотаранными устройствами для задержания транспортных средств.

Все входы (выходы) в категорированные помещения (здания, сооружения) должны быть оборудованы средствами обнаружения, управления доступом и (при необходимости) наблюдения и оценки ситуации. Аварийные выходы должны обеспечивать беспрепятственный выход людей в чрезвычайных ситуациях.

Лица, проходящие через контрольно-пропускные пункты (посты), и их вещи могут быть досмотрены в установленном порядке, в том числе с применением средств обнаружения проноса запрещенных предметов.

Доступ и выполнение работ в особо важной зоне должны выполняться с применением правила двух (трех) лиц.

Требования по оборудованию периметров и контрольно-пропускных пунктов (постов) охраняемых зон, категорированных помещений (зданий, сооружений) инженерно-техническими средствами физической защиты, устанавливаются федеральными нормами и правилами и (или) ведомственными нормативными документами и уточняются на каждом конкретном объекте с учетом принятого перечня угроз, моделей нарушителей, результатов анализа уязвимости ядерного объекта и оценки эффективности системы физической защиты, а также категории ядерного объекта и особенностей выделения на нем охраняемых зон.

Основные требования к организации физической защиты при транспортировке ядерных материалов и ядерных установок изложены в отдельной главе данного пособия

В исключительных случаях при невозможности выполнения в полном объеме требований по обеспечению физической защиты на ядерном объекте, установленных Правилами и разработанными в соответствии с ними нормативными актами, администрация ЯО обязана принять необходимые компенсирующие мероприятия с использованием персонала физической защиты, технических средств и организационных мер. Достаточность компенсирующих мероприятий должна быть подтверждена оценкой эффективности системы физической защиты и согласована с федеральным органом исполнительной власти или организацией, в чьем подчинении находится ядерный объект, а также (при необходимости) с МВД России.

О каждом выявленном случае хищений ядерных материалов или совершения диверсии, попытки совершения таких действий и при обнаружении пропавшего ядерного материала администрация ЯО обязана в течение часа с момента выявления случившегося

сообщить в федеральный орган исполнительной власти, а также в организацию, в ведении которых находится данный объект, органы Федеральной службы безопасности Российской Федерации, органы Министерства внутренних дел Российской Федерации, уведомить федеральные органы исполнительной власти, осуществляющие государственный надзор, а затем в течение 10 дней представить письменные доклады в указанные органы федеральной власти и организации.

8.11. Типовые структуры системы физической защиты ядерного объекта

Современная СФЗ ЯО имеет свою функциональную, топологическую структуру, структуру управления и информационную структуру.

Функциональная типовая структура СФЗ ЯО включает в себя:

- силы охраны, обеспечивающие охрану ЯО в соответствии с зональным принципом охраны территорий, зданий, сооружений, в которых хранятся и используются ЯМ, ядерно-опасные изделия и размещаются ЯЭУ, а также транспортных средств, перевозящих ЯМ;
- службу безопасности ЯО, осуществляющую управление и координацию всей деятельности по физической защите на ЯО в соответствии с федеральной и отраслевой нормативной документацией;
- комплекс физических барьеров и инженерных сооружений, затрудняющих преодоление нарушителями границ охраняемых зон (доступ к транспортируемым ЯМ) и обеспечивающих силам охраны необходимый резерв времени на пресечение этих действий;
- комплекс технических и программно-технических средств и систем, предназначенных для обнаружения вторжения нарушителя

в охраняемые зоны и замедления его продвижения с помощью скрытых активных элементов, проноса (провоза) ЯМ, взрывчатых веществ и предметов из металла, наблюдения за обстановкой в охраняемых зонах с помощью телевидения, обеспечения автоматизированного управления доступом и учета пребывания персонала в определенных зонах ЯО, сбора, обработки и отображения информации, обеспечения бесперебойной связи между всеми подразделениями и службами, связанными с обеспечением физической защиты.

Силы охраны ЯО являются составной частью системы физической защиты. Охрану ядерных объектов осуществляют воинские части (подразделения) внутренних войск, вневедомственной охраны МВД России, Минобороны России или ведомственной охраны, командиры (руководители) которых несут ответственность за ее состояние. Перечень объектов, подлежащих охране внутренними войсками МВД России, определяется Правительством Российской Федерации.

Порядок несения службы по охране объектов, задачи, выполняемые подразделениями охраны, определяются нормативными правовыми актами Президента Российской Федерации, Правительства Российской Федерации и соответствующих федеральных органов исполнительной власти.

Подготовка подразделений охраны к выполнению возложенных задач осуществляется по учебным программам и планам, разрабатываемым соответствующими федеральными органами исполнительной власти. В целях подготовки к действиям при чрезвычайных ситуациях, проверки эффективности систем физической защиты и совершенствования взаимодействия с персоналом ядерного объекта, органами внутренних дел МВД России и ФСБ России проводятся учения. Порядок проведения учений определяется ведомственными нормативными актами.

Уведомление заинтересованных органов и организаций об учениях производится заблаговременно.

Взаимодействие в системе физической защиты на объектовом уровне осуществляется в соответствии с взаимно согласованными межведомственными нормативными актами, а также разработанными и утвержденными в установленном порядке планами взаимодействия.

Типовая топологическая структура СФЗ ЯО зависит от категорий используемых ЯМ и ядерно-опасных изделий, особенностей ЯЭУ и пунктов хранения ЯМ.

В общем случае СФЗ предусматривает иерархическую структуру охраняемых зон ЯО (рис. 8.1).

На ЯО Российской Федерации действует трехзонная структура охраняемых зон СФЗ. К ним относятся защищенная (ЗЗ), внутренняя (ВЗ), особо важная (ОВЗ), а также зоны ограниченного доступа (ЗОД). При организации охраняемых зон должно обеспечиваться условие: особо важная зона должна размещаться во внутренней зоне, внутренняя зона должна размещаться в защищенной зоне.

Предметы физической защиты, в соответствии с присвоенными им категориями, должны размещаться в соответствующих охраняемых зонах. При организации зонирования объекта должно обеспечиваться усиление физической защиты от периферии к центру, то есть к защищаемым ПФЗ. Если в процессе проведения оценки эффективности СФЗ выясняется, что существующих охраняемых зон недостаточно для нейтрализации потенциальных угроз, то могут организовываться дополнительные охраняемые зоны (рубежи) внутри существующих зон или ПФЗ размещаются в других охраняемых зонах.

Защищенная зона (территория промышленной площадки ЯО, отдельно стоящее здание ЯО) оборудуется многорубежными периметровыми средствами обнаружения, основанными на

различных физических принципах, средствами телевизионного наблюдения и физическими барьерами. Санкционированный проход в защищенную зону обеспечивается на контрольно-пропускных пунктах (КПП) автоматизированной системой управления доступом, предусматривающей также учет лиц (факт и время прохода). Автотранспортные КПП оборудуются противотаранными устройствами, препятствующими прорыву автотранспорта в защищенную зону. КПП также оборудуются средствами обнаружения ЯМ, взрывчатых веществ и предметов из металла.

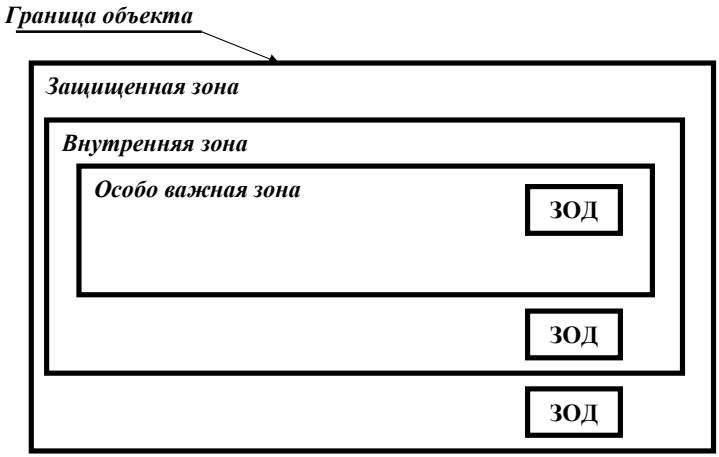


Рис. 8.1. Структура охраняемых зон СФЗ ЯО

Внутренняя и особо важная зоны (отдельное здание или сооружения внутри защищенной зоны, отдельное помещение или их совокупность внутри здания) оборудуются периметровыми системами обнаружения, телевизионного наблюдения; входы в здания и помещения — автоматизированными системами управления доступом, позволяющими контролировать доступ в

них, а также средствами обнаружения ядерных материалов, взрывчатых веществ и предметов из металла.

Создание зон ограниченного доступа (ЗОД на рис. 8.1) внутри указанных охраняемых зон ЯО обусловлено необходимостью обеспечить ограниченный, управляемый и контролируемый доступ персонала ЯО в пункты управления и иные жизненноважные объекты СФЗ.

Защита этих зон должна быть адекватна их важности и наращиваться в последовательности: защищенная, внутренняя, особо важная и локальная высокоопасная зоны.

Любая система физической защиты имеет свою *типовую структуру управления* (рис. 8.2).

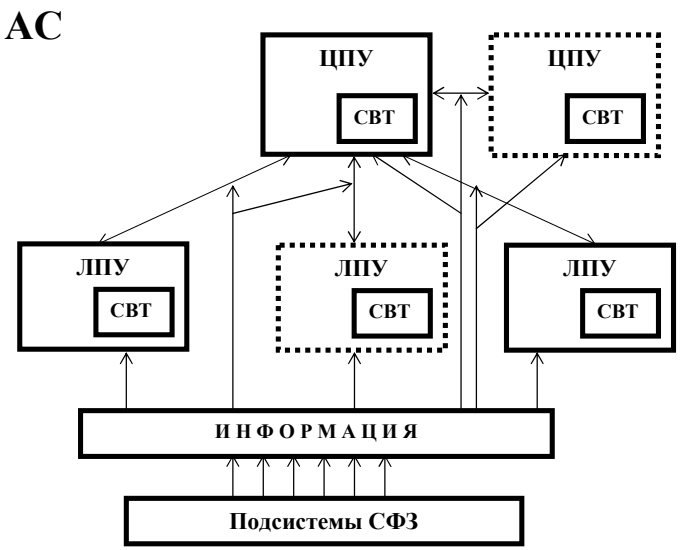


Рис. 8.2. Структура управления и информационная структура СФЗ ЯО

В типовом случае, когда на ЯО существуют все охраняемые зоны, управление системой физической защиты ЯО в целом осуществляется с центрального пункта управления (ЦПУ).

Управление отдельными компонентами СФЗ может осуществляться с локальных пунктов управления (ЛПУ), соединенных с ЦПУ.

Пункты управления должны обеспечивать защиту находящихся в них лиц от стрелкового оружия. Доступ в помещения пунктов управления должен осуществляться с применением средств контроля и управления доступом.

Информация, поступающая на локальный пункт управления, должна быть доступна оператору центрального пункта управления.

Для организации управления физической защитой должна быть предусмотрена система двусторонней связи между пунктами управления, а также между пунктами управления и силами реагирования.

Оператором центрального пункта управления является штатный сотрудник службы безопасности ядерного объекта, наделенный администрацией этого объекта соответствующими полномочиями для выполнения задач в условиях штатных и чрезвычайных ситуаций. Запрещается возлагать на операторов пунктов управления какие-либо функции, которые могут помешать выполнению ими своих основных обязанностей.

Типовая информационная структура СФЗ ЯО (рис. 8.2) определяется потоками информации между различными подсистемами СФЗ и средствами вычислительной техники (СВТ), установленными в пунктах управления, на которых концентрируется информация со средств и систем охранной сигнализации, телевизионного наблюдения, управления и контроля доступа персонала в охраняемые зоны, обнаружения проноса (провоза) ЯМ, взрывчатых веществ и предметов из металла, мнемосхемами охраняемых зон, средствами проводной и радиосвязи со службой безопасности, силами охраны, органами МВД, ФСБ, МЧС и Минобороны России.

Средства и системы радиосвязи используются в целях повышения эффективности системы комплексной безопасности предприятий, усиления физической защиты стационарных и подвижных ядерно-опасных объектов, оперативного управления и взаимодействия служб безопасности предприятия, сил охраны, а также подразделений, привлекаемых для выполнения совместных работ в случае возникновения нештатных ситуаций.

Таким образом, СФЗ представляет собой (рис. 8.2) сложную распределенную многоуровневую автоматизированную систему (АС) предназначенную для сбора, обработки, хранения, отображения и передачи информации о состоянии физической защиты различных зон ЯО. Такая АС состоит из подсистем допуска персонала, управления доступом в охраняемые зоны, обнаружения несанкционированного доступа и охранной сигнализации, телевизионного наблюдения, обнаружения ЯМ, взрывчатых веществ и предметов из металла, задержки проникновения нарушителя с помощью физических барьеров и иных инженерно-технических средств, специальной связи и обеспечивающих подсистем (электропитания, освещения и др.).

Как АС она выполняет следующие функции:

- получение достоверной информации о действиях, в том числе несанкционированных, персонала ЯО или иных лиц (проникновение в охраняемые зоны, пронос запрещенных предметов и т.п.);
- разграничение информации, передаваемой различным организационным структурам ЯО и другим заинтересованным организациям;
- управление различными техническими средствами и системами (телекамеры, средства освещения, замковые устройства, управляемые физические барьеры и т.п.);

•документирование необходимой информации о функционировании СФЗ, выдачу ретроспективных справок;

•обмен информацией с другими системами обеспечения безопасности ЯО (радиационного мониторинга, противопожарных мер, учета и контроля ЯМ, технологической безопасности и т.п.) и, при необходимости, системами управления более высокого уровня (предприятия, отраслевого, федерального).

На всех уровнях управления и этапах функционирования СФЗ (передача, сбор, обработка, анализ, хранение данных, передача управляющих команд) должна обеспечиваться защита информации, обращаемая в АС СФЗ, на основе применения комплекса средств и мероприятий по предотвращению утечки информации или исключению воздействия на нее по техническим каналам, по предупреждению случайных или преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения или нарушения работоспособности технических средств.

Следовательно, современные СФЗ должны интегрировать в себя не только подсистемы, описанные в предыдущей главе, но и подсистему защиты информации.

В завершение данного раздела приведем обобщающую функциональную структуру СФЗ ЯО (рис. 8.3).

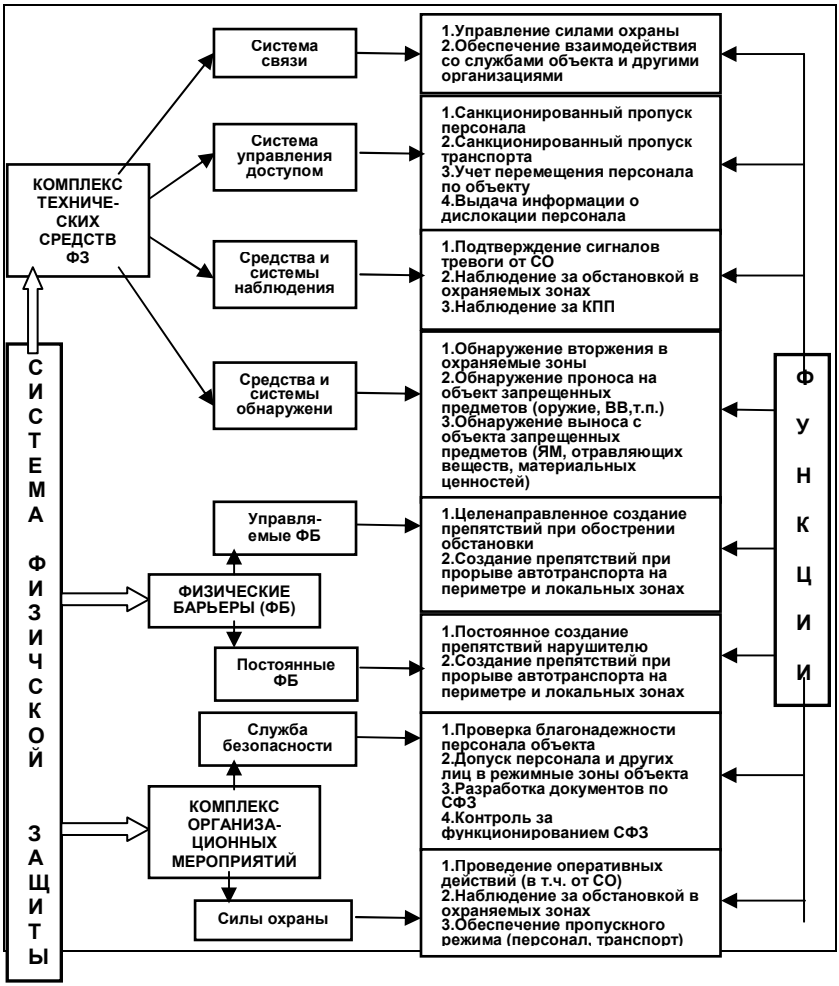


Рис. 8.3. Функциональная структура системы физической защиты ядерного объекта

В качестве комментария к рис. 8.3 можно отметить следующее. Основным назначением комплекса технических средств физической защиты является получение информации о несанкционированных действиях и выработка соответствующих управляющих воздействий. Физические барьеры призваны затруднить осуществление потенциальными нарушителями запланированных акций. Организационные мероприятия, в том числе действия сил охраны по пресечению указанных действий нарушителя, устанавливают порядок (правила) на объекте в плане обеспечения физической защиты и позволяют в итоге завершить решение задач по защите ЯМ и пресечению акций нарушителей.

Физическая защита обеспечивается на федеральном уровне и на уровне ядерного объекта (ЯО).

В частности, государство должно обеспечивать защиту ЯМ, используемого, хранящегося на ЯО или находящегося в процессе транспортирования от крупномасштабных угроз, таких как нападение на объект или транспорт с ЯМ больших групп террористов, использование ими летательных аппаратов, бронетехники и тому подобное.

Физическая защита ЯМ на уровне объекта осуществляется силами и средствами, находящимися на самом объекте. Это, прежде всего, силы охраны и те инженерно-технические средства, которые используются для решения задач физической защиты.

Силы и средства физической защиты объединяются в систему физической защиты (СФЗ).

8.12. Государственная система физической защиты

Физическая защита ЯО осуществляется в рамках государственной системы физической защиты.

Государственная система физической защиты представляет собой совокупность государственных органов власти и управления, федеральных органов исполнительной власти, осуществляющих государственное управление использованием атомной энергии и государственное регулирование безопасности при использовании атомной энергии, объектов использования атомной энергии (ядерных объектов), других федеральных органов исполнительной власти и организаций, в рамках своих полномочий принимающих участие в обеспечении физической защиты, а также выполняемых ими мероприятий и действий по обеспечению физической защиты.

Государственная система физической защиты предназначена для создания условий, предотвращающих возможности хищений и несанкционированного использования ядерных материалов, а также диверсий в отношении ядерных материалов, ядерных установок и пунктов хранения ядерных материалов.

Задачи по обеспечению физической защиты решаются на федеральном и ведомственном уровнях, а также непосредственно на уровне ядерного объекта.

Ядерные материалы и ядерные установки являются источниками повышенной опасности. На федеральном уровне принимаются законодательные акты в области безопасности ядерной деятельности, определяются угрозы по отношению к ядерным материалам и установкам, требования по их физической защите, а также правила и экономические условия реализации этих требований.

Государственную систему физической защиты составляют:

- Правительство Российской Федерации;
- Министерство обороны Российской Федерации, Федеральное агентство Российской Федерации по атомной энергии, другие федеральные органы исполнительной власти и организации, имеющие подведомственные ядерные объекты, эксплуатирующие

организации и ядерные объекты, непосредственно обеспечивающие реализацию системы физической защиты;

•Федеральная служба Российской Федерации по атомному надзору, Федеральная служба безопасности Российской Федерации, Министерство внутренних дел Российской Федерации, Министерство транспорта и связи Российской Федерации и Федеральная таможенная служба Российской Федерации, а также специализированные организации, принимающие участие в создании и совершенствовании систем физической защиты на ядерных объектах и при транспортировке ядерных материалов.

В целях решения задач физической защиты федеральные органы исполнительной власти и организации, имеющие в своем ведении ядерные объекты, в рамках своих полномочий:

•обеспечивают выполнение международных обязательств, вытекающих из Конвенции о физической защите ядерного материала;

•организуют и координируют работу по физической защите на подведомственных ядерных объектах, участвуют в организации охраны ядерных объектов воинскими частями (подразделениями) внутренних войск МВД России, вневедомственной охраной;

•организуют совместно с заинтересованными федеральными органами исполнительной власти транспортировку ядерных материалов и обеспечивают их физическую защиту;

•разрабатывают и утверждают ведомственные нормативные акты по вопросам обеспечения физической защиты, не противоречащие Правилам и федеральным нормам и правилам в этой области;

•участвуют в разработке федеральных норм и правил в области физической защиты;

•принимают решение о признании подведомственных ядерных объектов пригодными эксплуатировать ядерные установки или пункты хранения ядерных материалов и осуществлять собственными силами или с привлечением других организаций деятельность по созданию (совершенствованию) и функционированию систем физической защиты;

•разрабатывают отраслевые научно-технические программы и планы работ по обеспечению физической защиты;

•осуществляют финансирование работ по физической защите;

•осуществляют контроль за организацией и состоянием физической защиты на подведомственных ядерных объектах.

Вопросы для самоконтроля

1. Какие нормативно-правовые документы, относящиеся к физической защите ЯО, Вам известны?
2. Каковы задачи физической защиты ЯО?
3. Какие существуют элементы (предметы) физической защиты на ЯО?
4. Опишите направления деятельности администрации ЯО, связанные с созданием или совершенствованием СФЗ.
5. Каковы общие принципы создания СФЗ ЯО?
6. Объясните специфику ЯО.
7. Какие существуют основные угрозы безопасности ЯО?
8. Какие существуют информационные источники об угрозах ЯО?
9. Какие факторы необходимо учитывать при разработке модели нарушителя безопасности ЯО?
10. Каковы возможные мотивы нарушителей безопасности ЯО?
11. Опишите порядок создания и совершенствования СФЗ ЯО.

12. Объясните дифференциацию требований по физической защите ЯО.

13. Какие существуют организационные мероприятия по обеспечению физической защиты ЯО?

14. Какие предъявляются требования к инженерно-техническим средствам СФЗ ЯО?

15. Опишите функциональную типовую структуру СФЗ ЯО.

16. Опишите топологическую структуру ЯО.

17. Какова специфика системы управления ЯО?

18. Из чего состоит государственная система физической защиты?

9. СОЗДАНИЕ И СОВЕРШЕНСТВОВАНИЕ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ

В предыдущих главах были приведены сведения о современных системах физической защиты ядерных объектов, т.е. дан ответ на вопрос, *что такое СФЗ*.

В настоящей главе сделана попытка ответить на другой немаловажный вопрос: *как создать или совершенствовать* (что на практике чаще всего и делается) систему физической защиты.

Процесс создания (совершенствования) систем физической защиты ЯО имеет отличия по отношению к аналогичной деятельности применительно к другим техническим и организационно-техническим системам. Прежде всего, надо учитывать тот факт, что СФЗ – человеко-машинная система. Далее, ее функционирование основано на конфликте сторон. И, наконец, СФЗ функционирует в условиях неопределенности [П.4].

Все это делает процесс создания СФЗ специфичным, существенно возрастает роль ранних (аналитических) стадий и этапов, на которых проводится анализ и принимаются концептуальные решения по структуре, составу и функциям СФЗ в целом и отдельных ее составных частей. Поэтому ниже основное внимание будет уделено именно предпроектной стадии создания СФЗ [9.1 – 9.6].

9.1. Стадии и этапы создания СФЗ ЯО

Стадии и этапы жизненного цикла создания СФЗ представлены на рис. 9.1.

Работа начинается с изучения ЯО (его геополитическое расположение, характер производства, архитектурные особенности, климатические и природные условия и тому подобное).

Предпроектная стадия начинается с *анализа уязвимости* ЯО [9.1] с целью определения так называемых «жизненно-важных цен-

тров» (ЖВЦ) ЯО. В качестве примеров таких ЖВЦ можно привести: места хранения ЯМ, элементы систем, важных для безопасности ЯУ, и тому подобное. В дальнейшем будем их называть предметами физической защиты (ПФЗ). Для каждого ПФЗ формируются потенциальные угрозы (хищение ЯМ, диверсия на ЯУ) и модели вероятных нарушителей.

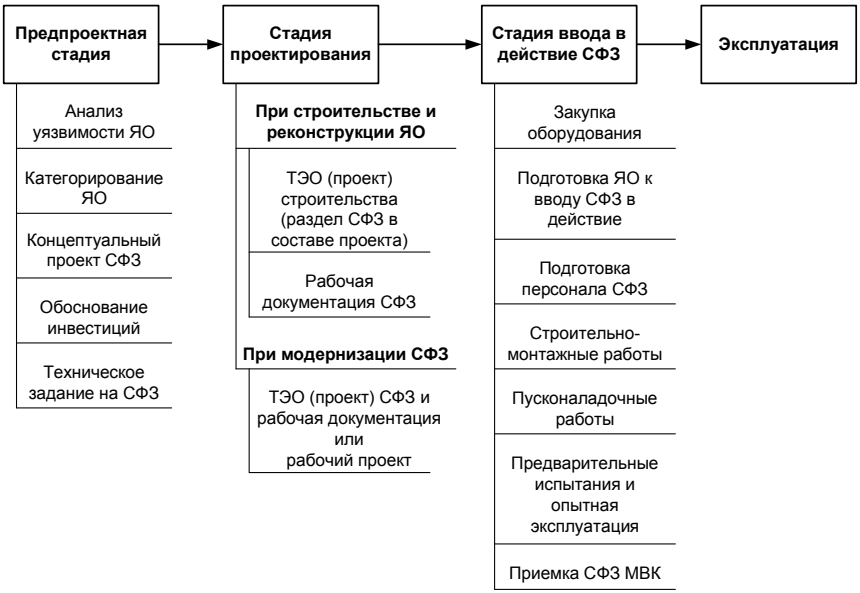


Рис. 9.1. Стадии и этапы создания (совершенствования) СФЗ

Затем производится *категорирование* ПФЗ, мест их нахождения (помещений и зданий ЯО) и ЯО в целом. В качестве критериев для категорирования выступают категория ЯМ [8.3] и возможные последствия несанкционированных действий (ПНСД).

Концептуальное проектирование СФЗ направлено на синтез («крупными мазками») структуры и состава СФЗ и оценку основных характеристик выбранного варианта (вариантов) системы [9.2].

После того как определены и прокатегорированы ПФЗ, производится *оценка эффективности* существующей СФЗ с помощью специальных методик [9.3] и компьютерных программ. Подробно процесс оценки эффективности и используемый для этих целей инструментарий изложен в главе 11.

На этапе *обоснования инвестиций* большее внимание уделяют экономическим аспектам, схемам реализации предложенных выше концептуальных решений.

После указанных этапов появляются исходные данные для составления обоснованного *технического задания* на СФЗ.

На стадии рабочего проектирования разрабатывается технико-экономическое обоснование (ТЭО) или проект СФЗ и чертежи, по которым в дальнейшем строители и монтажники будут реализовывать комплекс инженерных и технических средств физической защиты (КТСФЗ) [9.4, 9.5, 9.6].

Стадия *ввода СФЗ в действие* включает закупку в соответствии с ранее выпущенным проектом необходимого оборудования, проведение строительных и монтажно-наладочных работ, испытания (различных видов) и приемку СФЗ. На этой стадии также проводятся все подготовительные работы: приведение в соответствие схемы управления объектом с новой структурой и принципами функционирования СФЗ, обучение персонала физической защиты. Важным элементом является проведение предварительных испытаний и опытной эксплуатации СФЗ, когда персонал объекта моделирует процесс самостоятельного использования СФЗ. После устранения выявленных недостатков СФЗ принимается государственной или межведомственной комиссией в эксплуатацию.

Все сказанное относится также и к процессу совершенствования СФЗ, когда работа начинается не «с нуля».

Следует отметить, что на всех стадиях создания и совершенствования СФЗ должна проводиться оценка эффективности СФЗ и других ее характеристик, чтобы иметь «индикаторы» правильности

принимаемых на всех стадиях организационных и инженерно-технических решений.

После ввода СФЗ в действие начинается *стадия функционирования* СФЗ. Ответственность за ее эффективное функционирование возлагается на ЯО в лице его руководителя [8.3]. В процессе функционирования СФЗ обеспечивается требуемый уровень защиты объекта. Это достигается и применением соответствующей тактики действий охраны, и поддержанием его квалификации путем проведения переподготовки кадров. Важно также поддерживать работоспособность и требуемые характеристики инженерно-технического комплекса, обеспечивая своевременный ремонт оборудования и заказ запаса инструментов и приборов (ЗИП). Контроль за состоянием физической защиты ЯОО осуществляют федеральные надзорные органы, ведомственные комиссии, а также сама служба безопасности объекта (самоконтроль).

С учетом специфики СФЗ как человеко-машинных систем, работающих в условиях неопределенности (потенциальный нарушитель нам точно не известен, мы лишь прогнозируем его возможные действия), как было отмечено выше, возрастает роль предпроектной стадии (см. рис. 9.1). Остановимся более подробно на отдельных этапах этой стадии.

9.2. Анализ уязвимости ЯО

В соответствии с [9.1] анализ уязвимости ЯО проводит его администрация, с привлечением, при необходимости, специализированных организаций.

В результате этой работы определяются предметы физической защиты, места их расположения и модели вероятных нарушителей как «проводников» потенциальных угроз по отношению к каждому ПФЗ. В результате мы получаем ответ на вопрос: *что и от кого защищать?*

Для проведения анализа уязвимости на объекте создается рабочая группа, «первую скрипку» в которой играют специалисты – технологи, досконально знающие свой объект.

Предметом физической защиты в процессе хранения, производства и использования ЯМ являются сами ядерные материалы. Места их нахождения известны, и это наиболее простой случай определения ПФЗ.

Сложнее обстоит дело при анализе уязвимости ядерных установок. Эта работа требует проведения специальных исследований, направленных на выявление критических элементов оборудования ЯУ (уязвимых мест), несанкционированные действия против которых могут привести к серьезным негативным последствиям (радиологическое заражение местности и т.п.). Выявленные в результате этой работы уязвимые места и будут предметами физической защиты.

В существующих методах проведения анализа уязвимости используются в основном составление логических схем событий и математический аппарат теории графов [П.4].

В процессе анализа обычно строится дерево повреждений. Например, если конечным событием является плавление активной зоны реактора, то промежуточными событиями, которые приводят к конечному, могут быть повреждения различных элементов оборудования (насосов, трубопроводов, кабелепроводов, контроллеров и т.п.),

ошибки оператора. При рассмотрении аспектов физической защиты эти повреждения и неприемлемые с позиций безопасности действия людей являются специально организованными нарушителем.

Формируя такую многоуровневую схему, мы в итоге придем к местам, где находится соответствующее оборудование, которое и требует защиты.

При этом учитывается тот факт, что конечное событие может наступить либо при наступлении любого единичного события нижнего уровня, либо только при их логическом сочетании (например, по схеме «И»).

9.3. Процедура концептуального проектирования СФЗ ЯО

С целью обоснования предлагаемых организационных и инженерно-технических решений вводится отдельный этап – разработка концептуального проекта.

Процедура концептуального проектирования СФЗ представлена на рис. 9.2.

На начальном этапе формируются исходные данные с использованием результатов, полученных на предыдущих этапах (анализ уязвимости ЯО и т.п.). Учитывается специфика объекта. Например, если это АЭС, то вероятна террористическая акция, если это хранилище ЯМ (уран, плутоний и др.), то более вероятна акция хищения ЯМ и, как следствие, нарушение режима ядерного нераспространения.

Рис. 9.2. Процедура концептуального проектирования СФЗ

Для проведения этой работы формируется рабочая экспертная группа из представителей ЯО и других заинтересованных организаций.

Первоначально проводится оценка эффективности той СФЗ, которая уже функционирует на объекте.

Затем начинается собственно концептуальное проектирование, основанное на синтезе СФЗ по критерию «эффективность-стоимость».

В итоге осуществляется выбор и обоснование структуры СФЗ в целом и отдельных ее подсистем, предъявляются требования к отдельным ее элементам.

В частности, выбирается структура и состав комплекса технических средств физической защиты, который включает в себя средства обнаружения, оценки ситуации (наблюдения), управления доступом, связи и др. При этом желательно использовать типовые решения [9.6].

При выборе состава СФЗ возможны различные сочетания технических средств, физических барьеров и организационных решений, при этом каждый выбранный вариант будет обеспечивать определенный уровень эффективности СФЗ в целом.

Выбор оптимального варианта осуществляется с использованием критерия «эффективность-стоимость». Данная задача может решаться в двух постановках:

- максимизация эффективности СФЗ при ограничении стоимости (ресурсов);
- минимизация стоимости СФЗ при заданном (допустимом) уровне эффективности.

Вопросы для самоконтроля

1. Каковы особенности построения СФЗ как человеко-машинной системы?
2. Какие существуют стадии жизненного цикла создания (совершенствования) СФЗ ЯО?
3. Опишите этапы предпроектной стадии.
4. Какие существуют этапы анализа уязвимости ЯО? Каковы их цели и задачи?
5. Какие существуют этапы концептуального проектирования СФЗ ЯО? Каковы их цели и задачи?
6. Опишите рабочее проектирование СФЗ.
7. Опишите ввод СФЗ в действие. Какие при этом решаются задачи?
8. Как обеспечивается функционирование СФЗ? Какие при этом решаются задачи?
9. Опишите подходы к синтезу СФЗ по критерию «эффективность-стоимость».

10. ФИЗИЧЕСКАЯ ЗАЩИТА ЯДЕРНЫХ МАТЕРИАЛОВ ПРИ ПЕРЕВОЗКАХ

В данной главе рассмотрены вопросы, связанные с обеспечением физической защиты перевозок ЯМ в современных условиях, на примере автоматизированной системы обеспечения безопасности транспортирования (АСБТ), которая является составной частью всей системы обеспечения физической защиты транспортируемых ЯМ [10.1 – 10.3].

10.1. Особенности обеспечения безопасности ядерных материалов при перевозках

Массовые перевозки ЯМ в СССР начались с 50-х годов. До 90-х они осуществлялись, в основном, железнодорожным транспортом и, как исключение, автомобильным.

В условиях противоборства двух систем (социалистической и капиталистической) основное внимание уделялось скрытности перевозок и обеспечению ядерной и радиационной безопасности. Задача сокрытия маршрутов и масштабов перевозок от иностранных государств достигалась режимными мерами: ограничением круга лиц, осведомленных о перевозках, легендированием и выполнением других мероприятий по обеспечению государственной тайны. Ядерная и радиационная безопасность достигалась путем создания все более совершенных транспортно-упаковочных контейнеров и обеспечением безопасности при проведении погрузочно-разгрузочных работ.

В стране в те времена практически отсутствовало такое явление, как терроризм, что позволяло обеспечивать физическую защиту перевозимых ЯМ только силами караула внутренних войск МВД России. Задача караула сводилась, в первую очередь, к предупре-

дительным мерам по недопущению случайного нарушителя к транспорту.

В новых экономических условиях при переходе страны к рыночным отношениям по экономическим соображениям возросло использование автомобильного транспорта при перевозках ЯМ.

Происходившие в России (после распада СССР) процессы (возрастание социальной напряженности в обществе, возникновение конфликтов на границах с бывшими союзными республиками, появление такого явления, как терроризм, наличие большого количества бесконтрольного оружия) заставили пересмотреть отношение к физической защите ядерных материалов и установок, в том числе транспортируемых ЯМ. В документе федерального уровня [8.3] впервые появились требования по оборудованию транспортных средств инженерно-техническими средствами физической защиты, что позволило повысить эффективность охраны транспорта.

С ростом проявлений сепаратизма и терроризма в стране, возникновением вооруженных конфликтов на территории РФ, повышением уровня оснащенности и подготовки террористов, обеспечить сохранность ЯМ в ходе перевозки только силами и средствами физической защиты транспорта стало гораздо сложнее. Это наглядно показали проведенные в последнее время исследования и учения. Возникла необходимость создания специальных мобильных сил (сил реагирования), которые совместно с силами, осуществляющими охрану конкретного груза, могли бы пресечь несанкционированные действия. Для решения этой задачи необходимо знать место и причины возникновения ситуации на момент совершения несанкционированных действий. Чтобы обеспечить своевременное реагирование, информация о нападении должна доводиться до сил реагирования в реальном масштабе времени. Поэтому возникла необходимость в разработке системы, которая обеспечивала бы в любой точке территории России связь транспорта с предприятием-грузоотправителем, предприятием-грузополуча-

телем, вышестоящими организациями, а также оповещение силовых структур о несанкционированных действиях или возникновении чрезвычайной ситуации. Учитывая, что могут возникнуть такие условия, когда сигнал о несанкционированных действиях или возникновении чрезвычайной ситуации по разным причинам не сможет быть своевременно доведен до сил реагирования, появилось требование постоянного мониторинга передвижения транспортов, осуществляющих перевозки ЯМ.

Кроме этого, потребовалось автоматизировать деятельность охраны транспорта по осуществлению контроля сохранности специального груза, а также повысить защиту ЯМ от несанкционированных действий в ходе перевозки.

10.2. Организация перевозок ЯМ

Перевозки ЯМ – один из видов деятельности ядерных объектов, осуществляемый со следующими целями:

- обеспечение технологического цикла производства ЯМ;
- доставка продукции предприятия потребителям.

В ходе перевозки решаются следующие задачи:

- доставка потребителям ЯМ или изделий на их основе;
- обеспечение ядерной, радиационной, транспортной и пожарной безопасности;
- обеспечение физической защиты ЯМ.

Классификация перевозок ЯМ с точки зрения обеспечения физической защиты

Перевозки ЯМ подразделяются по виду перевозок:

- на внутриплощадочные;
- между промышленными площадками;

- между предприятиями и организациями;
- международные.

Внутриплощадочные перевозки осуществляются между цехами или между цехом и складом завода, находящимся в защищенной зоне.

Перевозки между промышленными площадками осуществляются в пределах одного предприятия.

Перевозки между предприятиями и организациями осуществляются между предприятиями Росатома, а также для доставки продукции на базе ЯМ другим потребителям. К данному виду перевозок также относятся перевозки между площадками, если часть маршрута проходит за пределами охраняемой территории.

Международные перевозки связаны с доставкой ЯМ потребителям, находящимся на территории других государств, в том числе транзит через территорию третьих стран.

Основная часть перевозок ЯМ осуществляется внутри страны.

По виду используемого транспорта перевозки ЯМ подразделяются на:

- железнодорожные;
- автомобильные.
- морские;
- речные;
- воздушные.

В настоящее время большинство перевозок ЯМ осуществляется железнодорожным и автомобильным транспортом.

Характеристика видов перевозок с точки зрения уязвимости ЯМ

В настоящее время наибольшую угрозу обеспечению безопасности перевозок ЯМ несет в себе ядерный терроризм.

Целями его могут быть:

- хищение ЯМ или изделий на их основе, что приводит к нарушению режима ядерного нераспространения;
- проведение террористического акта – распыление радионуклидов путем подрыва ЯМ или изделий на их основе.

Стационарные ядерные объекты, с точки зрения физической защиты, характеризуются наличием:

- охраняемых зон, оборудованных средствами обнаружения, физическими барьерами, системами управления доступом;
- значительных сил, выделяемых для охраны;
- сил реагирования, расположенных в непосредственной близости от охраняемых зон.

В отличие от стационарных объектов, перевозка ЯМ является наиболее уязвимой операцией с точки зрения возможности совершения несанкционированных действий. Это обусловлено, прежде всего, невозможностью создания запретной зоны вокруг транспортного средства с ЯМ (в движении).

Это существенным образом затрудняет обеспечение физической защиты ЯМ.

Необходимо отметить, что в зависимости от вида перевозок и используемых транспортных средств, влияние указанных факторов может возрастать или ослабевать.

Анализ видов перевозок позволяет определить степень достаточности мероприятий по обеспечению защиты ЯМ от несанкционированных действий.

10.3. Основные задачи физической защиты при перевозках ЯМ

В настоящее время физическая защита транспортов, осуществляющих перевозки ЯМ, строится по аналогии с физической защи-

той стационарных объектов, но имеет несколько другое содержание. Она предусматривает: проведение организационных мер, оборудование транспортов инженерно-техническими средствами физической защиты, выделение сил охраны, а также сил реагирования на случай совершения несанкционированных действий, доведение до соответствующих органов сигнала о совершении несанкционированных действий, а также оповещение сил реагирования о возникшей ситуации.

В идеальном случае силы охраны должны обеспечивать пресечение несанкционированных действий. Однако, учитывая возможности современных террористов, их оснащение и вооружение, фактор внезапности нападения, более реально требовать от сил охраны обеспечить при использовании инженерно-технических средств физической защиты сдерживание нарушителей до прибытия сил реагирования.

Это условие может быть записано в следующем виде:

$$T_{\text{з}} \rangle T_{\text{реаг}},$$

где $T_{\text{з}}$ – время, в течение которого физическая защита транспортного средства может обеспечивать защиту ЯМ от хищения; $T_{\text{реаг}}$ – время, необходимое силам реагирования для прибытия к месту совершения несанкционированных действий.

Время $T_{\text{з}}$ характеризуется интервалом, в течение которого нарушителям необходимо преодолеть противодействие сил охраны, проникнуть внутрь грузового отсека, изъять транспортные упаковочные контейнеры с ЯМ и увезти их в неизвестном направлении.

Время $T_{\text{реаг}}$ характеризуется пропускной способностью каналов связи, временем реагирования должностных лиц соответствующих органов на пришедшее тревожное сообщение, удаленностью сил реагирования от места возникновения ситуации.

Задача состоит в том, чтобы определить оптимальный состав охраны транспорта и инженерно-технических средств физической

защиты, которые позволили бы сдержать нарушителей до прибытия сил реагирования. Решение данной задачи осуществляется исходя из критерия «эффективность – стоимость».

Порядок обеспечения физической защиты приведен в следующем разделе.

10.4. Организация физической защиты в ходе перевозок ЯМ

В ходе перевозки решаются три задачи: предупреждения, своевременного обнаружения и пресечения несанкционированных действий в отношении ЯМ.

Предупреждение несанкционированных действий достигается:

- своевременным информированием соответствующих министерств и ведомств о предстоящей перевозке ЯМ, а также о местонахождении транспортных средств в ходе перевозки;
- осуществлением сбора информации об обстановке в районах пролегания маршрута предстоящей перевозки ЯМ, а также о потенциальных угрозах, которые могут возникнуть в ходе перевозки;
- осуществлением контроля за перемещением транспорта с ЯМ.

Своевременное обнаружение несанкционированных действий достигается:

- установкой на транспортном средстве инженерно-технических средств физической защиты;
- бдительным несением службы личным составом охраны транспорта.

Пресечение несанкционированных действий в отношении ЯМ достигается:

- прочностью физических барьеров к преодолению;
- своевременным оповещением о совершении несанкционированных действий;

- слаженными действиями личного состава охраны транспорта по отражению нападения;
- своевременным прибытием сил реагирования к месту совершения несанкционированных действий в отношении ЯМ.

Физическая защита транспортов строится на тех же принципах, что и ФЗ стационарных объектов, которые описаны выше. Вместе с тем, физическая защита не должна создавать препятствий функционированию транспортных средств и должна адаптироваться к технологическим процессам, проводимым на транспорте в периоды подготовки, проведения и окончания перевозки ЯМ, в том числе в условиях ликвидации чрезвычайной ситуации с учетом принятых мер ядерной, радиационной, технологической и пожарной безопасности.

Физическая защита ЯМ в ходе перевозок включает в себя: организационные мероприятия, автоматизированную систему обеспечения безопасности транспортирования и действия подразделений охраны и сил реагирования.

Организационные мероприятия – это комплекс мероприятий, включающий разработку нормативно-распорядительных документов, создание организационной структуры физической защиты, разработку мероприятий, проводимых в период подготовки, проведения и завершения перевозки ЯМ, а также в условиях угрозы или совершения несанкционированных действий, в ходе ликвидации чрезвычайной ситуации или последствий несанкционированных действий.

Организационные мероприятия проводятся на отраслевом уровне предприятиями отрасли, осуществляющими перевозки ЯМ, другими заинтересованными организациями.

Перечень организационных мероприятий и порядок их выполнения отражаются в:

- плане подготовки к перевозке, разрабатываемом на предприятии-грузоотправителе;
- плане взаимодействия на случай совершения несанкционированных действий и возникновения ЧС, разрабатываемом предприятием совместно с заинтересованными структурами других министерств и ведомств;
- планах действий в ЧС, разрабатываемых во всех структурах, с которыми организовано взаимодействие;
- аварийных карточках, должностных инструкциях.

Автоматизированная система обеспечения безопасности транспортировки – это система, состоящая из персонала, подсистем охранной сигнализации, наблюдения, контроля и управления доступом, связи, защиты информации, средств активной задержки и физических барьеров, обеспечивающая безопасность транспортировки. Структура АСБТ показана на рис. 10.1.

АСБТ должна обеспечить выполнение следующих задач:

- обнаружение несанкционированного проникновения в транспортное средство и грузовой отсек (кузов);
- предотвращение беспрепятственного доступа посторонних лиц внутрь грузового отсека (кузова);
- задержку (замедление) проникновения нарушителей к контейнерам с ЯМ;
- отслеживание перемещения всех транспортов, оснащенных системой АСБТ, по территории Российской Федерации;
- осуществление оперативного контроля состояния физической защиты транспортов с ЯМ;
- осуществление обмена информацией между транспортным средством и диспетчерскими пунктами в режиме реального времени;

- автоматическое формирование сигнала тревоги и передача его на диспетчерские пункты и пункты управления МВД России при попытке совершения несанкционированных действий;
- автоматизацию процесса сбора, учета, хранения и отображения информации о перевозках ЯМ;
- защиту информации, передаваемой по средствам связи.

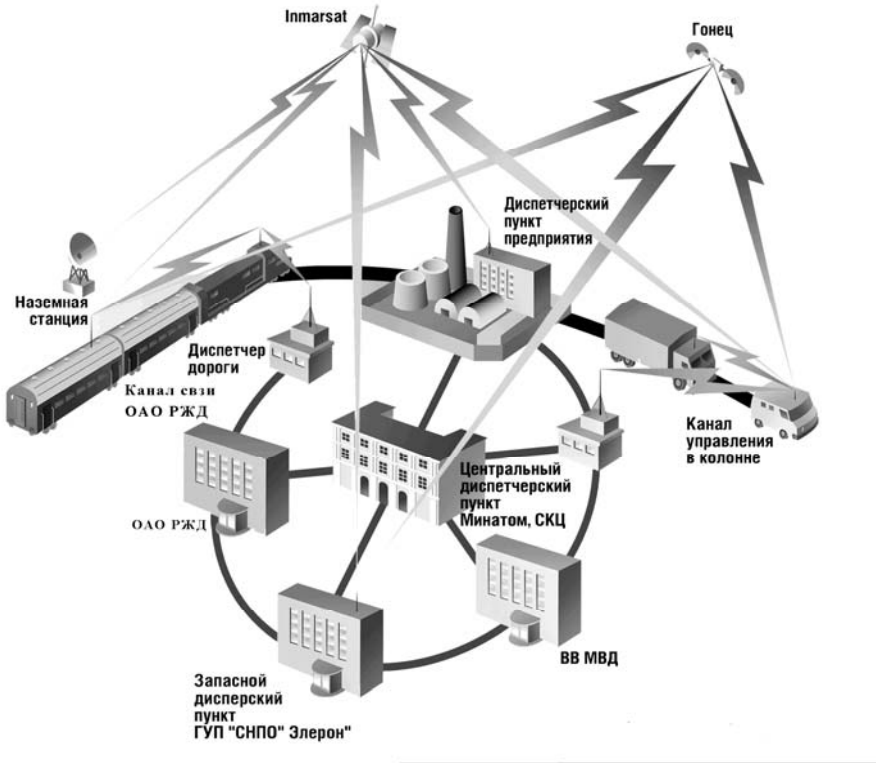


Рис. 10.1. Структура АСБТ

АСБТ оборудуются транспортные средства, диспетчерские пункты Росатома, автоматизированные рабочие места, развернутые в других министерствах и ведомствах.

В состав АСБТ транспортных средств входят:

- подсистема охранной сигнализации;
- подсистема тревожно-вызывной сигнализации;
- подсистема наблюдения (оценки ситуации);
- подсистема контроля и управления доступом;
- средства активной задержки;
- физические барьеры:
- комплекс средств автоматизации;
- подсистема связи;
- подсистема защиты информации.

В состав АСБТ диспетчерских пунктов и автоматизированных рабочих мест, развернутых в других министерствах и ведомствах, входят:

- подсистема контроля перевозок;
- подсистема связи;
- подсистема защиты информации;
- подсистема оповещения.

Подсистема охранной сигнализации предназначена для своевременного обнаружения попыток или фактов совершения несанкционированных действий и доведения тревожного сообщения до сопровождающего и охраны транспорта. Она включает 1-2 рубежа технических средств охраны, устанавливаемых внутри грузового отсека (кузова).

Подсистема тревожно-вызывной сигнализации предназначена для экстренного вызова часовыми начальника караула и контроля нахождения часовых на постах.

Подсистема наблюдения (оценки ситуации) предназначена для наблюдения за подступами к охраняемому транспорту, состоянием и наличием груза в грузовом отсеке.

Подсистема контроля и управления доступом предназначена для исключения несанкционированного доступа внутрь грузового

отсека (кузова), а также к другим системам, осуществляющим управление инженерно-техническими средствами физической защиты.

Средства активной задержки предназначены для сдерживания нарушителя при его проникновении внутрь грузового отсека (кузова) путем применения скрытых элементов и способов воздействия, затрудняющих его действия или временно выводящих нарушителя из строя.

В состав физических барьеров входят:

- комплект элементов механического усиления конструкции транспортного средства и запирающих устройств;
- запорно-пломбировочные устройства;
- замковые устройства.

Комплект элементов механического усиления конструкции транспортного средства и запирающих устройств предназначен для затруднения несанкционированного проникновения внутрь транспортного средства или в грузовой отсек (кузов). Он включает в себя защитные, блокирующие устройства, ударопрочные пленки, цепи и другое.

В качестве защитных устройств могут выступать различные виды кузовов, вагонов и автомобилей, усиление стенок вагонов, кабин и кузовов автомобилей бронезащитой.

Блокирующие устройства обеспечивают предотвращение несанкционированной выгрузки транспортно-упаковочных контейнеров (ТУК) из транспортного средства.

Ударопрочные пленки предназначены для предотвращения проникновения внутрь вагона или кабины автомобиля путем разбития стекол.

Цепи предназначены для предотвращения смещения ТУК (транспортно-упаковочного контейнера с ЯМ) в ходе перевозки, а

также создания дополнительного физического барьера в случае совершения несанкционированных действий.

Запорно-пломбировочные устройства предназначены для обеспечения возможности обнаружения вмешательства в защищаемый объект (внутренний объем грузового отсека транспортного средства).

Замковые устройства предназначены для обеспечения санкционированного доступа в грузовой отсек по правилу двух (трех) лиц и создания дополнительной задержки для нарушителя на путях возможного доступа к ЯМ.

Подсистема контроля перевозок предназначена для обеспечения постоянного контроля за местом нахождения транспортных средств и состояния физической защиты в ходе перевозки ЯМ.

Она включает в себя:

- диспетчерские пункты;
- автоматизированные рабочие места, развернутые в министерствах и ведомствах, а также в подчиненных им организациях, участвующих в обеспечении безопасности перевозок ЯМ.

Комплекс средств автоматизации (КСА) предназначен для обработки информации, циркулирующей в АСБТ.

Он подразделяется на комплекс средств автоматизации, установленных в транспортных средствах, и комплекс средств автоматизации, установленных на диспетчерских пунктах и автоматизированных рабочих местах.

Комплекс средств автоматизации транспортных средств позволяет обеспечить:

- обработку информации, поступающей от технических средств физической защиты;
- управление техническими средствами охраны и средствами активной задержки;

- информационный обмен по средствам связи с диспетчерскими пунктами предприятия-грузоотправителя и Росатома;
- передачу в ручном и автоматическом режимах на диспетчерские пункты тревожных сообщений о совершении несанкционированных действий или возникновении ЧС;
- автоматизированный сбор, учет, хранение информации, обрабатываемой комплексом в ходе перевозки.

Комплекс средств автоматизации диспетчерских пунктов позволяет обеспечить:

- дистанционный мониторинг местонахождения транспортов отрасли, перевозящих ЯМ, состояние технических средств физической защиты;
- информационный обмен по средствам связи: между диспетчерскими пунктами и транспортными средствами, между диспетчерским пунктом Росатома (диспетчерскими пунктами предприятий) и автоматизированными рабочими местами министерств и ведомств (организаций), участвующих в обеспечении безопасности перевозок;
- автоматизированный сбор, учет, хранение и отображение информации о всех поступивших и отправленных сообщениях, перемещениях транспортных средств отрасли, совершении несанкционированных действий, возникновении ЧС с привязкой к электронной карте;
- информационную поддержку выработки решений на основе полученной информации.

Комплекс средств автоматизации автоматизированных рабочих мест позволяет обеспечить:

- информационный обмен с диспетчерским пунктом Росатома (диспетчерским пунктом предприятия);
- автоматизированный сбор, учет, хранение и отображение информации обо всех поступивших и отправленных сообщениях, пе-

ремещениях транспортных средств отрасли, совершении несанкционированных действий, возникновении ЧС с привязкой к электронной карте;

- информационную поддержку выработки решений на основе полученной информации.

Комплекс средств автоматизации включает в себя комплексы программного, технического и информационного обеспечения.

Система оповещения предназначена для своевременного оповещения сил реагирования в случае совершения несанкционированных действий или возникновения ЧС в отношении транспорта, перевозящего ЯМ.

Система связи предназначена для обеспечения связи:

- внутри транспорта (колонны, состава);
- между транспортным средством и диспетчерскими пунктами Росатома, предприятия-грузоотправителя;
- между диспетчерским пунктом Росатома (предприятия-грузоотправителя) и взаимодействующими министерствами и ведомствами (организациями);

Кроме этого она должна обеспечивать:

- определение местонахождения транспортного средства;
- работу системы оповещения;
- возможность сопряжения с радиосистемами подразделений министерств и ведомств, привлекаемых для ликвидации несанкционированных действий и ЧС.

Система связи включает:

- подсистему проводной связи;
- подсистему УКВ связи;
- подсистему космической связи;
- подсистему сотовой связи;
- подсистему определения местонахождения транспортного средства.

Система защиты информации предназначена для защиты информации, циркулирующей в системе связи.

Данная система строится на основе анализа угроз информационной безопасности АСБТ, выражающихся в следующих возможных действиях:

- искажение (подмена) передаваемой в системе информации, навязывание ложных или ранее переданных сообщений с целью препятствования передаче достоверной информации;
- воздействие по каналам связи на технические средства системы сбора данных с датчиков, направленное на дезорганизацию функционирования элементов системы и нарушение информационного обмена в системе;
- попытка получения возможным нарушителем конфиденциальной информации, циркулирующей в системе;
- попытка нарушения идентификации источников информации;
- попытка подбора кодов доступа.

Защите подлежат:

- собственно информация, не подлежащая распространению;
- средства и системы информатизации, средства и системы связи и передачи данных;
- технические средства приема, передачи и обработки информации (телефонии, радиосвязи);
- датчики охранной сигнализации;
- технические средства и системы, не обрабатывающие непосредственно защищаемую информацию, но размещенные в помещениях, где обрабатывается (циркулирует) защищаемая информация;
- помещения пунктов управления, диспетчерских пунктов, в которых ведутся конфиденциальные разговоры, раскрывающие особенности функционирования систем физической защиты.

Защита информации в АСБТ достигается:

- оснащением диспетчерских пунктов (автоматизированных рабочих мест) оборудованием в защищенном исполнении;
- использованием в средствах вычислительной техники лицензионного системного программного обеспечения;
- контролем несанкционированных действий обслуживающего персонала, а также других лиц, не допущенных к работе с оборудованием ФЗ;
- проверкой прикладного программного обеспечения на отсутствие недекларированных возможностей;
- использованием комплекса средств защиты информации при ее передаче по проводным, радио и иным каналам связи.

Действия сил охраны и сил реагирования

Действия сил охраны – специфические действия, выполняемые личным составом караула на этапах непосредственной подготовки, в ходе и по завершении перевозки, при совершении несанкционированных действий или возникновении ЧС.

Порядок несения караульной службы определяется уставом, наставлениями МВД России или организационно-распорядительными документами Росатома, разработанными для ведомственной охраны.

Действия сил реагирования – специфические действия подразделений от силовых структур, направленные на пресечение несанкционированных действий или ликвидацию последствий их совершения.

10.5. Оценка эффективности физической защиты транспортируемых ЯМ

Для оценки эффективности организационных и проектно-технических мероприятий, направленных на обеспечение физической защиты транспортируемых ЯМ, применяются следующие методы:

- проведение учений;
- математическое моделирование (аналитический метод);
- имитационно-игровые методы.

При использовании всех этих методов необходимо учитывать тот факт, что оцениваются результаты боестолкновения между нарушителями и силами охраны, что позволяет сделать вывод о достаточности защитных мер и определить направления совершенствования системы физической защиты.

Проведение учений позволяет наиболее полно учесть реальные условия, в которых возникает чрезвычайная ситуация (несанкционированные действия нарушителей). Например, можно организовать нападение учебных нарушителей на транспортные средства, перевозящие ЯМ.

В этом случае боевое столкновение нарушителей и сил охраны, сопровождающих груз, будет проходить в условиях, приближенных к реальным (рельеф местности, растительность, время года и суток и т.п.). Однако результат боестолкновения будет зависеть от сложившейся в данных конкретных условиях ситуации. Для получения сравнительно устойчивого в статистическом отношении результата надо проводить учения многократно, что влечет за собой большие затраты материальных и людских ресурсов.

Математическое моделирование, основанное на применении аналитических расчетных соотношений, ограничено в применении, так как формализовать (описать математически) все реальные ус-

ловия, в которых происходит боестолкновение, не представляется возможным. Слишком много факторов с переменными вероятностными характеристиками влияет на этот процесс.

Имитационно-игровые методы позволяют более реально отразить конкретные условия. В данном случае существуют ручные и компьютерные методы.

Примером ручных методов является методика «Table Top» [10.2] разработки Окриджской национальной лаборатории США. В соответствии с этой методикой на плане местности производится пошаговое моделирование действий нарушителей и сил охраны. Ход попеременно передается одной из сторон. В течение одного хода в соответствии с принятыми правилами игры можно производить перемещение транспортных средств, людей, производить выстрелы и тому подобное. Игра продолжается до тех пор, пока у одной из сторон не останется достаточных сил (численности) для противодействия. Для получения статистически устойчивого результата игра повторяется многократно, результаты усредняются, чтобы выявить тенденцию.

Более современным подходом является использование компьютерных программ (например, программа «Полигон», разработанная в Росатоме на предприятии ФГУП «СНПО «Элерон»»), позволяющих более реалистично представить условия, в которых происходит боестолкновение (учет рельефа местности, автоматизация принятия решения о попадании в цель при стрельбе из различных видов оружия в различных условиях и тому подобное).

При проведении моделирования используются два компьютера: нападающих и защитников, на экранах мониторов которых отображается только та информация, которая была бы доступна каждой из сторон в реальных условиях. Например, если рельеф мест-

ности скрывает одного из нападающих, то он не будет отображаться на мониторе защитников. Если же он выйдет из-за укрытия, он тут же появится на мониторе противника.

Игра, так же как и в Table Top, проводится в пошаговом режиме.

На рис. 10.2 показан фрагмент моделирования боестолкновения, отображаемый на одном из мониторов.

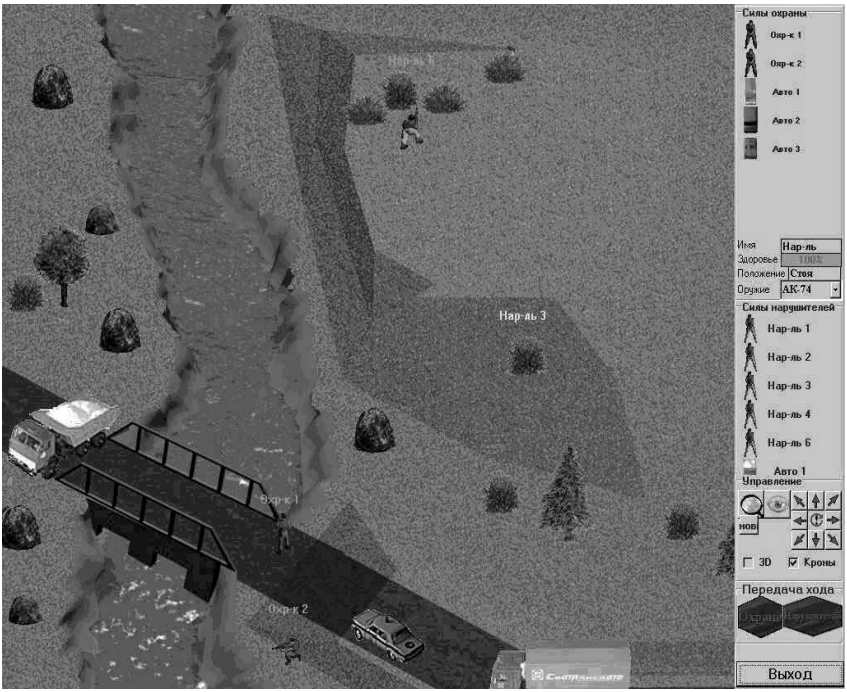


Рис. 10.2. Фрагмент моделирования

В итоге одного сеанса моделирования определяются исход боестолкновения (кто победил) и время боя.

Применение таких методов приближает нас к действительности и повышает достоверность результатов моделирования.

Если дополнить время боя временами преодоления нарушителем преград, выполнения акции по изъятию ЯМ и уходу, то получим полное время действий нарушителя (после усреднения результатов нескольких сеансов моделирования), которое можно сравнивать с ожидаемым временем прибытия сил реагирования и сделать вывод об эффективности ФЗ.

На практике подобные программы применяются для обоснования предлагаемых организационных и проектно-технических решений. Допустим, необходимо решить вопрос о том, на какие мероприятия по усилению физической защиты транспортного средства целесообразно потратить выделенные для этого средства. Например, что лучше: одеть персонал охраны в бронежилеты, предоставить им приборы ночного видения или укрепить (бронировать) стенки транспортных средств и тому подобное. После проведения моделирования можно дать обоснованные рекомендации по выбору оптимального варианта.

Вопросы для самоконтроля

1. Каковы особенности организации физической защиты транспортируемых ЯМ?
2. Как классифицируются перевозки ЯМ?
3. Опишите автоматизированную систему обеспечения безопасности транспортирования (АСБТ) ЯМ.
4. Какие существуют подсистемы АСБТ?
5. Какие основные задачи физической защиты решаются при перевозках ЯМ?
6. Как осуществляется предупреждение несанкционированных действий при перевозках ЯМ?
7. Как осуществляется обнаружение несанкционированных действий при перевозках ЯМ?
8. Какую роль выполняют средства связи при перевозках ЯМ?
9. Как обеспечивается защита информации в автоматизированной системе безопасности транспортирования?
10. Как оценивается эффективность физической защиты транспортируемых ЯМ?

11. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ

Для объективной оценки приспособленности любой системы с целью выполнения возложенных на нее задач необходимо иметь метод оценки эффективности данной системы. Такие методы могут быть качественными, но лучше, если в их основу положены количественные показатели, позволяющие сравнивать различные варианты системы. В данном разделе рассмотрены основы оценки эффективности СФЗ [П.4, 11.1 – 11.5].

11.1. Эффективность СФЗ ЯО

Эффективность как свойство конкретного класса систем зависит от их специфики. В частности, применительно к СФЗ можно дать следующее определение.

Эффективность СФЗ – свойство системы, заключающееся в способности СФЗ противостоять действиям нарушителя в отношении ядерных материалов (ЯМ), ядерных установок (ЯУ), других уязвимых мест (УМ) ЯО и предметов физической защиты (ПФЗ) с учетом определенных в процессе анализа уязвимости ЯО угроз и моделей нарушителя. Обеспечение необходимого уровня эффективности СФЗ должно предусматривать комплекс работ по контролю и анализу выполнения СФЗ возложенных на нее задач по обеспечению физической защиты и определению путей повышения эффективности СФЗ или поддержанию ее на требуемом уровне.

Для унификации подходов к оценке эффективности в Росатоме разработаны соответствующие нормативные документы [11.1, 11.2].

Целью оценки эффективности СФЗ является оценка способности СФЗ пресечь несанкционированные действия нарушителя. Под

термином «пресечение» понимается своевременный выход сил охраны на рубежи (к месту) нейтрализации нарушителя.

Задачами оценки эффективности являются:

- выявление элементов СФЗ, преодолевая которые, нарушитель имеет наибольшую вероятность совершения диверсий или хищения ЯМ;
- рассмотрение и выявление наиболее вероятных сценариев действий нарушителя для совершения диверсий или хищения ЯМ;
- выявление уязвимых мест действующих СФЗ, формально отвечающих требованиям, установленным в нормативных документах;
- анализ причин появления уязвимых мест в СФЗ;
- оценка вероятности пресечения тех или иных действий нарушителя силами охраны, действующими по сигналу тревоги при внешней и внутренней угрозе;
- выбор оптимальных проектных решений на этапе создания и модернизации СФЗ;
- подготовка предложений администрации ЯО и силам охраны ЯО по совершенствованию СФЗ и ее отдельных структурных элементов.

Проведение оценки эффективности СФЗ обязательно на этапе проектирования СФЗ при ее создании или совершенствовании. Количественный показатель эффективности может быть использован в процессе проектирования СФЗ для сравнения конкурирующих вариантов СФЗ, в том числе для обоснования целесообразности проведения модернизации СФЗ. При этом сравниваются показатели эффективности существующей СФЗ и предлагаемого варианта СФЗ.

Для действующей СФЗ оценка эффективности проводится в полном объеме при отсутствии на ЯО результатов ранее проведенной оценки эффективности СФЗ с привлечением специализированной организации, а также в следующих случаях:

- при планируемых изменениях на объекте в СФЗ ЯО;
- по результатам проведения анализа уязвимости ЯО;
- при выявлении новых уязвимых мест в результате государственного надзора, ведомственного и внутриобъектового контроля безопасности ЯО.

В указанных случаях может проводиться как оценка эффективности СФЗ в полном объеме, так и уточнение результатов оценки эффективности, проведенной при проектировании СФЗ.

Основанием для проведения оценки эффективности при планируемых изменениях на объекте и в СФЗ ЯО являются:

- изменение структуры объекта и дислокации УМ и ПФЗ ЯО;
- изменение вида или способа охраны;
- изменение численности подразделений охраны;
- передислокация мест расположения сил охраны;
- другие причины, связанные с изменением времени реагирования сил охраны на сигналы тревоги;
- изменение структуры и состава комплекса технических средств физической защиты (КТСФЗ).

Основанием для проведения оценки эффективности по результатам проведения анализа уязвимости действующего ЯО, а также государственного надзора, ведомственного и внутриобъектового контроля безопасности ЯО являются:

- уточнение модели нарушителя;
- уточнение и выявление новых УМ и ПФЗ, в отношении которых могут быть совершены несанкционированные действия;
- выявление новых угроз для ЯО и способов их осуществления;
- изменение технологических процессов на ЯО;
- выявление элементов СФЗ, которые не отвечают предъявляемым к ним требованиям;
- выявление элементов СФЗ, преодолевая которые нарушитель имеет благоприятные возможности для совершения диверсий или хищения ЯМ или других ПФЗ;

- другие причины, повышающие уязвимость ЯМ, ЯУ и других ПФЗ.

11.2. Показатели эффективности СФЗ ЯО

Как отмечалось выше, в качестве основного критерия оценки эффективности СФЗ принимается способность СФЗ пресечь несанкционированные действия нарушителя. Эффективность СФЗ оценивается количественными показателями, отражающими вероятность пресечения несанкционированных действий нарушителя силами охраны, действующими по сигналу тревоги.

Показатели эффективности зависят от определенных в процессе анализа уязвимости ЯО угроз, моделей нарушителя и уязвимых мест. Для оценки эффективности СФЗ применяют:

- дифференциальный показатель эффективности, учитывающий вероятность пресечения акции нарушителя против одной цели (УМ, ПФЗ);
- интегральный показатель, представляющий собой усредненный с учетом важности целей показатель эффективности СФЗ по ЯО в целом.

При оценке эффективности учитываются:

- вероятности обнаружения нарушителя техническими средствами физической защиты (ТСФЗ);
- время задержки нарушителя физическими барьерами (ФБ);
- времена движения сил охраны и нарушителя на ЯО;
- взаимное расположение технических средств (возможность определения направления движения нарушителей);
- наличие систем и средств оптико-электронного наблюдения;
- наличие средств идентификации вторжения (контрольно-следовая полоса, пломбы);
- тактика действий сил охраны;

- оснащение нарушителя (транспортные средства, инструменты, оружие и др.).

Оценка эффективности основана на событийно-временном анализе развития конфликтной ситуации в системе «охрана – нарушитель» при внешней и внутренней угрозах.

Цели нарушителя рассматриваются только в стационарном состоянии.

Оценка эффективности СФЗ проводится для двух типов акций нарушителя:

- хищение ЯМ и других ПФЗ;
- диверсия против ЯМ, ЯУ или пункта хранения ЯМ.

Работы обычно проводятся в два этапа. На первом этапе, на основе инженерных расчетов, проводится предварительная оценка эффективности СФЗ. На втором этапе, с помощью специализированного программного обеспечения, проводится окончательная оценка эффективности СФЗ.

Работа проводится в следующей последовательности:

- формирование рабочей группы и организация совещания специалистов по оценке эффективности СФЗ ЯО;
- сбор исходных данных для проведения оценки эффективности СФЗ ЯО;
- разработка формализованного описания ЯО;
- оценка эффективности СФЗ ЯО при внешней угрозе;
- оценка эффективности СФЗ ЯО при внутренней угрозе;
- оформление и анализ результатов оценки эффективности СФЗ ЯО.

Оценка эффективности СФЗ проводится отдельно для внешних и внутренних угроз.

Оценка эффективности СФЗ при внешней угрозе проводится для всех УМ ЯО и ПФЗ с учетом моделей нарушителя, разработан-

ных при проведении анализа уязвимости ЯО и уточненных на этапах сбора ИД и составления формализованного описания объекта.

При расчетах показателя эффективности предполагается, что внешний нарушитель при преодолении каждого из рубежей СФЗ может выбрать один из двух вариантов действий:

- вариант 1 – внешний нарушитель преодолевает рубеж ФЗ по возможности скрытно. Такой вариант характеризуется низким значением вероятности обнаружения и значительным временем преодоления ФБ;
- вариант 2 – внешний нарушитель преодолевает рубеж ФЗ по возможности быстро, в том числе, используя специальные силовые инструменты и взрывчатые вещества для разрушения ФБ. Такой вариант характеризуется высоким значением вероятности обнаружения и малым временем преодоления ФБ.

Оценка эффективности СФЗ при внешней угрозе должна проводиться для обоих вариантов действий нарушителя.

Интегральный показатель эффективности СФЗ ЯО при внешней угрозе ($P_{\text{внеш.}}$) оценивается исходя из выражения

$$P_{\text{внеш.}} = \sum_{j=1}^{J} ß_j * P_{\text{внеш.}\,j},$$

где J – число целей нарушителя на ЯО (УМ ЯО, ПФЗ); $ß_j$ – весовой коэффициент, отражающий важность (категорию) j-й цели; $P_{\text{внеш.}j}$ – дифференциальный показатель эффективности СФЗ – вероятность предотвращения акции внешнего нарушителя против j-й цели.

Весовой коэффициент $ß_j$ определяется следующим образом: рабочая группа экспертным путем присваивает каждой цели нарушителя ранг (R_j) от 1 до 10 в зависимости от последствий, которые может повлечь за собой акция нарушителя, или категории, присвоенной УМ ЯО, ПФЗ. Больший ранг присваивается более важной цели.

$ß_j$ рассчитывается по формуле

$$ß_j = R_j / \sum_{j=1}^{J} R_j .$$

Дифференциальный показатель эффективности СФЗ оценивается исходя из выражения:

$$P_{\text{внеш},j} = 1 - \prod_{k=1}^{K} (1 - P_{\text{внеш},jk}),$$

где K – общее количество отдельных тактических групп сил охраны (периметровая тревожная группа и другие), участвующих в развитии конфликтной ситуации при проникновении нарушителя на ЯО; $P_{\text{внеш},jk}$ – вероятность пресечения k-й тактической группой сил охраны акции внешнего нарушителя против j-й цели.

При рассмотрении нескольких сценариев действий нарушителя против j-й цели дифференциальный показатель эффективности СФЗ этого УМ ЯО, ПФЗ принимается равным минимальному значению по всем рассмотренным сценариям.

Сценарий действий нарушителя, соответствующий минимальному значению вероятности предотвращения акции против j-й цели, принимается в качестве критического.

Вероятность предотвращения k-й тактической группой сил охраны акции внешнего нарушителя против j-й цели в общем случае является функцией:

$$P_{\text{внеш},jk} = f(P_{ojl}, P_{\text{зах},jkl}) \ (l=1,..., L),$$

где L – общее количество рубежей СФЗ, которые необходимо преодолеть внешнему нарушителю для проникновения к j-й цели; P_{ojl} – вероятность обнаружения нарушителя, действующего против j-й цели на l-м рубеже СФЗ; $P_{\text{зах},jkl}$ – вероятность захвата k-й тактической группой сил охраны, действующей по сигналам начиная с l-го рубежа СФЗ, нарушителя, совершающего акцию против j-й цели.

Вероятности обнаружения принимаются равными значениям тактико-технических характеристик для соответствующих ТСФЗ, указанным в технической документации.

Численные значения вероятностей $P_{\text{внеш}.jk}$ оцениваются согласно выражениям, приведенным в справочном приложении к нормативному документу [11.1].

Вероятности захвата нарушителя определяются для соответствующей оперативной ситуации с учетом выполнения условия:

$$\Delta T = T_{\text{о}} - T_{\text{н}} < 0,$$

где ΔT – резерв времени сил охраны; $T_{\text{о}}$ и $T_{\text{н}}$ – времена действий охраны и нарушителя (с момента поступления сигнала тревоги) соответственно.

Вероятности захвата оцениваются согласно выражению

$$P(\Delta T = T_{\text{о}} - T_{\text{н}} < 0) = F(-x),$$

где $F(x)$ – функция распределения стандартной нормальной случайной величины; x – математическое ожидание приведенного резерва времени сил охраны, определяемое из выражения

$$x = \frac{M[T^{O}] - M[T^{H}]}{\sqrt{D[T^{O}] + D[T^{H}]}},$$

где $M[T]$ и $D[T]$ – соответственно математическое ожидание и дисперсия времен сил охраны и нарушителя.

Значения времен нарушителя и охраны складываются из составляющих, относящихся к различным этапам их действий (для нарушителя – время преодоления ФБ периметра, локальных зон, зданий, помещений; для сил охраны – время сборов, время движения, время осмотра участка периметра и т.п.).

Расчет математических ожиданий и дисперсий времен действий нарушителя и охраны производится исходя из соотношения для суммы независимых случайных величин, согласно которому при

$$T = \sum_{i=1}^{I} t_i$$

имеем

$$M[T] = \sum_{i=1}^{I} M[t_i], \qquad D[T] = \sum_{i=1}^{I} D[t_i],$$

где t_i, i=1,..., I – отдельные случайные величины; $M[t_i]$ и $D[t_i]$ – математические ожидания и дисперсии величин t_i.

Эффективность СФЗ при внутренней угрозе проводится для всех УМ ЯО и ПФЗ с учетом полномочий различных групп персонала объекта. Под группой персонала понимается группа сотрудников ЯО, имеющих одинаковые полномочия доступа.

Оценка эффективности должна проводиться для каждой группы персонала отдельно.

При расчетах показателя эффективности предполагается, что внутренний нарушитель при преодолении каждого из рубежей СФЗ может выбрать один из двух вариантов действий.

- Вариант 1. Внутренний нарушитель преодолевает рубеж ФЗ, используя свои служебные полномочия, по путям санкционированного прохода. При этом, для уменьшения вероятности пресечения акции, внутренний нарушитель может пытаться выбросить/забросить запрещенные к проносу предметы из/в зону ФЗ, используя каналы, не доступные для проникновения человека (трубопроводы, окна верхних этажей, между прутьев решетки и пр.).
- Вариант 2. Внутренний нарушитель преодолевает рубеж ФЗ «силовым» способом, используя несанкционированный канал проникновения, аналогично внешнему нарушителю. Предполагается, что последующие рубежи ФЗ нарушитель преодолевает также «силовым» способом.

Оценка эффективности СФЗ при внутренней угрозе проводится в предположении, что сценарий действий нарушителя состоит из двух частей: проход с использованием своих полномочий до какой-

либо зоны ФЗ и затем – «силовой» прорыв. В частном случае второй этап действий нарушителя может отсутствовать.

При оценке рассматриваются различные наборы инструментов и материалов, которые нарушитель может проносить на объект и использовать при прорыве к цели и совершении акции.

При оценке учитывается возможность использования для совершения несанкционированных действий инструментов и материалов, находящихся на ЯО всилу производственной или иной необходимости.

Интегральный показатель эффективности СФЗ ЯО при внутренней угрозе ($P_{\text{внут.}}$) для каждой из целей оценивается исходя из выражения

$$P_{\text{внут.}} = \sum_{i=1}^{I} \gamma_i * P_{\text{внут.}i},$$

где I – число групп персонала, выделенных на объекте, применительно к рассматриваемой цели; γ_i – весовой коэффициент, равный отношению числа лиц, относящихся к i-й группе к общему числу сотрудников ЯО; $P_{\text{внут.}i}$ – дифференциальный показатель эффективности СФЗ ЯО при внутренней угрозе – вероятность предотвращения акции нарушителем из числа i-й группы допуска против рассматриваемой цели.

Дифференциальный показатель эффективности СФЗ ЯО оценивается, исходя из выражения:

$$P_{\text{внут.}i} = 1 - (\prod_{l=1}^{L} (1 - P_{\text{внут.}il})) * (1 - P_{li}),$$

где L – количество рубежей ФЗ, преодолеваемых нарушителем с использованием своих служебных полномочий; $P_{\text{внут.}il}$ – вероятность задержания нарушителя, проносящего запрещенные предметы или объект хищения, на контрольно-пропускном пункте (КПП) l-го рубежа ФЗ; P_{li} – вероятность захвата нарушителя, действующе-

го «силовым» способом из секции, находящейся за *l*-м рубежом ФЗ.

При рассмотрении нескольких сценариев действий внутреннего нарушителя против *j*-й цели, дифференциальный показатель эффективности СФЗ этого УМ ЯО, ПФЗ принимается равным минимальному значению по всем рассмотренным сценариям.

Вероятность задержания нарушителя на КПП, проносящего запрещенные предметы и материалы, в общем случае определяется из выражения

$$P^*_{\text{внут.}}=1-(1-P^*_{\text{досм.}} * P_{\text{досм.}}) * (1-P^*_{\text{мет.}} * P_{\text{мет.}}) *$$

$$(1-P^*_{\text{ВВ}} * P_{\text{ВВ}}) * (1-P^*_{\text{ЯМ}} * P_{\text{ЯМ}}) ,$$

где $P^*_{\text{досм.}}$ – вероятность проведения личного досмотра; $P_{\text{досм.}}$ – вероятность обнаружения запрещенных предметов при досмотре; $P^*_{\text{мет.}}$ – вероятность проведения досмотра с применением металлообнаружителя; $P_{\text{мет.}}$ – вероятность обнаружения металлических предметов при помощи металлообнаружителя; $P^*_{\text{ВВ}}$ – вероятность проведения досмотра с применением детектора ВВ; $P_{\text{ВВ}}$ – вероятность обнаружения ВВ при помощи детектора ВВ; $P^*_{\text{ЯМ}}$ – вероятность проведения досмотра с применением детектора ЯМ; $P_{\text{ЯМ}}$ – вероятность обнаружения ЯМ при помощи детектора.

Примечание. *Если у нарушителя отсутствует тот или иной запрещенный к проносу материал или предмет, то вероятность обнаружения для соответствующего детектора принимается равной 0.*

Вероятности захвата внутреннего нарушителя, действующего «силовым» способом (P_{li}), определяются аналогично вероятностям захвата внешнего нарушителя. При этом не учитываются рубежи ФЗ, пройденные внутренним нарушителем легальным способом (если нарушитель дошел до секции, находящейся за *l*-м рубежом ФЗ, то он считается необнаруженным).

Показатель эффективности СФЗ является основным показателем качества, характеризующим применение СФЗ по назначению. Однако на практике любая система характеризуется и другими показателями. Например, немаловажным фактором являются затраты на создание и эксплуатацию системы. Важны также и другие свойства системы (надежность, помехоустойчивость и др.).

Чтобы оценить СФЗ на наличие каждого из этих свойств, необходимо:

- выбрать количественный показатель, характеризующий данное свойство;
- разработать методику его оценки;
- иметь необходимые исходные данные.

Например, количественным показателем затрат является стоимость необходимого оборудования СФЗ и работ по оснащению ЯО техническими средствами физической защиты. Методика получения стоимостных показателей достаточно проста и традиционна – это сметные расчеты. Размерность данного показателя (рубль или USD) также понятна.

Надежность КТСФЗ, как и любой другой технической системы, характеризуется показателями безотказности (среднее время наработки на отказ и др.), ремонтопригодности (среднее время восстановления и др.) и т.п.

Помехоустойчивость обычно характеризуется таким показателем, как среднее время наработки на ложное срабатывание технических средств.

Можно предложить использовать показатели, характеризующие такие «тонкие» свойства системы, как скорость развертывания сигнализационных средств (для мобильных технических средств), маскируемость и др.

Имеются соответствующие методики, которые позволяют получить количественную оценку указанных показателей, а также соответствующие базы исходных данных.

Выше рассмотрены методы оценки эффективности СФЗ и других показателей.

Следует отметить, что работа по сбору необходимых исходных данных, подготовке к расчетам и непосредственно оценке эффективности СФЗ требует проведения значительного количества рутинных действий и вычислений. При этом в процессе разработки концептуального проекта оценка эффективности проводится неоднократно, по мере выбора оптимальных (целесообразных) решений. Эти и ряд других факторов неизменно приводят к мысли о необходимости автоматизации процедуры оценки эффективности СФЗ и, как следствие, к разработке специализированных компьютерных программ. Техническая революция в области создания и применения персональных компьютеров сделала эту задачу актуальной и выполнимой.

11.3. Компьютерные программы для оценки эффективности СФЗ ЯО

В России широко известны специализированные компьютерные программы, разработанные в США, предназначенные для оценки эффективности СФЗ, такие как [11.3, 11.4]:

EASY, SAVI – программы MS DOS, предназначенные для оценки эффективности СФЗ при «внешней» угрозе;

ET – программа MS DOS, предназначенная для оценки эффективности при «внутренней» угрозе;

ASSESS – программа (для WINDOWS), предназначенная для оценки эффективности СФЗ при «внешней» и «внутренней» угрозах, при наличии сговора «внешнего» и «внутреннего» нарушителей, для расчета вероятности нейтрализации вооруженного противника.

Наибольшее распространение в России получила программа ASSESS, переданная российским ЯО в рамках международного

сотрудничества. Эта программа имеет ряд существенных преимуществ по сравнению с более ранними американскими специализированными компьютерными программами.

Однако в ходе применения программы ASSESS российскими ЯО и с приобретением практического опыта работ был выявлен ряд недостатков этой программы, ограничивающих возможности ее применения на российских ЯО. Например, в программе ASSESS заложена жесткая тактика действий сил реагирования, не всегда соответствующая российской специфике. Кроме того, в составе программы ASSESS отсутствует база данных по реальным тактико-техническим характеристикам ТСФЗ и ФБ, относящихся к чувствительной информации.

В России также ведутся работы по созданию отечественных специализированных компьютерных программ оценки эффективности СФЗ, позволяющих максимально полно учитывать российскую специфику. Можно отметить следующие компьютерные программы, разработанные ГУП «СНПО «Элерон»» [11.5]:

АЛЬФА – программа (для MS DOS), предназначенная для оценки эффективности СФЗ при «внешней» угрозе на объектах с жестко заданной структурой рубежей СФЗ;

ВЕГА-2 – программа (для WINDOWS), предназначенная для оценки эффективности СФЗ как при «внешней», так и при «внутренней» угрозах, позволяющая производить расчеты на основе аналитического метода и имитационного моделирования.

Особенно следует отметить программный комплекс (ПК) ВЕГА-2, который позволяет более гибко описывать тактики действий сил охраны и вероятного нарушителя, учитывает целеуказующую функцию средств обнаружения, существенную для объектов с разветвленным деревом целей нарушителя, позволяет оценить вклад применения охранного телевидения на различных рубежах ФЗ и имеет другие возможности. Программный комплекс ВЕГА-2 по-

стоянно совершенствуется и модернизируется с учетом практического опыта его применения на конкретных ЯО.

Остановимся более подробно на компьютерных программах ASSESS и ВЕГА-2.

Эти программы объединяет общий подход к их построению. Программы являются модульными, при этом рабочие модули программ объединяются специальными оболочками-менеджерами в программные комплексы.

Программа ASSESS (разработка США) содержит следующие основные модули:

Facility (объект) – модуль, предназначенный для описания объекта с точки зрения его физической защиты;

Outsider (внешний нарушитель) – модуль, предназначенный для оценки эффективности системы физической защиты при внешней угрозе;

Insider (внутренний нарушитель) – модуль, предназначенный для оценки эффективности системы физической защиты при внутренней угрозе;

Collusion (сговор) – модуль, предназначенный для оценки эффективности системы физической защиты при сговоре внешнего и внутреннего нарушителей;

Neutralization (нейтрализация) – модуль, предназначенный для оценки результатов боестолкновения сил реагирования (охраны) и нарушителя.

Как уже отмечалось ранее, программа ASSESS является WINDOWS приложением, и работа с ней производится с помощью стандартных приемов, используемых для работы в WINDOWS. В связи с этим, при дальнейшем изложении материала вопросы запуска программ, сохранения, загрузки, копирования и удаления файлов не рассматриваются.

Для инициализации работы программы ASSESS необходимо запустить файл Assess.exe, активизирующий работу менеджера.

Работа с программой начинается с создания файла описания объекта с помощью запуска программы Facility.

Объект физической защиты описывается так называемыми схемами последовательности действий нарушителя (СПДН), представляющими собой графическое описание объекта, включающее в себя:

- зоны защиты – какие-либо части территории объекта, например, не охраняемая (внешняя) территория, охраняемая территория, охраняемое здание, помещение, место дислокации цели нарушителя;
- элементы защиты – основные элементы, составляющие систему физической защиты (например, ограждение, стена здания, дверь, окно, контрольно-пропускной пункт и другие);
- слои защиты – совокупности элементов защиты, разделяющие зоны защиты объекта.

Каждый элемент защиты описывается двумя основными характеристиками:

- продолжительность задержки действий нарушителя;
- вероятность обнаружения нарушителя.

Последовательности элементов защиты, преодолевая которые нарушитель может проникнуть к цели, называются маршрутом движения нарушителя.

Интерфейс программы Facility позволяет пользователю в удобном и наглядном виде создавать графическое описание объекта защиты. При этом один файл описания соответствует одной цели нарушителя. Если на объекте имеется несколько различных целей, расположенных в разных зонах защиты, необходимо для каждой из них создавать свой файл описания.

Программа Facility позволяет одновременно описывать объект защиты в двух состояниях: рабочее и нерабочее время. Эти состояния объекта могут отличаться между собой. Например, транспортный контрольно-пропускной пункт в нерабочее время

может быть закрыт и будет работать только как участок охраняемого периметра.

Для ввода характеристик элементов защиты в программу ASSESS включены базы данных по вероятностям обнаружения нарушителя и временам задержки его действий. При этом данные вводятся для различных способов преодоления элемента физической защиты, таких как:

- без оборудования;
- с ручными инструментами;
- с инструментами с приводом (специальные инструменты);
- с помощью взрывчатых веществ;
- с помощью автотранспорта (там, где это возможно).

Каждый элемент защиты может включать в себя до трех различных элементов обнаружения и физических барьеров, имеющих различные характеристики. Кроме того, при описании элемента защиты определяется наличие или отсутствие на нем специальных средств обнаружения запрещенных к проносу материалов и предметов, наличие или отсутствие часовых сил охраны, вводятся их характеристики.

Программа позволяет учесть, какие зоны защиты могут преодолеваться нарушителем на автотранспорте, а какие нет.

После завершения описания объекта файл описания сохраняется, и можно приступить к проведению оценок при внешней и внутренней угрозах. Для этого надо закрыть программу Facility и выйти в программу-менеджер.

На рис. 11.1 представлен пример рабочего экрана файла описания объекта.

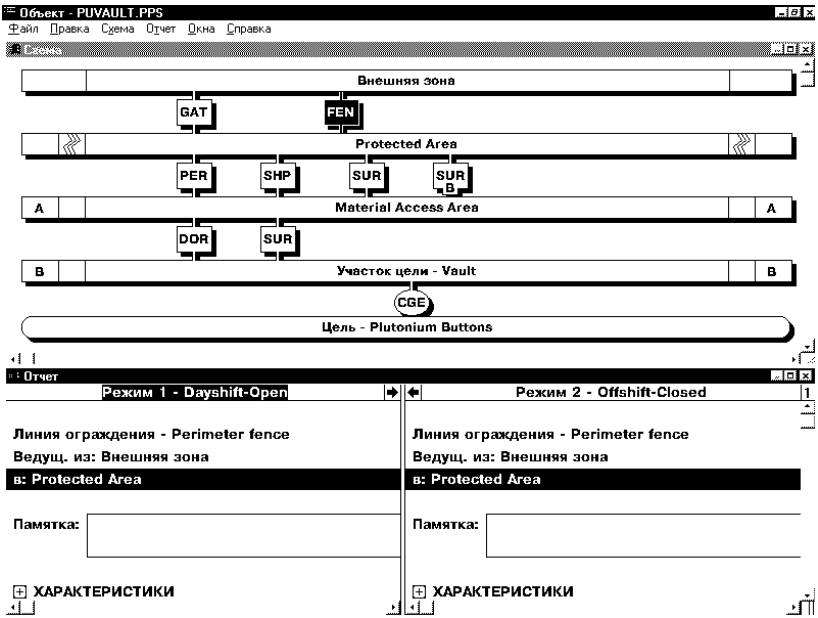


Рис. 11.1. Пример рабочего экрана программы Facility

Для инициализации программы оценки эффективности при внешней угрозе необходимо выделить в окне программы-менеджера сохраненный файл программы Facility и запустить программу Outsider.

Перед проведением оценки необходимо определить модель нарушителя, для которой будет выполнена оценка. Для этого необходимо задать угрозу, определить стратегию нарушителя, методы его действий. Выход в справочные меню этих характеристик осуществляется двойным «кликом» на соответствующем разделе рабочего экрана программы Outsider.

Для проведения оценки эффективности необходимо в меню программы Outsider выбрать опцию «Анализ». Если описание объ-

екта не завершено или выполнено некорректно, программа выдаст соответствующее сообщение.

В результате оценки программа определит так называемый критический маршрут нарушителя, т.е. маршрут, на котором эффективность системы физической защиты минимальна, и выделит его на экране красным светом. В текстовой части окна отобразится информация о численном значении показателя эффективности, резерве времени сил реагирования.

Программа позволяет проводить оценку эффективности по десяти различным наихудшим, с точки зрения задач охраны, маршрутам нарушителя и для десяти различных времен реагирования сил охраны в заданном интервале времени.

На рис. 11.2 представлен пример рабочего экрана файла оценки эффективности при внешней угрозе.

Для инициализации программы оценки эффективности при внутренней угрозе необходимо выделить в окне программы-менеджера сохраненный файл программы Facility и запустить программу Insider.

Перед проведением оценки эффективности СФЗ при внутренней угрозе необходимо определить список внутренних нарушителей, лиц, имеющих допуск в различные охраняемые зоны объекта, а также определить их полномочия. Перечень полномочий определяет, в какие зоны охраны допущен внутренний нарушитель, каким процедурам досмотра он подвергается при проходе и т.д.

В результате проводимой оценки эффективности программа Insider рассчитывает вероятности обнаружения системой физической защиты каждого типа внутренних нарушителей как на пути движения к цели, так и на пути ухода с объекта.

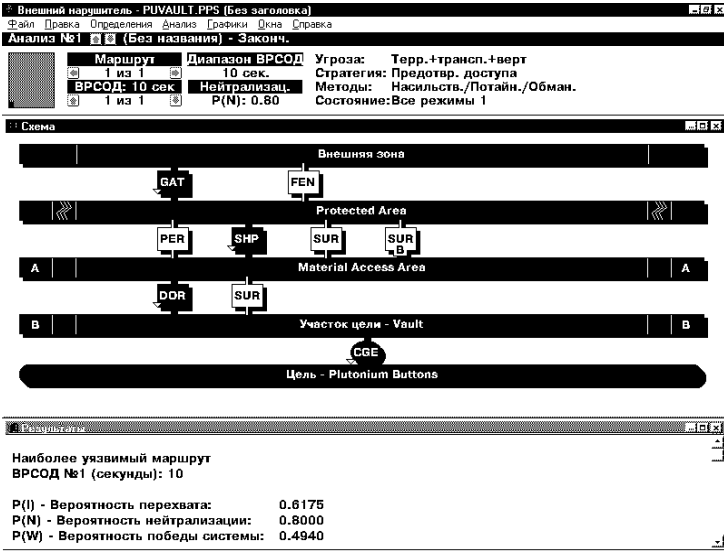


Рис. 11.2. Пример рабочего экрана программы Outsider

На рис. 11.3 представлен пример рабочего экрана файла оценки эффективности при внутренней угрозе.

Для инициализации программы оценки эффективности при сговоре необходимо провести оценку эффективности при внешней и внутренней угрозах и сохранить полученные результаты, выделить в окне программы-менеджера сохраненный файл программы Facility и запустить программу Collusion.

Модуль определяет, понижается ли значение показателя эффективности СФЗ при внешней угрозе, если внешнему нарушителю помогает внутренний, перемещая ему навстречу ядерный материал из места его хранения или использования в менее важную зону охраны, пользуясь своими полномочиями.

Если эффективность СФЗ не снижается, программа делает вывод о нецелесообразности сговора. В случае если эффективность

СФЗ снижается, программа рассчитывает и отображает ее численное значение.

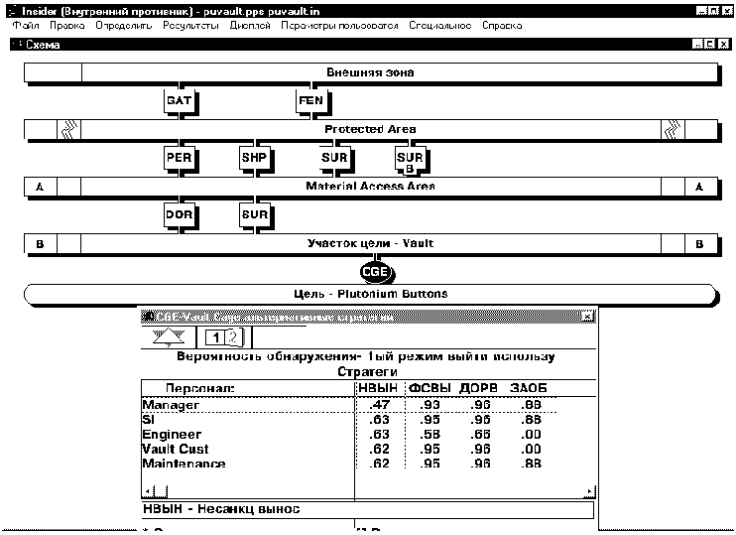


Рис. 11.3. Пример рабочего экрана программы Insider

Программа Neutralization не имеет жесткой «привязки» к модулю описания объекта и запускается из программы-менеджера выбором соответствующего приложения в меню.

Программа Neutralization позволяет оценивать вероятность победы сил охраны при боестолкновении с нарушителем.

Перед проведением непосредственных расчетов задаются численность сил охраны (реагирования) и нарушителя, временные интервалы, в течение которых к силам охраны может прибыть подкрепление. Кроме того, для каждого бойца задаются его основные характеристики, такие как:

- вид оружия;
- расстояние между противоборствующими сторонами;

- уровни защиты при ведении огня и перезарядке оружия.

Кроме значения вероятности нейтрализации нарушителя модуль позволяет оценить ожидаемое время боя, количество выживших и погибших с обеих сторон, а также исследовать чувствительность рассчитанного значения вероятности нейтрализации к изменению характеристик нарушителей и сил охраны.

Российская компьютерная программа ВЕГА-2 [11.5] разработана как программный комплекс, объединяющий в себе ряд программ-модулей, таких как:

- модуль описания объекта;
- расчетный модуль;
- модуль формирования отчета;
- автоматизированные базы данных по средствам обнаружения, физическим барьерам, моделям нарушителей.

Программа ВЕГА-2 является WINDOWS приложением.

Работа с программой начинается с запуска модуля описания объекта. В результате работы с модулем разрабатывается формализованное описание объекта с точки зрения его физической защиты, включающее в себя:

- зоны защиты – какие-либо части территории объекта, например, не охраняемая (внешняя) территория, защищенная внутренняя и особо важная зоны;
- секции – элементы формализованного описания ЯО, описывающие локализованные части объекта, отделенные от других частей рубежами ФЗ. Секциями описываются территория ЯО, локальные зоны, помещения (группы помещений и т.д.);
- цели нарушителя – элементы формализованного описания ЯО, описывающие уязвимые места объекта или предметы физической защиты;

- переходы – элементы формализованного описания ЯО, описывающие вероятные каналы проникновения нарушителя, например, дверь, окно, стена и др.

Каждый переход является элементом вероятного маршрута движения нарушителя и описывается двумя основными характеристиками: временем преодоления и вероятностью обнаружения нарушителя. Для удобства описания переходов в составе программы ВЕГА-2 разработаны специальные шаблоны описания типовых переходов, позволяющие пользователю в удобном и наглядном виде вводить необходимые для расчетов исходные данные.

На рис. 11.4 и 11.5 представлены примеры рабочих экранов основного окна модуля описания и шаблона описания двери соответственно.

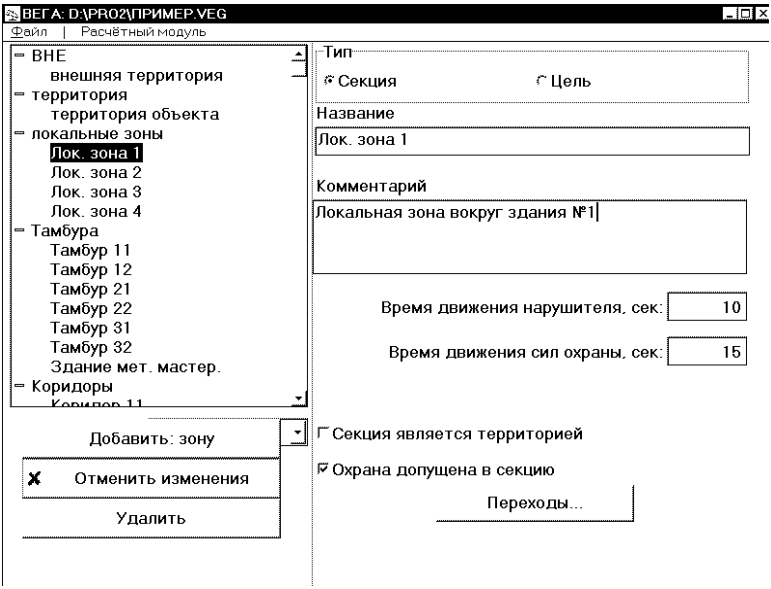


Рис. 11.4. Пример рабочего экрана модуля описания объекта

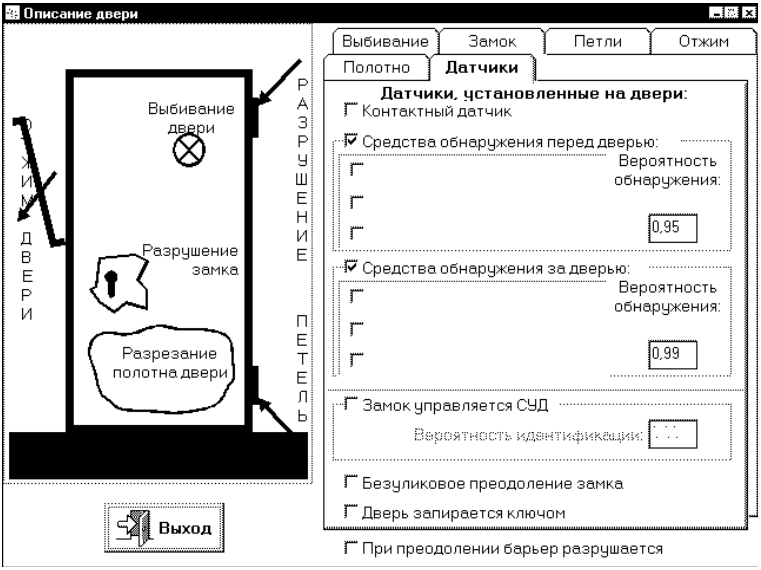


Рис. 11.5. Пример рабочего экрана шаблона описания «Дверь»

К модулю описания объекта подключены автоматизированные справочники по средствам обнаружения и временам преодоления физических барьеров, а также специализированные расчетные процедуры для оценки времен разрушения для отдельных типов физических барьеров.

В отличие от программы ASSESS, файл описания объекта программы ВЕГА-2 описывает все цели нарушителя, находящиеся на объекте.

После завершения описания объекта хотя бы одной цели можно приступать к проведению оценки эффективности СФЗ. Для этого необходимо выбрать опцию «расчетный модуль».

Расчетный модуль объединяет в себе расчетные процедуры как для внешней, так и для внутренней угрозы. При внешней угрозе имеется возможность проведения расчетов для диверсионной ак-

ции и акции хищения ядерных материалов. При этом возможно провести оценку аналитическим методом или с помощью имитационного моделирования.

Для проведения оценки эффективности при внешней угрозе необходимо инициализировать расчетный модуль, задав модель вероятного нарушителя. Для этого в модуль встроена автоматизированная база данных моделей нарушителя

На рис.11.6 представлен пример главного рабочего экрана расчетного модуля.

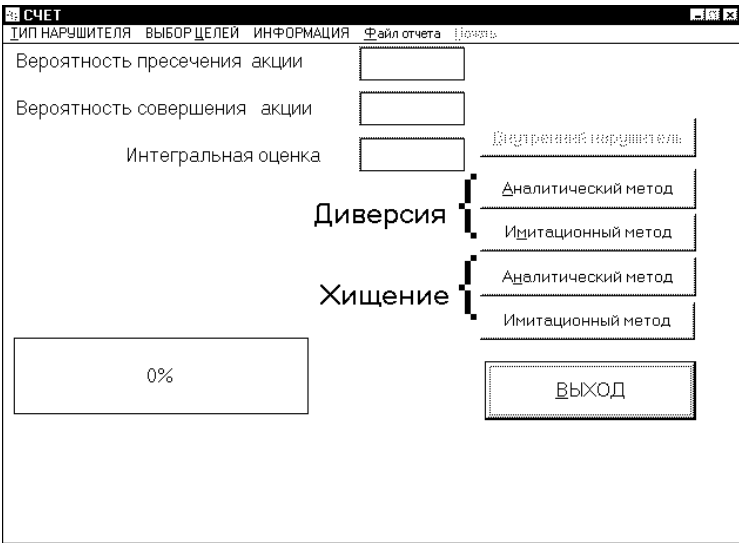


Рис. 11.6. Пример главного рабочего экрана расчетного модуля

После задания модели нарушителя можно приступать к расчетам. Программный модуль позволяет проводить оценку эффективности СФЗ для:

- конкретной цели нарушителя;
- группы целей, относящихся к одной категории важности;

- объекта в целом.

Результатом оценки эффективности является вероятность пресечения нарушителя силами реагирования, рассчитанная для наихудшей, с точки зрения охраны, ситуации. При этом расчетный модуль отражает критический маршрут нарушителя, которому соответствует оценка.

Для проведения оценки эффективности при внутренней угрозе необходимо в главном окне расчетного модуля выбрать опцию «внутренний нарушитель».

Для оценки эффективности при внутренней угрозе так же, как и в программе ASSESS, необходимо определить список внутренних нарушителей, лиц, имеющих допуск в различные охраняемые зоны объекта, а также определить их полномочия. Перечень полномочий определяет, в какие зоны охраны допущен внутренний нарушитель, каким процедурам досмотра он подвергается при проходе и т. д.

Основным отличием программы ВЕГА-2 от программы ASSESS является то, что при оценке эффективности при внутренней угрозе предполагается, что внутренний нарушитель может перейти к силовым действиям для проникновения в зону охраны, секцию или к цели, если он не имеет права легального доступа к ним. При этом учитывается наличие или отсутствие на контрольно-пропускных пунктах специальных средств обнаружения запрещенных к проносу материалов и предметов (оружие, ядерные материалы, взрывчатые вещества), а также наличие или отсутствие этих материалов и предметов у нарушителя. Таким образом, программа оценки эффективности при внутренней угрозе оценивает:

- вероятность обнаружения внутреннего нарушителя при попытке вноса им в разрешенную зону или секцию запрещенных материалов и предметов, используя каналы легального прохода;
- вероятность пресечения силовых действий внутреннего нарушителя в зависимости от его оснащения;

- итоговый показатель эффективности при внутренней угрозе для каждого типа нарушителя с учетом комбинации скрытных и силовых действий в зависимости от его оснащения.

На рис. 11.7 представлен пример рабочего экрана расчетного модуля при внутренней угрозе.

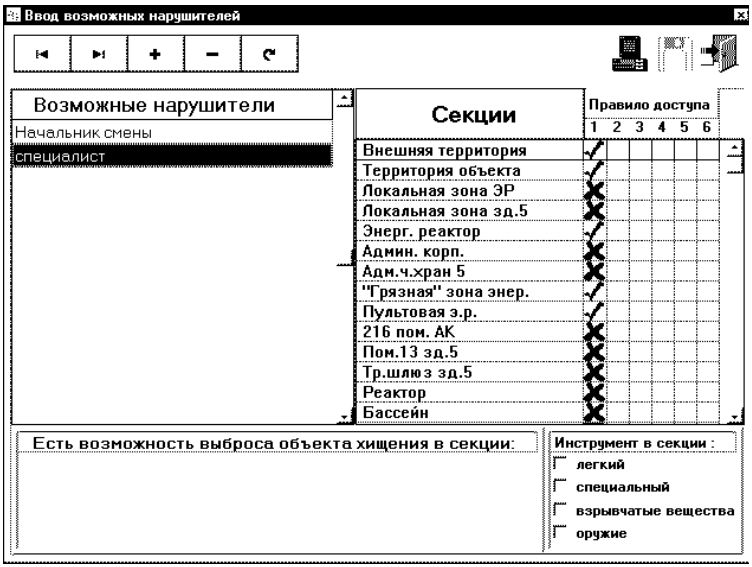


Рис. 11.7. Пример рабочего экрана расчетного модуля при внутренней угрозе

При расчетах для внутренней угрозы проводится оценка эффективности СФЗ как при движении нарушителя к цели (диверсионная акция), так и при попытке ухода с объекта (акция хищение).

Модуль формирования отчетов автоматически формирует отчет о результатах оценки эффективности при внешней и внутренней угрозах для выбранной цели нарушителя. При необходимости отчет может быть распечатан.

Вопросы для самоконтроля

1. Какова задача оценки эффективности СФЗ?
2. Какие существуют показатели эффективности СФЗ?
3. Как проводится оценка эффективности защиты ЯО от внешнего нарушителя?
4. Как проводится оценка эффективности защиты ЯО от внутреннего нарушителя?
5. Какие существуют компьютерные программы для оценки эффективности СФЗ?
6. Опишите формализованный объект.

12. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ

Развитие систем физической защиты ядерных объектов связано с все большей интеграцией методов автоматизированной обработки информации. При этом сохранение таких характеристик информации, обрабатываемой системой физической защиты, как целостность, доступность и конфиденциальность, во многом стало определять эффективность работы самой системы ФЗ. Последствия от воздействия различных угроз, приводящих к искажению (разрушению) или разглашению информации, а также ограничения в санкционированной доступности к ней могут привести к сбоям работы СФЗ и к чувствительным последствиям. В данном случае приобретает актуальность решение проблемы обеспечения безопасности информации, обращаемой в СФЗ ЯО.

Особенностью проблемы обеспечения информационной безопасности является наравне с ее комплексностью тот факт, что на решение ее накладывает свои требования специфика ЯО и ее СФЗ.

При этом теоретической базой рассмотрения должна стать теория защиты информации, которая получила свое фундаментальное развитие в трудах отечественных ученых, практической базой – опыт ведущих специалистов, работающих в этой области, нормативной базой – нормативные документы федерального и отраслевого уровня, методической базой – [П.3, 12.1 – 12.13].

12.1. Основы методологии обеспечения информационной безопасности объекта

Анализ подходов к обеспечению информационной безопасности (ИБ) СФЗ ЯО базируется на определенном теоретическом базисе, который включает в себя термины и определения, а также описание типовых процедур, связанных с проектированием, созданием

и эксплуатацией соответствующих систем. Методология обеспечения информационной безопасности любого объекта (на примере автоматизированных систем) изложена в нормативных документах Государственной технической комиссии при Президенте РФ (ГТК РФ) [12.1] и в хорошо известных работах В.А. Герасименко и А.А. Малюка [12.2, 12.3].

Под термином «информационная безопасность», согласно определению ГТК РФ [12.1], понимается состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системой, от внутренних или внешних угроз, которые могут привести к следующим последствиям:

- искажению информации (нарушение целостности);
- утрате или снижению степени доступности (нарушение доступности);
- нежелательному разглашению информации (нарушение конфиденциальности).

В конечном итоге эти нарушения приводят к материальному и моральному ущербу владельца или пользователя информации.

Комплекс мероприятий, направленных на обеспечение информационной безопасности, связывают с определением «защита информации». Эти мероприятия проводятся с целью предотвращения ущерба от действия угроз безопасности информации, где угроза является потенциальной возможностью нарушения безопасности информации [12.4].

Первое и самое главное, от чего зависит уровень обеспечения ИБ объекта – это правильная формулировка и оптимальная реализация политики безопасности (ПБ). В соответствии с определением ГТК РФ [12.1] политика безопасности – это правила разграничения доступа, представляющие собой совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа. Таким образом, политика информационной безопасности СФЗ ЯО –

это формальная спецификация правил и рекомендаций, на основе которых пользователи этой системы используют, накапливают и распоряжаются ее информационными ресурсами.

Политику безопасности необходимо формулировать для конкретного объекта на уровне руководителей объекта. Цель обеспечения ИБ объекта не может быть достигнута, пока на самом высоком уровне не будет определено, чего следует добиваться, и не будут выделены ресурсы, которые позволят должным образом защитить информационную инфраструктуру объекта и обеспечить управление ею.

Политика безопасности должна быть согласована с основами теории защиты информации, а также со всеми нормативно-правовыми документами, соблюдение которых требуется от организации.

Политика информационной безопасности должна быть определена в момент проектирования СФЗ ЯО (в некоторых случаях требуется разработать ПБ для уже существующей системы).

Процесс выработки ПБ включает в себя следующие этапы:

1. Организационный (определение состава группы разработчиков ПБ; определение способа выработки ПБ – на основе какой информации будет определена ПБ, кем эта информация будет предоставляться и какова степень доверия к этой информации; вид представления ПБ как документа).

2. Описание позиции организации (отношение руководства объекта к ИБ).

3. Определение применимости ПБ – ответ на вопросы о том где, как, когда, кем и к чему применима данная ПБ, т.е. перечисление всех пользователей и ресурсов, кого эта ПБ касается.

4. Определение ролей и обязанностей – указание ответственных лиц и их обязанностей в отношении разработки и внедрения различных аспектов ПБ, а также в случае нарушения ПБ.

5. Выработка мер защиты, реализующих ПБ на конкретном объекте, обоснование выбора именно такого перечня мер защиты, указание на то, какие угрозы ИБ наиболее эффективно предотвращаются какими мерами защиты.

6. Выработка мер по соблюдению ПБ (задачи конкретным подразделениям объекта).

В отношении защиты информации ПБ должна определять:

- кто может иметь доступ к конфиденциальной информации вообще и при особых обстоятельствах;
- как регламентируется соглашение о неразглашении конфиденциальной информации между руководством и сотрудниками организации и какова ответственность за нарушение данного соглашения;
- как должна храниться и передаваться конфиденциальная информация (зашифрованной, заархивированными файлами, закодированной с помощью специальных программ и т.д.);
- в каких системах может храниться и обрабатываться конфиденциальная информация;
- информация какой степени секретности может быть распечатана на физически незащищенных принтерах;
- как конфиденциальная информация удаляется из систем и запоминающих устройств (например, размагничиванием носителей данных, чисткой жестких дисков, резкой бумажных копий).

Рассмотрение ряда вопросов, относящихся к разработке политики безопасности СФЗ ЯО, может стать методической основой предметной области, связанной с информационной безопасностью СФЗ ЯО. В этом случае необходимо рассмотреть особенности СФЗ ЯМ как информационного объекта (глава 8), провести классификацию информации, которая обращается в рассматриваемых системах, рассмотреть модель вероятного нарушителя, провести класси-

фикацию угроз ИБ и возможных последствий реализации этих угроз, рассмотреть каналы утечки или нарушения целостности информации, требования и порядок разработки подсистемы защиты информации, сформулировать требования по ЗИ от несанкционированного доступа (НСД) с учетом требований по классификации СФЗ.

Перед тем, как перейти к рассмотрению перечисленных вопросов, необходимо описать нормативную базу, определяющую разработку, реализацию и использование систем обеспечения информационной безопасности СФЗ ЯО.

12.2. Нормативные документы

При обеспечении информационной безопасности СФЗ ЯО необходимо учитывать требования законодательных и нормативных правовых актов. При этом можно выделить следующие виды документов:

- Федеральные законы «Об использовании атомной энергии», «О государственной тайне», «Об информации, информационных технологиях и защите информации»;
- документ, утвержденный постановлением Правительства РФ: «Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» (№ 456 от 19.07.2007);
- документы, утвержденные Президентом РФ: «Перечень сведений, подлежащих засекречиванию по Минатому России», «Перечень сведений конфиденциального характера» (№188 от 06.03.97);
- федеральные документы по защите информации, составляющей государственную и служебную тайну. Основные требования по защите информации, составляющей государственную и

служебную тайну, порядок разработки, введения в действие и эксплуатации технических систем и иных объектов информатизации в защищенном исполнении определены «Специальными требованиями и рекомендациями по защите информации, составляющей государственную тайну, от утечки по техническим каналам» (СТР), утвержденными решением Гостехкомиссии России от 23.05.97 №55, другими федеральными и отраслевыми нормативными документами по защите информации;

- отраслевые документы. К ним относятся следующие документы Минатома России:

1. Отраслевые методические рекомендации: «Концепция информационной безопасности СФЗ ЯОО» [12.6] .

В концепции ИБ СФЗ ЯО (далее – Концепция) на основе анализа современного состояния и тенденций развития систем физической защиты ядерно-опасных и иных значимых объектов охраны, а также проблемы информационной безопасности определены цели, задачи и объекты информационной безопасности.

Концепция представляет собой систему взглядов на проблему информационной безопасности СФЗ ЯО и служит методологической основой:

- разработки комплекса нормативных и методических документов, регламентирующих деятельность в области информационной безопасности СФЗ;
- создания и эксплуатации конкретных систем защиты информации в СФЗ ЯО.

В концепции, исходя из назначения, структуры, состава и функций СФЗ, изложены цели и задачи обеспечения информационной безопасности СФЗ, особенности функционирования современных СФЗ, объекты информационной безопасности, характерные свойства функционирования СФЗ с точки зрения информаци-

онной безопасности, защищаемые в СФЗ сведения, модель вероятного нарушителя СФЗ с точки зрения информационной безопасности, перечень и анализ угроз и возможных способов нарушения информационной безопасности, основные направления и мероприятия по защите информации.

2. Руководящий документ «Общие требования по защите информации в СФЗ ЯОО» [12.7]. Данный документ определяет требования по защите информации в СФЗ ЯО Минатома России и предназначен для заказчиков и разработчиков систем физической защиты, технических и программных средств и систем, а также средств защиты информации, являющихся компонентами СФЗ и предназначенных к использованию в СФЗ.

3. Руководящий документ «СФЗ ЯОО. Автоматизированные системы управления и обеспечения физической защиты. Защита информации от несанкционированного доступа. Классификация автоматизированных систем и требования по безопасности информации» [12.8]. Настоящий руководящий документ (РД) устанавливает классификацию автоматизированных систем управления и обеспечения физической защиты ядерно-опасных объектов на базе средств вычислительной техники (СВТ), подлежащих защите от несанкционированного доступа и воздействий эксплуатационного персонала и посторонних лиц, в том числе и от несанкционированных программных воздействий, нарушающих безопасность информационных ресурсов и работоспособность СВТ. К каждому из классов ставится в соответствие совокупность требований по безопасности информации.

Руководящий документ является нормативным техническим документом для заказчиков, разработчиков и эксплуатационного персонала СФЗ и их автоматизированных систем при постановке и

реализации требований по безопасности информации, для органов контроля за состоянием СФЗ и ее подсистемы защиты информации.

Настоящий временный РД до его замены руководящим документом федерального уровня может использоваться в качестве нормативного документа, на соответствие требованиям которого в системе сертификации № РОСС RU.0001.01БИ00 производится сертификация программных и программно-технических средств защиты информации от НСД, предназначенных к использованию в СФЗ, а также аттестация СФЗ по требованиям безопасности информации.

4. Отраслевой документ «Положение о порядке использования систем радиосвязи на предприятиях Минатома России» [12.9]. Данный документ определяет порядок создания, развертывания и эксплуатации на предприятиях Министерства систем и средств радиосвязи, используемых в системах комплексной безопасности стационарных и подвижных ЯО, в том числе систем физической защиты.

5. Временный руководящий документ «Классификация систем транкинговой радиосвязи, используемых в системах физической защиты, по требованиям безопасности информации» [12.10]. Настоящий документ вводит классификацию систем транкинговой радиосвязи, предназначенных для использования в системах физической защиты Минатома России по требованиям безопасности информации.

12.3. Классификация информации в СФЗ ЯО с учетом требований к ее защите

Характерными свойствами функционирования СФЗ ЯО как автоматизированной системы, обрабатывающей информацию, с точки зрения информационной безопасности, являются:

- наличие информации, составляющей государственную и служебную тайну, а также информации конфиденциального характера о различных аспектах функционирования СФЗ и непосредственно ЯО, в том числе, возможно, количественных и качественных характеристиках ЯМ; ядерно-опасных изделий и ЯЭУ;
- наличие служебной информации системы защиты информации от НСД в СФЗ, требующее обеспечения ее конфиденциальности и целостности;
- территориальное размещение компонентов СФЗ в различных охраняемых зонах ЯО, доступ в которые имеет ограниченный и строго дифференцированный персонал;
- размещение компонентов СФЗ в транспортных средствах, перевозящих ЯМ;
- строгое разделение функциональных обязанностей, распределение полномочий и прав на выполнение регламентных действий между персоналом СФЗ;
- относительное постоянство используемых штатных программных средств, включенных в регламент работы СФЗ, и узкая функциональная специализация СФЗ в отличие от автоматизированных систем общего назначения;
- исключение доступа части персонала, связанного с управлением и обеспечением функционирования СФЗ, в обслуживаемую им охраняемую зону.

Из анализа перечисленных особенностей функционирования СФЗ ЯО следует вывод о необходимости защиты информации в СФЗ ЯО, что обусловлено наличием в системе информации, составляющей государственную и служебную тайну, раскрывающей систему физической защиты конкретного ЯО, а также чувствительной по отношению к несанкционированным воздействиям на нее, в результате чего может быть снижена эффективность функционирования СФЗ в целом или ее отдельных элементов.

Основные требования по защите информации, составляющей государственную и служебную тайну, порядок разработки, введения в действие и эксплуатации технических систем и иных объектов информатизации в защищенном исполнении определены «Специальными требованиями и рекомендациями по защите информации, составляющей государственную тайну, от утечки по техническим каналам» (СТР), утвержденными решением Гостехкомиссии России от 23.05.97 №55, а также другими федеральными и отраслевыми нормативными документами по защите информации [12.6 – 12.8], к которым необходимо добавить:

- «Перечень сведений, подлежащих засекречиванию по Минатому России»;
- «Перечень сведений конфиденциального характера», утвержденный Указом Президента Российской Федерации от 06.03.97 №188.

Прежде всего, должны защищаться сведения, в результате разглашения, утраты, утечки по техническим каналам, уничтожения, искажения или подмены которых может быть нарушено функционирование СФЗ или снижена эффективность ее функционирования. Эти сведения должны защищаться в первую очередь в тех компонентах СФЗ, где они наиболее доступны для потенциального нарушителя, т.е. необходимо следовать принципу «равнопрочности защиты». Необходимо также учитывать вопрос «времени жизни»

защищаемой информации, имея в виду снижение или потерю ценности такой информации для потенциального нарушителя в результате ее изменения, замены по истечении определенного временного интервала.

Объем и степень секретности обрабатываемой и передаваемой между различными уровнями управления СФЗ информации (уровень чувствительности ресурсов), режим обработки данных и соответственно уровень требований по защите информации будут различны в зависимости от степени интеграции различных подсистем СФЗ, от характера взаимодействия в конкретной системе, а также с системами учета и контроля ядерных материалов, технологической безопасности.

В данном случае можно выделить информационные объекты и сведения, которые необходимо защищать.

К объектам защиты относятся:

• собственно информация, составляющая государственную и служебную тайну, а также чувствительная по отношению к несанкционированным воздействиям на нее, представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, информационных массивов и баз данных;

• средства и системы информатизации (автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, специализированные микропроцессоры), средства и системы связи и передачи данных (технические средства приема, передачи и обработки информации, телефонной и радиосвязи, звукозаписи, звукоусиления, звуковоспроизведения, телевизионные устройства и другие технические средства обработки речевой, алфавитно-цифровой, графической и видеоинформации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное про-

граммное обеспечение), используемые для обработки, хранения и передачи защищаемой информации;

• датчики охранной сигнализации;

• технические средства и системы, не обрабатывающие непосредственно защищаемую информацию, но размещенные в помещениях, где обрабатывается (циркулирует) защищаемая информация;

• помещения пунктов управления СФЗ, в которых ведутся конфиденциальные разговоры, раскрывающие особенности функционирования СФЗ.

В СФЗ, с учетом конкретных особенностей функционирования ЯО и применяемых технических средств и систем, необходимо защищать следующие сведения, раскрывающие:

• систему физической защиты предприятий, отдельных производств, зданий, сооружений, в которых производятся работы с ЯМ или ядерно-опасными изделиями, осуществляется их хранение, размещаются ЯУ, в том числе при их транспортировке;

• структуру и систему функционирования комплекса инженерно-технических средств СФЗ;

• топологию ЯО, его отдельных охраняемых зон и их СФЗ с указанием схем расположения средств СФЗ и их обеспечивающих подсистем;

• маршруты и конкретные сроки транспортировки ЯМ;

• систему защиты автоматизированных систем управления СФЗ и контроля доступа от несанкционированного воздействия;

• наличие, место установки или принцип действия скрытых технических средств СФЗ;

• технические характеристики технических средств СФЗ;

• содержание таблиц кодовых комбинаций для запирающих устройств повышенной стойкости;

• систему защиты пропусков, магнитных карт, устройств идентификации личности от подделки для конкретных объектов;

• характеристики контроля работоспособности СФЗ и ее составляющих;

• действия сил охраны и персонала СФЗ на попытки нарушения СФЗ;

• размещение и оснащение, маршруты и графики патрулирования сил охраны;

• расчетное время прибытия сил охраны или службы безопасности к месту нарушения по сигналу тревоги;

• расчетное время задержки нарушителя инженерными средствами физической защиты для конкретного объекта;

•служебную информацию системы защиты информации от НСД (пароли, ключи, таблицы санкционирования и т.д.) в СФЗ;

• демаскирующие признаки СФЗ и ее составляющих, раскрывающие информацию, подлежащую защите (внешний вид и особенности установки технических средств СФЗ; функциональные и побочные излучения технических средств СФЗ; реакция сил охраны при различных воздействиях на технические средства СФЗ).

Требования по защите информации в СФЗ ЯО могут быть эффективно выполнены только при наличии в СФЗ подсистемы ЗИ, которая является необходимой составной частью СФЗ как АС.

Основой создания политики безопасности СФЗ ЯО является определение каналов утечки информации и характера информационных угроз, а также формулирование модели потенциального нарушителя ИБ СФЗ ЯО. Рассмотрим эти факторы отдельно с учетом требований отраслевых документов [12.6,12.7].

12.4. Каналы утечки информации в СФЗ ЯО

С учетом особенностей функционирования СФЗ возможны следующие основные каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств [12.6, 12.7]:

- несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники и связи;
- побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы защищенной зоны ЯО;
- акустическое излучение информативного речевого сигнала;
- прослушивание телефонных и радиопереговоров, ведущихся в СФЗ;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- воздействие на технические и программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена (электромагнитное, через специально внедренные электронные и программные средства);
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев и других средств отображения информации с помощью оптических средств;

• визуальное наблюдение за ЯО в зонах прямой видимости, в том числе с помощью фотографических и оптико-электронных средств разведки.

Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах защищенной зоны ЯО. Это возможно как следствие:

• непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций и технологического оборудования помещений;

• случайного прослушивания телефонных разговоров при проведении профилактических работ;

• случайного прослушивания радиопереговоров;

• просмотра информации с экранов дисплеев и других средств ее отображения.

12.5. Перечень и анализ угроз информационной безопасности СФЗ ЯО

Основными источниками угроз информационной безопасности СФЗ ЯО в общем случае являются [12.6, 12.7]:

• стихийные бедствия и катастрофы;

• отказы и неисправности технических средств и средств информатизации СФЗ;

• деятельность человека, непосредственно и опосредованно влияющая на информационную безопасность и являющаяся основным источником угроз.

По сфере воздействия на СФЗ и ее информационные ресурсы источники угроз информационной безопасности могут быть разде-

лены на внешние и внутренние, с точки зрения их нахождения вне или внутри системы при ее проектировании и функционировании, а также места приложения возможных способов нарушения информационной безопасности.

Внешние угрозы исходят от природных явлений (стихийных бедствий), катастроф, внешних нарушителей, а также от лиц, не входящих в состав пользователей и обслуживающего персонала СФЗ и не имеющих непосредственного контакта с СФЗ как системой информатизации и ее информационными ресурсами.

Внутренние угрозы исходят от пользователей и обслуживающего персонала СФЗ с различными правами доступа (как допущенного, так и не допущенного к защищаемым сведениям), а также разработчиков системы (при осуществлении авторского надзора и доработок системы).

Отказы и неисправности технических средств и средств информатизации СФЗ также относятся к определенному типу угроз:

- отказы и неисправности технических средств обнаружения, телевизионного наблюдения, идентификации личности, управления доступом, систем сбора и обработки информации от всех датчиков, средств и систем информатизации, в том числе из-за нарушений в системе электропитания;
- отказы и неисправности средств защиты информации и технических средств контроля эффективности принятых мер по защите информации;
- сбои программного обеспечения, программных средств защиты информации и программных средств контроля эффективности принятых мер по защите информации.

К угрозам, связанным с деятельностью человека как основного источника угроз, могут быть отнесены:

1. Непреднамеренные действия человека по отношению к информации и СФЗ как автоматизированной системе:

• непреднамеренная деятельность человека, в том числе некомпетентные действия персонала, приводящие к таким событиям, как пожары, технические аварии и т.д.;

• некомпетентные действия и ошибки, допущенные при проектировании СФЗ, ее отдельных подсистем, в том числе подсистемы защиты информации;

• некомпетентные или ошибочные действия пользователей и обслуживающего персонала СФЗ, в том числе администратора АС (администратора безопасности), приводящие к нарушению целостности и доступности информации, а также работоспособности СФЗ, непреднамеренному заражению компьютеров программами-вирусами при использовании посторонних программ;

• некомпетентные или неосторожные действия персонала при профилактике, техническом обслуживании или ремонте технических средств, приводящие к повреждению аппаратуры;

• неправильное обращение с магнитными носителями при их использовании или хранении;

• халатность и недостаточно четкое исполнение служебных обязанностей.

2. Умышленная (преднамеренная) деятельность человека:

• деятельность разведывательных и специальных служб по добыванию информации, навязыванию ложной информации, нарушению работоспособности СФЗ в целом и отдельных ее составляющих;

• противозаконная и преступная деятельность международных, отечественных групп и формирований, а также отдельных лиц, направленная на проникновение на ядерно-опасные объекты, хищение ядерных материалов, а также несанкционированные, в том числе диверсионные, действия в отношении ядерных материалов,

установок или транспортных средств, перевозящих ядерные материалы;

• нарушение пользователями и обслуживающим персоналом СФЗ установленных регламентов сбора, обработки и передачи информации, а также требований информационной безопасности.

Преднамеренные действия вероятных нарушителей:

• хищение оборудования, влекущее за собой нарушение работоспособности системы, утрату данных;

• хищение магнитных носителей, в том числе временное, с целью копирования, подделки или уничтожения данных, получения доступа к данным и программам;

• разрушение оборудования, магнитных носителей или дистанционное стирание информации (например, с помощью магнитов);

• несанкционированное считывание информации или копирование данных с магнитных носителей (жестких и гибких дисков, оперативного запоминающего устройства, в том числе и остатков «стертых» файлов) и с использованием терминалов, оставленных без присмотра;

• внесение изменений в базу данных или в отдельные файлы в пределах выделенных полномочий для подделки или уничтожения информации;

• считывание или уничтожение информации, внесение в нее изменений в базах данных или в отдельных файлах с присвоением чужих полномочий путем подбора или выявления паролей при похищении или визуальном наблюдении, использования программных средств для преодоления защитных свойств системы, использования включенного в систему терминала, оставленного без присмотра;

• несанкционированное изменение своих полномочий на доступ или полномочий других пользователей в обход механизмов безопасности;

• сбор и анализ использованных распечаток, документации и других материалов для копирования информации или выявления паролей, идентификаторов, процедур доступа и ключей;

• визуальный перехват информации, выводимой на экран дисплеев или вводимой с клавиатуры для выявления паролей, идентификаторов и процедур доступа;

• перехват электромагнитного излучения от технических средств СФЗ для копирования информации и выявления процедур доступа;

• копирование информации и паролей при негласном пассивном подключении к кабелю локальной сети или приеме электромагнитного излучения сетевого адаптера;

• выявление паролей легальных пользователей при негласном активном подключении к кабелю локальной сети при имитации запроса сетевой операционной системы;

• установка скрытых передатчиков (для вывода информации или паролей с целью копирования данных или доступа к ним по легальным каналам связи с компьютерной системой) в результате негласного посещения в нерабочее время, посещения с целью ремонта, настройки, профилактики оборудования или отладки программного обеспечения, скрытной подмены элементов оборудования при оставлении их без присмотра в рабочее время;

• создание условий для разрушения информации или нарушения работоспособности системы, несанкционированного доступа к информации на разных этапах производства или доставки оборудования, разработки или внедрения системы путем включения в аппаратуру и программное обеспечение аппаратных и программных

закладок, программ-вирусов, ликвидаторов с дистанционным управлением или замедленного действия и т.п.;

• воздействие на объекты систем и сетей связи или на передаваемые в сетях данные при осуществлении различных манипуляций над сообщениями и программным обеспечением этих объектов как на стадии установления соединения, так и на стадиях передачи данных и разрыва установленного соединения, приводящее к модификации, удалению, задержке, переупорядочиванию, дублированию регулярных и посылке ложных сообщений, воспрепятствованию передаче сообщений, осуществлению ложных соединений;

• проникновение в систему через внешний (например, телефонный) канал связи с присвоением полномочий одного из легальных пользователей с целью подделки, копирования или уничтожения данных;

• проникновение в систему через телефонную сеть при перекоммутации канала на модем злоумышленника после вхождения легального пользователя в связь и предъявлении им своих полномочий с целью присвоения прав этого пользователя на доступ к данным;

• визуальное наблюдение за ЯО в зонах прямой видимости, в том числе с помощью фотографических и оптико-электронных средств разведки.

В зависимости от конкретной структуры СФЗ, в том числе используемых в системе сетей связи, и протоколов передачи данных перечень возможных воздействий нарушителя на технические и программные средства и передаваемую информацию будет различен.

Возможные способы нарушения информационной безопасности СФЗ могут быть подразделены на информационные, программно-математические, физические, радиоэлектронные и организационно-правовые.

Информационные способы нарушения информационной безопасности включают:

- противозаконный сбор, распространение и использование информации;
- манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование данных и программ;
- незаконное уничтожение информации;
- хищение информации из баз данных;
- нарушение адресности и оперативности информационного обмена;
- нарушение технологии обработки данных и информационного обмена.

Программно-математические способы нарушения информационной безопасности включают:

- внедрение программ-вирусов;
- внедрение «программных закладок» как на стадии проектирования системы (в том числе путем заимствования «зараженного» закладками программного продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или воздействие на информацию и средства ее защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации подсистемы защиты информации.

Физические способы нарушения информационной безопасности включают:

- уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, целенаправленное внесение в них неисправностей;

• уничтожение, хищение и разрушение машинных или других оригиналов носителей информации;

• хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей (паролей) средств защиты информации от несанкционированного доступа;

• воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз информационной безопасности;

• диверсионные действия по отношению к объектам информатизации (взрывы, поджоги, технические аварии и т.д.).

Радиоэлектронные способы нарушения информационной безопасности включают:

• перехват информации в технических каналах ее утечки (побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации, наводок в коммуникациях (сети электропитания, заземления, радиотрансляции, пожарной сигнализации и так далее) и линиях связи, путем прослушивания конфиденциальных разговоров с помощью акустических, виброакустических и лазерных технических средств разведки, прослушивания конфиденциальных телефонных и радиоразговоров, визуального наблюдения за работой средств отображения информации);

• перехват информации в сетях передачи данных и линиях связи;

• внедрение электронных устройств перехвата информации в технические средства и помещения;

• навязывание ложной информации по сетям передачи данных и линиям связи;

• радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы нарушения информационной безопасности включают невыполнение требований законодательства и задержки в разработке и принятии необходимых нормативных документов в области информационной безопасности.

Результатом реализации угроз информационной безопасности и осуществления посягательств (способов воздействия) на информационные ресурсы и средства информатизации СФЗ в общем случае являются:

• нарушение секретности (конфиденциальности) информации (разглашение, утрата, хищение, утечка и перехват и т.д.);

• нарушение целостности информации (уничтожение, искажение, подделка и т.д.);

• нарушение санкционированной доступности информации и работоспособности СФЗ как автоматизированной системы (блокирование данных и самой АС, разрушение элементов АС, компрометация подсистемы защиты информации и т.д.).

Наиболее реальными и опасными угрозами информационной безопасности СФЗ являются несанкционированный доступ и несанкционированные воздействия по отношению к информации, обрабатываемой средствами вычислительной техники и связи, а также несанкционированный доступ к средствам ее обработки (чувствительным ресурсам АС СФЗ), которые могут быть реализованы нарушителями (персоналом СФЗ и посторонними лицами, в том числе сотрудниками подразделений ЯО, работающими в пределах защищенной, внутренней, особо важной зон ЯО, а также зон ограниченного доступа, но не допущенными к работе в АС СФЗ). Их действия могут привести как к утечке или нарушению целостности информации, так и к нарушению работоспособности

технических средств СФЗ и санкционированной доступности информации.

12.6. Модель вероятного нарушителя информационной безопасности СФЗ ЯО

Для создания политики безопасности, проектирования СФЗ для конкретного объекта и реализации СФЗ в целом и ее системы обеспечения информационной безопасности в частности, необходимо учитывать модель вероятного нарушителя СФЗ, в том числе с точки зрения возможностей нарушения информационной безопасности [12.6, 12.7].

В качестве вероятных нарушителей могут выступать внешние и внутренние нарушители, а также внешние нарушители в сговоре с внутренними.

К внешним нарушителям относятся лица, не имеющие права доступа в защищаемую зону, действия которых направлены на проникновение на ядерно-опасный объект, хищение ядерных материалов, совершение диверсии в отношении ЯО и ЯМ или сбор разведданных о ЯО.

В качестве внутреннего нарушителя могут выступать лица из числа персонала СФЗ и посторонние лица, в том числе сотрудники подразделений ЯО, работающие в пределах защищенной, внутренней, особо важной зон ЯО, а также зон ограниченного доступа, но не допущенные к работе в АС СФЗ, разработчики различных технологических и охранных систем, а также различные специалисты, привлекаемые для оказания услуг.

Все они имеют разного уровня допуск к информационным ресурсам и возможность реализации угроз информационной безопасности СФЗ, в том числе с помощью технических средств.

Каждый из этих нарушителей отличается друг от друга уровнем осведомленности о функционировании основных жизнеобес-

печивающих систем ЯО и его СФЗ, возможности, подготовленности и оснащенности к преодолению СФЗ в противоправных целях.

Модель нарушителя разрабатывается с учетом расположения и функционирования конкретного ЯО для каждой защищаемой зоны, утверждается Заказчиком и является основополагающим документом для оценки эффективности СФЗ объекта.

При разработке модели нарушителя учитываются:

- тип нарушителя;
- характер информационных угроз;
- численность вероятного нарушителя, его вооружение и оснащенность;
- возможные способы преодоления рубежей и контроля доступа;
- решаемые нарушителем задачи на основе добываемой информации о ЯО и его СФЗ;
- возможность доступа в жизненно важные объекты информатизации СФЗ (пункты управления, «серверные», хранилища информации, узлы связи, к коммуникациям и к системе электропитания), к средствам защиты и техническим средствам СФЗ;
- полномочия внутреннего нарушителя;
- возможность совместных действий нарушителей различных типов.

В своей противоправной деятельности вероятный нарушитель может использовать портативные средства перехвата информации (для внешнего нарушителя), средства воздействия на информацию, технические средства СФЗ и средства информатизации, финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

Получить защищаемую информацию о ЯО и его СФЗ вероятный нарушитель может посредством:

• санкционированного доступа к защищаемой информации, т.е. использования внутренним нарушителем доступной ему для выполнения служебных обязанностей информации;

• использования технических средств наблюдения и перехвата информации из-за пределов защищаемой зоны, визуального наблюдения за ЯО, в том числе с помощью фотографических и оптико-электронных средств;

• разглашения ее обслуживающим персоналом с соответствующими правами доступа;

• осуществления несанкционированного доступа в охраняемые зоны и к информационным ресурсам СФЗ;

• хищения различных информационных носителей.

Сбор информации о ЯО и его СФЗ может осуществляться вероятным нарушителем путем изучения и анализа:

• принципов и структуры построения и функционирования объекта аналогичного класса и его СФЗ;

• степени оснащения объекта техническими средствами обнаружения и техническими конструкциями, выполняющими функцию задержки, построенными на различных физических принципах и имеющими разную конструкцию, системы организации доступа на ЯО, динамики и организации пропуска на объект грузов, в том числе и ядерных материалов;

• принципов построения технических средств СФЗ по характеристикам их физических полей;

• уязвимых мест технических средств СФЗ, не вызывающих срабатывание датчиков (систем), путем имитации непосредственного вторжения на охраняемую территорию;

• тактической схемы действий сил охраны ЯО в различных условиях функционирования объекта с оценкой временных и вероятностных характеристик ложных тревог;

• информативности потоков, циркулирующих в системах (тревожной сигнализации, сигналов изменения логики принятия решений и др.), а также сигналов контроля целостности линий связи;

• возможности подавления (нарушения) функционирования технических средств и средств информатизации СФЗ дистанционными методами (активными помехами, воздействием на датчики средств обнаружения, линии связи, устройства систем сбора и обработки информации, ослепление средств оптического и инфракрасного диапазонов и т.п.);

• функционирования системы защиты информации от НСД в СФЗ с целью ее компрометации;

• возможности воздействия на системы электропитания и заземления средств информатизации;

• пропускной системы и системы доступа на ЯО.

В связи с этим, основной задачей службы безопасности и сил охраны, с точки зрения информационной безопасности, является предотвращение этих акций со стороны вероятного нарушителя и своевременная нейтрализация его действий.

12.7. Мероприятия по комплексной защите информации в СФЗ ЯО

Исходя из модели вероятного нарушителя СФЗ и перечня угроз информационной безопасности, разрабатывается подсистема защиты информации, которая реализуется в виде комплекса средств и мероприятий по защите информации в СФЗ [12.6].

Основными направлениями защиты информации являются:

• обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения и подделки за счет несанкционированного доступа (НСД) и специальных воздействий;

• обеспечение защиты информации, в том числе речевой, от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

Подсистема защиты информации должна предусматривать комплекс организационных, программных, технических и криптографических средств и мер по защите информации (рис. 12.1) в процессе традиционного документооборота, при автоматизированной обработке и хранении информации, при ее передаче по каналам связи, при ведении на пунктах управления СФЗ разговоров, раскрывающих информацию с ограниченным доступом в отношении СФЗ.

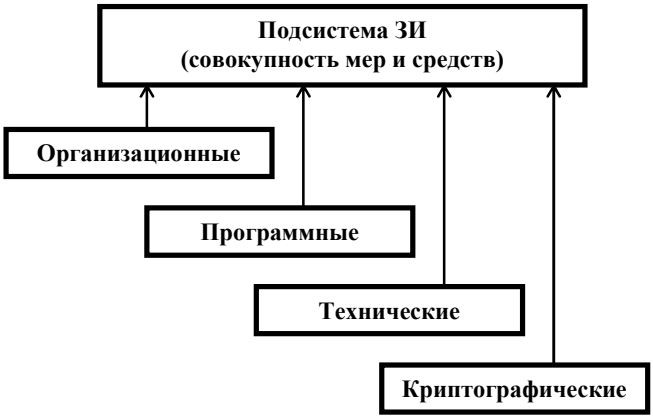


Рис. 12.1. Структура подсистемы ЗИ

В качестве основных мер защиты информации, циркулирующей в технических средствах и обсуждаемой на пунктах управле-

ния СФЗ, при транспортировке ЯМ в рамках указанных направлений обеспечения информационной безопасности осуществляются:

• реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации секретного (конфиденциального) характера;

• физическая защита собственно пунктов управления СФЗ и других жизненно важных объектов и технических средств информатизации, в том числе размещенных в транспортных средствах, перевозящих ЯМ, с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения, транспортные средства посторонних лиц, хищение документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри защищенной зоны технических средств разведки или промышленного шпионажа;

• ограничение доступа персонала и посторонних лиц в здания и в помещения (в зоны ограниченного доступа), где размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация секретного (конфиденциального) характера, непосредственно к самим средствам информатизации и коммуникациям;

• разграничение доступа пользователей и обслуживающего персонала к данным, программным средствам обработки (передачи) и защиты информации;

• учет документов, информационных массивов, регистрация действий пользователей информационных систем и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;

• применение сертифицированных по требованиям безопасности информации технических и программных средств;

• криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи (при необходимости, определяемой особенностями функционирования конкретных СФЗ);

• надежное хранение традиционных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;

• необходимое резервирование технических средств и дублирование массивов и носителей информации;

• снижение уровня и информативности ПЭМИН, создаваемых различными элементами автоматизированных систем и технических средств СФЗ;

• снижение уровня акустических излучений;

• электрическая развязка цепей питания, заземления и других цепей объектов информатизации, выходящих за пределы контролируемой территории;

• активное зашумление в различных диапазонах;

• противодействие оптическим средствам наблюдения и лазерным средствам перехвата;

• проверка эффективности защиты помещений пунктов управления СФЗ и технических средств и систем в реальных условиях их размещения и эксплуатации с целью определения достаточности мер защиты с учетом установленной категории;

• предотвращение внедрения в автоматизированные системы программ-вирусов, программных закладок.

В целях дифференцированного подхода к защите информации, осуществляемого в целях разработки и применения необходимых и

достаточных средств защиты информации, а также обоснованных мер по достижению требуемого уровня информационной безопасности, в СФЗ должно проводиться:

- категорирование помещений пунктов управления СФЗ, в которых ведутся конфиденциальные разговоры, раскрывающие особенности функционирования СФЗ;
- категорирование технических средств и систем, предназначенных для обработки, передачи и хранения информации, составляющей государственную тайну;
- классификация автоматизированных систем СФЗ;
- классификация систем транкинговой радиосвязи.

Категорирование помещений пунктов управления СФЗ и технических средств и систем производится в установленном порядке в соответствии с существующими требованиями в зависимости от степени секретности обсуждаемых вопросов (обрабатываемой, хранимой и передаваемой информации) и условий расположения (эксплуатации) этих помещений и средств в охраняемых зонах относительно мест возможного перехвата.

Общие требования и решения по защите информации от несанкционированного доступа определяются на основании Руководящего документа Гостехкомиссии России [12.9], исходя из конкретных условий функционирования АС СФЗ и с учетом таких дополнительных признаков, как:

- категорийность охраняемой зоны физической защиты (защищенная, внутренняя, особо важная);
- особенности полномочий персонала СФЗ по отношению к защищаемым информационным ресурсам АС СФЗ при коллективной обработке данных, включая использование правила «двух (трех) лиц» при выполнении действий в особо важных и локальных высокоопасных зонах;

• режим обработки данных в АС СФЗ (автоматический, полуавтоматический).

При классификации систем транкинговой радиосвязи учитываются:

• уровень защищенности ресурсов этих систем (базовых станций, мобильных радиостанций, радиотелефонов), включая циркулирующую в системе информацию (речевую, цифровые информационные и управляющие данные) от НСД;

• уровень их защищенности от отказа или прерывания обслуживания абонентов;

• режим функционирования (автономный, комплексный – с выходом на другие системы связи, включая АТС, УАТС);

• средства и методы администрирования систем транкинговой радиосвязи.

Дифференциация подхода к установлению различных наборов требований по защите информации и выбору методов и средств защиты в зависимости от класса АС СФЗ и категории технических средств и систем определяется уровнем чувствительности ресурсов АС СФЗ по отношению к нарушению их безопасности, а также степенью опасности для людей и окружающей среды в случае осуществления несанкционированных действий с ЯМ и установками, возникающими из-за нарушений информационной безопасности АС СФЗ.

Мероприятия по комплексной защите информации разрабатываются и реализуются в соответствии с требованиями стандартов и иных государственных нормативных документов по защите информации.

Перечень необходимых средств и мер защиты информации определяется по результатам обследования проектируемой (модернизируемой) СФЗ в целом или ее отдельных составляющих. При этом следует учитывать, что стоимость реализации защиты информации

должна быть соизмерима с риском, который является приемлемым для конкретного ЯО.

Система физической защиты должна быть аттестована на соответствие требованиям безопасности информации с учетом обработки и передачи в ней сведений соответствующей степени секретности (конфиденциальности).

С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность технических средств, должен осуществляться контроль состояния и эффективности защиты информации.

Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

12.8. Требования по организации и проведению работ по защите информации в СФЗ ЯО

Проведение работ по защите информации должно проводиться на всех стадиях разработки и внедрения. Основные требования по их организации изложены в отраслевом руководящем документе [12.7].

Организация и проведение работ по защите информации, составляющей государственную и служебную тайну, на различных стадиях разработки и внедрения СФЗ, в том числе при ее обработке техническими средствами и от утечки по техническим каналам оп-

ределяется в целом действующими федеральными и отраслевыми нормативными документами.

Разработка СФЗ и ее подсистемы защиты информации может осуществляться как подразделениями ЯО, так и специализированными предприятиями, имеющими лицензию на соответствующий вид деятельности, в том числе в области защиты информации.

Право на обработку информации, составляющей государственную тайну, предоставляется только предприятиям, получившим лицензию Федеральной службы безопасности на право проведения работ со сведениями, составляющими государственную тайну, а на оказание услуг сторонним предприятиям по разработке подсистемы защиты информации или ее отдельных компонент — предприятиям, имеющим необходимые лицензии на право осуществления соответствующих видов деятельности в области защиты информации.

Научно-техническое руководство и непосредственную организацию работ по созданию подсистемы защиты информации осуществляет главный конструктор СФЗ или другое должностное лицо, обеспечивающее научно-техническое руководство всей разработкой СФЗ.

В случае разработки подсистемы защиты информации или ее отдельных компонентов специализированным предприятием, на ЯО определяются подразделения (или отдельные специалисты), ответственные за организацию и проведение (внедрение и эксплуатацию) мероприятий по защите информации в ходе выполнения работ с использованием сведений, составляющих государственную и служебную тайну.

Разработка и внедрение подсистемы защиты информации осуществляется во взаимодействии разработчика со службой безопасности ЯО, которая осуществляет на ЯО методическое руководство и участие в разработке конкретных требований по защите информации, аналитического обоснования необходимости создания под-

системы защиты информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации, участвует в согласовании технических заданий на проведение работ, в аттестации СФЗ.

Порядок организации на ЯО работ по созданию и эксплуатации СФЗ и ее подсистемы защиты информации должен предусматривать:

- определение подразделений, в том числе специализированных предприятий, участвующих в разработке и эксплуатации СФЗ и ее подсистемы защиты информации, их задачи и функции на различных стадиях создания и эксплуатации СФЗ;
- порядок взаимодействия в этой работе предприятий, подразделений и специалистов;
- определение должностных лиц, ответственных за своевременность и качество постановки требований по защите информации, за качество и научно-технический уровень разработки СФЗ.

Ответственность за обеспечение защиты информации об организации и функционировании СФЗ возлагается на руководителя ЯО.

На ЯО в дополнение к действующему «Перечню сведений, подлежащих засекречиванию по Минатому России» разрабатываются перечни сведений конфиденциального характера, раскрывающих особенности функционирования ЯО и его СФЗ, и соответствующая разрешительная система доступа персонала к такому роду информации.

Устанавливаются следующие стадии создания подсистемы защиты информации:

- предпроектная стадия, включающая обследование объекта, для которого создается СФЗ, разработку аналитического обоснова-

ния необходимости создания подсистемы защиты информации и технического (частного технического) задания на ее создание;

•стадия проектирования (разработки проектов) и реализации СФЗ, включающая разработку подсистемы защиты информации в составе СФЗ;

•стадия ввода в действие подсистемы защиты информации, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию СФЗ на соответствие требованиям безопасности информации.

На предпроектной стадии по обследованию объекта, для которого создается СФЗ:

•определяются (уточняются) угрозы ЯО в целом и информационной безопасности в частности;

•определяется модель вероятного нарушителя СФЗ применительно к конкретным условиям функционирования ЯО;

•устанавливается необходимость обработки (обсуждения) секретной (конфиденциальной) информации на различных пунктах управления и в различных компонентах СФЗ, оценивается ее степень секретности, уровень чувствительности, объемы, характер и условия использования;

•определяются конфигурация и топология СФЗ в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри СФЗ, так и с другими системами (например, системами учета и контроля ЯМ, технологической безопасности);

•определяются технические средства и системы, предполагаемые к использованию в разрабатываемой СФЗ, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;

•определяются режимы обработки информации в системе управления СФЗ в целом и в отдельных компонентах;

•определяется, какие данные и системы являются важными и должны дублироваться;

•определяется категория помещений пунктов управления СФЗ;

•определяется категория технических средств и систем;

•определяется класс защищенности АС;

•определяется класс защищенности систем транкинговой радиосвязи;

•определяется степень участия персонала в обработке (передаче, хранении, обсуждении) информации, характер их взаимодействия между собой и со службой безопасности ЯО;

•определяются мероприятия по защите информации в процессе разработки СФЗ;

•разрабатывается аналитическое обоснование необходимости создания подсистемы защиты информации по результатам предпроектного обследования;

•задаются конкретные требования по защите информации, включаемые в ТЗ на разработку подсистемы защиты информации на основе действующих федеральных и отраслевых нормативных документов по защите информации с учетом установленных категории помещений пунктов управления СФЗ, технических средств и систем, класса защищенности АС и систем транкинговой радиосвязи.

На стадии проектирования и реализации СФЗ и подсистемы защиты информации в ее составе на основе предъявляемых к системе требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

•разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) СФЗ в соответствии с требованиями ТЗ на разработку подсистемы защиты информации;

•разработка раздела технического проекта на СФЗ в части защиты информации;

•строительно-монтажные работы в соответствии с проектной документацией, утвержденной заказчиком, размещение и монтаж технических средств и систем;

•разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;

•закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации (либо их сертификация);

•проверка эффективности защиты помещений пунктов управления СФЗ и технических средств и систем в реальных условиях их размещения и эксплуатации с целью определения достаточности мер защиты с учетом установленной категории;

•закупка сертифицированных образцов и серийно выпускаемых технических и программных (в том числе криптографических) средств защиты информации и их установка;

•разработка (доработка) или закупка и последующая сертификация «по назначению» и по требованиям безопасности информации прикладных программных средств и программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;

•организация охраны и физической защиты пунктов управления СФЗ и других зон ограниченного доступа, исключающих несанкционированный доступ к техническим средствам обработки,

хранения и передачи информации, их хищение и нарушение работоспособности;

•разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала СФЗ к обрабатываемой информации;

•определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации СФЗ;

•выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

•разработка организационно-распорядительной и рабочей документации по эксплуатации СФЗ в защищенном исполнении, а также средств и мер защиты информации (приказов, инструкций и других документов);

•выполнение других мероприятий, специфичных для конкретных СФЗ и направлений защиты информации.

Задание на проектирование оформляется отдельным документом, согласовывается с проектной организацией, службой безопасности ЯО в части достаточности мер по технической защите информации и утверждается заказчиком.

На стадии проектирования и реализации СФЗ оформляются также технический проект и эксплуатационная документация подсистемы защиты информации, состоящие из:

•пояснительной записки с кратким изложением состава средств и мер защиты и принятых решений по техническим, программным, в том числе криптографическим, организационным средствам и мерам защиты информации с указанием их соответствия требованиям ТЗ;

•описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;

•плана организационно-технических мероприятий по подготовке СФЗ к внедрению средств и мер защиты информации;

•технического паспорта СФЗ (технических паспортов составляющих ее компонент, зон ограниченного доступа — помещений пунктов управления СФЗ, серверных, узлов связи и т.п.;

•инструкций и руководств по эксплуатации технических и программных средств защиты для пользователей, администратора системы, а также для работников службы безопасности ЯО.

На стадии ввода в действие СФЗ и подсистемы защиты информации в ее составе осуществляются:

•опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе СФЗ и отработки технологического процесса обработки (передачи) информации;

•приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком;

•аттестация СФЗ по требованиям безопасности информации.

При положительных результатах аттестации владельцу СФЗ выдается «Аттестат соответствия» требованиям безопасности информации.

Для СФЗ, находящихся в эксплуатации до введения в действие настоящего документа, может быть предусмотрен по решению их заказчика (владельца) упрощенный вариант их доработки (реконструкции), переоформления организационно-распорядительной, техно-рабочей и эксплуатационной документации.

Необходимым условием является их соответствие действующим требованиям по защите информации и их аттестация.

Аттестация СФЗ по требованиям безопасности информации осуществляется аккредитованными в установленном порядке органами по аттестации.

Эксплуатация СФЗ осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией.

Контроль состояния и эффективности защиты информации осуществляется службой безопасности ЯО, отраслевыми и федеральными органами контроля и заключается в оценке выполнения требований нормативных документов, в том числе настоящего документа, а также обоснованности принятых мер.

12.9. Требования и рекомендации по защите информации в СФЗ ЯО

Представляется целесообразным сформулировать основные требования и рекомендации по защите информации в СФЗ ЯО, представленной в различном виде (речь, побочные электромагнитные излучения, визуальное изображение), подвергающейся наиболее распространенной угрозе, связанной с попытками несанкционированного доступа, относящейся к определенным объектам СФЗ (например, к пунктам управления СФЗ и других жизненно важных объектов информатизации) или субъектам, эксплуатирующим СФЗ (персонал ЯО). Рассмотрим такие требования и рекомендации отдельно, как это сделано в отраслевом руководящем документе [12.7].

Требования и рекомендации по защите речевой информации

Требования настоящего раздела направлены на обеспечение защиты речевой информации, циркулирующей в помещениях пунктов управления СФЗ и передаваемой по телефонным линиям и радиоканалам связи.

Эффективность защиты речевой информации, составляющей государственную тайну, должна соответствовать действующим нормам безопасности информации в зависимости от установленной категории помещений пунктов управления СФЗ.

В помещениях пунктов управления СФЗ должны устанавливаться только системы телефонной связи, радиотрансляции, оповещения, сигнализации и электрочасофикации, сертифицированные по требованиям безопасности информации, либо должна быть проведена проверка эффективности защиты этих устройств в реальных условиях их размещения, по результатам которой определяется необходимость применения дополнительных мер их защиты.

Оконечные устройства этих систем, имеющие выход за пределы защищенной зоны ЯО, должны быть защищены от утечки информации за счет электроакустических преобразований.

Средства защиты также должны быть сертифицированы.

Звукоизоляционные характеристики ограждающих конструкций и технологического оборудования защищаемого помещения должны соответствовать установленным нормам акустической защиты речевой информации.

Необходимо исключить передачу по незащищенным каналам проводной и радиосвязи информации, составляющей государственную и служебную тайну.

Это осуществляется за счет жесткой регламентации характера и содержания передаваемых сообщений.

Такого рода информация должна передаваться только по защищенным каналам связи, либо с использованием средств криптографического преобразования информации или скремблирования передаваемой информации в соответствии с принятыми в России стандартами.

Требования и рекомендации по защите информации от утечки за счет побочных электромагнитных излучений и наводок

Требования настоящего раздела направлены на обеспечение защиты информации, обрабатываемой на используемых в СФЗ средствах вычислительной техники и циркулирующей в системах телевизионного наблюдения (СТН), от утечки за счет побочных электромагнитных излучений и наводок от этих средств на провода и линии, выходящие за пределы защищенной зоны ЯО, их линий передачи информации, а также по цепям электропитания.

Для обработки информации, составляющей государственную тайну, должны применяться СВТ и СТН, сертифицированные по требованиям безопасности информации, либо образцы техники, прошедшие проверку эффективности защиты информации в реальных условиях их размещения.

Для обработки информации, составляющей служебную тайну, могут использоваться СВТ и СТН, удовлетворяющие установленным требованиям по электромагнитной совместимости.

В качестве СТН рекомендуется использовать только системы внутреннего телевидения, устройства магнитной записи изображения (видеомагнитофоны), устройства просмотра телевизионных изображений (проекторы), входные и выходные сигналы которых удовлетворяют требованиям ГОСТ 784-92 «Система вещательного телевидения. Основные параметры. Методы измерений», ГОСТ 22006-76 «Установки телевизионные прикладного назначения. Основные параметры», ОСТ 4.205.003 «Телевидение черно-белое.

Импульсные сигналы на входе и выходе функциональных частей телевизионных аналоговых многокадровых систем специального назначения», в которых передача телевизионной информации производится по кабельным линиям связи без использования каналов радиосвязи.

Технические средства и кабельные сети, предназначенные для обработки и передачи информации, составляющей государственную и служебную тайну, должны размещаться в пределах защищенной зоны ЯО.

Размещение и монтаж технических средств, предназначенных для вывода защищаемой информации (печатающие устройства, видеотерминалы, графопостроители и т.п.), необходимо проводить с учетом максимального затруднения визуального просмотра информации посторонними лицами, а также принимать дополнительные меры, исключающие подобный просмотр (шторы на окнах, жалюзи, непрозрачные экраны и т.п.).

Передача изображений в СТН должна осуществляться на видеочастоте, без использования ультракоротковолновых (УКВ) генераторов.

Прокладку соединительных линий СТН необходимо выполнять экранированным, надлежащим образом заземленным кабелем, с учетом исключения возможности гальванического подключения к ним.

Если на объекте защиты не могут быть выполнены требования по обеспечению необходимого расстояния до границы защищенной зоны ЯО для отдельных средств техники или системы в целом, то должны быть применены следующие дополнительные меры защиты (по отдельности или в комплексе):

- доработка технического средства с целью обеспечения требуемого затухания на границе контролируемой зоны;

•пространственное зашумление технических средств с помощью систем активной защиты (САЗ).

Требования к дополнительным мерам определяются по результатам проверки эффективности защиты информации в реальных условиях их размещения.

В случае если в состав СТН включены устройства вычислительной техники, обрабатывающие информацию в цифровом виде, их защита должна осуществляться в соответствии с требованиями по защите информации, обрабатываемой СВТ.

Разделительный трансформатор (подстанция) и автономный источник электропитания, от которых питаются СВТ и СТН, обрабатывающие защищаемую информацию, линии электропитания, цепи и очаг заземления (место зануления) должны располагаться в пределах защищаемой зоны ЯО.

Требования и рекомендации по защите информации от несанкционированного доступа

В настоящем разделе устанавливаются принципы классификации автоматизированных систем управления и обеспечения физической защиты ядерно-опасных объектов на базе средств вычислительной техники, подлежащих защите от несанкционированного доступа и воздействий эксплуатационного персонала и посторонних лиц, в том числе от несанкционированных программных воздействий, нарушающих безопасность информационных ресурсов и работоспособность СВТ, а также общие требования по защите информации от НСД.

Автоматизированные системы, являющиеся неотъемлемой составной частью СФЗ ЯО и предназначенные для управления системой физической защиты и обеспечения ее функционирования, уязвимы с точки зрения несанкционированного доступа к информации

АС СФЗ и воздействия на нее, в результате чего может быть снижена эффективность функционирования СФЗ в целом или ее отдельных элементов.

Деление АС СФЗ на соответствующие классы по условиям их функционирования в СФЗ проводится в целях разработки и применения необходимых средств защиты информации АС СФЗ, а также обоснованных мер по достижению требуемого уровня безопасности ЯО в зависимости от категории используемого ядерного материала, изделий на его основе, мест проведения работ с ними, а также особенностей ядерных установок.

Дифференциация подхода к установлению различных наборов требований по безопасности информации и выбору методов и средств защиты в зависимости от класса АС СФЗ определяется уровнем чувствительности ресурсов АС СФЗ по отношению к нарушению их безопасности, а также степенью опасности для людей и окружающей среды в случае осуществления несанкционированных действий с ядерными материалами, изделиями на их основе и установками, возникающими из-за нарушений информационной безопасности АС СФЗ.

Классификация распространяется на все виды АС действующих, реконструируемых и проектируемых СФЗ ядерно-опасных объектов, независимо от их назначения, места АС в СФЗ, уровня интеграции различных систем, уровня управления СФЗ.

К АС СФЗ относятся системы на базе СВТ различного уровня интеграции: от автономных средств, использующих микропроцессорную технику и реализующих отдельные элементы подсистем СФЗ, автоматизированных систем, реализующих в целом функции отдельных подсистем СФЗ (локальные АС), до сложных многоуровневых АС СФЗ с коллективным доступом и наличием различного уровня полномочий субъектов доступа (пользователей, операторов) к информационным ресурсам АС СФЗ.

При классификации АС СФЗ и предъявлении соответствующих требований по защите информации от НСД должны быть учтены требования федеральных и отраслевых документов.

Все интегрированные АС СФЗ ЯО относятся к первой группе защищенности по РД Гостехкомиссии [12.8], включающей многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных степеней секретности (конфиденциальности), и не все пользователи имеют право доступа ко всей информации АС СФЗ. В соответствии с действующим перечнем сведений, подлежащих засекречиванию, они могут быть отнесены к классу защищенности не ниже «1В», поскольку максимальный уровень конфиденциальности информации, одновременно обрабатываемой и хранимой в таких АС — не ниже степени «секретно».

Локальные АС СФЗ определенного функционального назначения, а также автономные средства, использующие микропроцессорную технику и реализующие отдельные элементы подсистем СФЗ, в которых циркулирует информация, не составляющая государственную тайну, или имеющие иные режимы обработки информации (например, коллективный с равными правами), могут быть отнесены к другим классам защищенности по РД Гостехкомиссии России, начиная с класса «2Б» и выше, поскольку режим обработки данных в АС СФЗ может быть только коллективным.

Исходя из особенностей назначения и функционирования АС СФЗ, последние имеют дополнительные по отношению к указанному РД Гостехкомиссии России признаки, по которым должна производиться группировка АС СФЗ в различные классы.

Классификация АС СФЗ и соответствующие требования изложены в руководящем документе Минатома России [12.8]. Принципы классификации и характеристики отдельных классов АС СФЗ ЯО будут рассмотрены в отдельном разделе данной работы.

Требования и рекомендации по защите информации в СФЗ ЯО от фотографических и оптико-электронных средств разведки

При использовании маскируемого оборудования или его элементов в рубежах охраны СФЗ, скрытии принципов функционирования инженерно-технических средств системы должны быть обеспечены меры их защиты от фотографических и оптико-электронных средств разведки.

Эффективность принимаемых мер защиты должна соответствовать действующим нормативным документам по противодействию фотографическим и оптико-электронным средствам разведки.

Основными организационными и техническими мероприятиями по защите информации о СФЗ ЯО от фотографических и оптико-электронных средств разведки являются:

- использование маскирующих свойств местности;
- использование условий ограниченной видимости;
- применение ложных сооружений и маскировочных конструкций;
- пространственные ограничения, направленные на исключение «контакта» между средствами разведки и защищаемым объектом.

Эти мероприятия используются на различных этапах жизненного цикла СФЗ ЯО.

Требования и рекомендации по физической защите пунктов управления СФЗ ЯО и других жизненно важных объектов информатизации

В целях обеспечения комплексной безопасности информации в СФЗ физической защите подлежат жизненно важные объекты информатизации СФЗ:

- центральный пункт управления (ЦПУ) СФЗ;
- локальные пункты управления (ЛПУ) СФЗ;
- помещения, в которых установлены серверы баз данных и коммуникационные серверы («серверные») – в случае, когда они устанавливаются в отдельном помещении;
- помещения, в которых хранятся носители информации («хранилища»);
- узлы связи;
- оконечные терминальные устройства и автономные средства, использующие микропроцессорную технику и реализующие отдельные элементы подсистем СФЗ;
- коммуникации СФЗ;
- системы электропитания (трансформаторные подстанции, автономные источники);
- системы управления СФЗ мобильных ЯО.

Помещения ЦПУ и его «серверной» должны размещаться в специально приспособленных для этого зонах ограниченного доступа, находящихся в пределах одной из внутренних или особо важных зон.

Вход и выход из этих помещений должен регулироваться автоматизированной системой контроля и управления доступом.

При круглосуточном характере работы сменного персонала

ЦПУ помещение ЦПУ не требует иных технических средств охраны и должно находиться на режиме самоохраны.

Доступ в эти помещения должен быть ограничен и строго дифференцирован по выполняемым функциям персонала.

Обслуживание ЦПУ и его «серверной» обеспечивается персоналом службы безопасности ЯО совместно с выделенными для этих целей специалистами подразделений, обеспечивающих бесперебойное функционирование средств вычислительной техники, связи, электропитания, кондиционирования и т.п.

Помещение «серверной», не требующее постоянного присутствия обслуживающего персонала, в дополнение к оконечным устройствам системы контроля и управления доступом, оборудуется техническими средствами охраны в соответствии с высшей категорией охраняемых ЯО и высшей степенью секретности обрабатываемой и хранимой информации, но не менее чем двумя рубежами охранной сигнализации с разными физическими принципами действия. При размещении серверов совместно с другим оборудованием непосредственно в помещении ЦПУ и при круглосуточном режиме работы сменного персонала ЦПУ к их физической защите не предъявляется дополнительных требований.

Информация баз данных СФЗ должна дублироваться, и одна из копий должна быть помещена в хранилище носителей информации, обслуживающее ЦПУ.

Для ЦПУ может быть предусмотрено резервирование.

Помещения ЛПУ различного функционального назначения и их «серверных» должны размещаться в специально приспособленных для этого зонах ограниченного доступа, находящихся в пределах защищенной или одной из внутренних зон в зависимости от «зоны обслуживания» или функционального назначения локальной АС.

Вход и выход из этих помещений должен регулироваться автоматизированной системой контроля и управления доступом.

При круглосуточном характере работы сменного персонала ЛПУ помещение ЛПУ не требует иных технических средств охраны и должно находиться на режиме самоохраны.

Доступ в эти помещения должен быть ограничен и строго дифференцирован по выполняемым функциям персонала.

Обслуживание ЛПУ и его «серверной» обеспечивается персоналом охраны или службы безопасности ЯО, назначаемым для каждой конкретной «зоны обслуживания» совместно с выделенными для этих целей специалистами подразделений, обеспечивающих бесперебойное функционирование средств вычислительной техники, связи, электропитания, кондиционирования и т.п.

Помещение «серверной», не требующее постоянного присутствия обслуживающего персонала, в дополнение к оконечным устройствам системы контроля и управления доступом оборудуется техническими средствами охраны в соответствии с высшей степенью секретности обрабатываемой и хранимой информации или высшей категорией охраняемых ЯО (в зависимости от функционального назначения и «зоны обслуживания»), но не менее чем двумя рубежами охранной сигнализации с разными физическими принципами действия. При размещении серверов совместно с другим оборудованием непосредственно в помещении ЛПУ и при круглосуточном режиме работы сменного персонала ЛПУ к их физической защите не предъявляется дополнительных требований.

Информация баз данных СФЗ должна дублироваться, и одна из копий должна быть помещена в хранилище носителей информации, обслуживающее соответствующий ЛПУ.

Хранилища носителей информации должны размещаться в специально приспособленных для этого зонах ограниченного доступа, находящихся в пределах той же охраняемой зоны, что и пункт управления СФЗ. Они должны быть оборудованы техническими средствами охраны в соответствии с высшей степенью сек-

ретности хранимых в них информационных носителей и сдаваться под охрану в нерабочее время.

Узлы связи (коммутаторы оперативной связи или АТС малой емкости) сети телефонной и радиосвязи СФЗ, распределительное и коммуникационное оборудование должны размещаться в пределах защищенной зоны в зонах ограниченного доступа, оборудованных автономными средствами или оконечными терминальными устройствами подсистемы контроля и управления доступом, или быть защищены от несанкционированного вскрытия техническими средствами охраны.

Оконечные терминальные устройства и автономные средства, использующие микропроцессорную технику, выполняющие определенные функции или реализующие отдельные элементы подсистем СФЗ, в частности, исполнительные механизмы подсистемы контроля и управления доступом в охраняемые зоны, должны быть защищены от хищения и подмены или задублированы элементами других подсистем СФЗ, например телекамерами подсистемы телевизионного наблюдения.

Коммуникации СФЗ (информационные кабели, кабельные колодцы и распределительные шкафы) должны прокладываться и выполняться в защищенном исполнении, в том числе с использованием сигнализации на вскрытие.

Электрические установки и кабели, предназначенные для электропитания технических средств СФЗ (включая трансформаторные подстанции, автономные источники, устройства защиты), должны размещаться в пределах защищенной зоны, в том числе источники электропитания — в зонах ограниченного доступа, оборудованных автономными средствами или оконечными терминальными устройствами подсистемы контроля и управления доступом.

Требования к персоналу

Эксплуатационный персонал СФЗ (руководители и операторы пунктов управления, администраторы АС, специалисты подразделений, обеспечивающих бесперебойное функционирование средств вычислительной техники, связи, электропитания, кондиционирования и тому подобное) должен иметь форму допуска, соответствующую сведениям, к которым этот персонал может иметь доступ в процессе выполнения производственных обязанностей, а также быть специально подготовленным для выполнения этих обязанностей.

Руководителями и операторами ЦПУ и локальных пунктов управления, в зону обслуживания которых входят особо важные и локальные высокоопасные зоны, должны быть штатные сотрудники службы безопасности ЯО. Администраторами АС СФЗ в целом, их баз данных и безопасности могут быть как штатные сотрудники службы безопасности, так и других подразделений ЯО, оформленные установленным порядком.

Руководителями и операторами локальных пунктов управления, в зону обслуживания которых входит только защищенная зона и (или) внешние периметры внутренних зон ЯО, могут быть штатные сотрудники подразделений охраны (военнослужащие МВД или штатные сотрудники ведомственной охраны ЯО). Администраторами этих ЛВС, их баз данных и безопасности могут быть как военнослужащие и штатные сотрудники ведомственной охраны, так и сотрудники других подразделений ЯО, оформленные установленным порядком.

Все эти категории специалистов, а также специалисты подразделений, обеспечивающих бесперебойное функционирование средств вычислительной техники, связи и электропитания должны знать требования по защите информации, необходимые им в про-

цессе эксплуатации СФЗ и ее подсистемы защиты информации, и применять их на практике.

12.10. Классификация автоматизированных систем СФЗ ЯО с точки зрения безопасности информации

При разработке, создании и эксплуатации АС СФЗ ЯО, реализующей требования по защите информации, а также для органов контроля за состоянием СФЗ и ее подсистемы ЗИ необходимо учитывать существующие требования по классификации АС. Эти требования сформулированы в РД [12.8], который устанавливает классификацию автоматизированных систем управления и обеспечения физической защиты ядерно-опасных объектов на базе средств вычислительной техники, подлежащих защите от несанкционированного доступа и воздействий эксплуатационного персонала и посторонних лиц, в том числе от несанкционированных программных воздействий, нарушающих безопасность информационных ресурсов и работоспособность СВТ. К каждому из классов ставится в соответствие совокупность требований по безопасности информации.

Рассматриваемый РД был разработан на основании требований РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», а также с учетом «Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов», «Концепции информационной безопасности СФЗ ЯОО» и РД Минатома России «Общие требования по защите информации в СФЗ ЯОО».

Данный РД может использоваться в качестве нормативного документа, на соответствие требованиям которого в системе сертификации № РОСС RU. 0001.01БИ00 производится сертификация

программных и программно-технических средств защиты информации от НСД, предназначенных к использованию в СФЗ, а также аттестация СФЗ по требованиям безопасности информации.

Общие принципы классификации

Классификация распространяется на все виды АС действующих, реконструируемых и проектируемых СФЗ ядерно-опасных объектов, независимо от их назначения, места АС в СФЗ, уровня интеграции различных систем, уровня управления СФЗ.

Автоматизированная система СФЗ может представлять собою как интегрированную АС, объединяющую всю информацию о состоянии физической защиты конкретного ядерно-опасного объекта, так и совокупность автономных средств и локальных АС определенного функционального назначения (обнаружения, наблюдения, управления доступом, связи), в которых циркулирует информация, необходимая для принятия решений по ряду аспектов состояния физической защиты ядерных материалов, изделий на их основе и установок.

Технической базой АС может быть как вычислительная сеть, так и терминальные комплексы, автономные ЭВМ (ПЭВМ) и специализированные микропроцессорные системы.

Характерными свойствами функционирования АС СФЗ являются:

- территориальное размещение АС СФЗ в различных охраняемых зонах (защищаемой – ЗЗ, внутренней – ВЗ, особо важной – ОВЗ и в зонах ограниченного доступа (ЗОД) ядерного объекта), доступ в которые имеет ограниченный и строго дифференцированный персонал;
- персонал АС СФЗ может не иметь права доступа в обслуживаемую им охраняемую зону;

•наличие информации, составляющей государственную и служебную тайну, раскрывающей систему физической защиты конкретного ЯО, а также чувствительной по отношению к несанкционированным воздействиям на нее, в результате чего может быть снижена эффективность функционирования СФЗ в целом или ее отдельных элементов;

•обработка информации, поступающей от специализированных средств, устройств и исполнительных механизмов (датчиков, телекамер, радиационных мониторов, элементов задержки и т.п.) в реальном масштабе времени, повышенные требования к времени реакции и надежностным характеристикам АС СФЗ;

•относительное постоянство используемых штатных программных средств, включенных в регламент работы АС СФЗ, и узкая функциональная специализация АС СФЗ в отличие от АС общего назначения;

•возможность использования режима автоматического выполнения прикладных программ СФЗ без участия оператора;

•строгое разделение функциональных обязанностей, распределение полномочий и прав на выполнение регламентных действий между эксплуатационным персоналом АС СФЗ;

•возможность интеграции с автоматизированными системами учета и контроля ядерных материалов, технологической безопасности;

•наличие служебной информации системы защиты информации АС СФЗ от НСД (паролей, ключей, таблиц санкционирования и т.п.), требующее обеспечения ее конфиденциальности.

Основными этапами классификации АС СФЗ являются:

•сбор и анализ исходных данных;

•выявление основных признаков АС СФЗ, необходимых для классификации;

•сравнение выявленных признаков АС СФЗ с классифицируемыми;

•присвоение АС СФЗ соответствующего класса защищенности информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС СФЗ, с точки зрения безопасности информации, являются:

•перечень защищаемых ресурсов АС СФЗ и их уровень чувствительности по отношению к нарушению их безопасности, т.е. степень негативного влияния на функционирование СФЗ несанкционированных воздействий по отношению к этим ресурсам (по использованию этой информации нарушителем при преодолении охраняемых зон, по модификации и уничтожению информации или отказу/блокированию АС);

•категорийность охраняемой зоны физической защиты (защищенная, внутренняя, особо важная, локальная высоко опасная);

•категории персонала СФЗ, имеющего доступ к штатным средствам АС СФЗ, с указанием уровня полномочий;

•матрица доступа или полномочий субъектов доступа по отношению к защищаемым ресурсам АС СФЗ при коллективной обработке данных в СФЗ, включая использование правила «двух (трех) лиц» при выполнении действий в особо важных и локальных высокоопасных зонах;

•режим обработки данных в АС СФЗ (автоматический, полуавтоматический).

Установление класса защищенности АС СФЗ производится заказчиком и разработчиком с привлечением специалистов по защите информации.

С учетом особенностей АС СФЗ ЯО к числу определяющих признаков, по которым производится группировка АС СФЗ в различные классы, относятся:

- наличие в АС СФЗ ресурсов различного уровня чувствительности;
- уровень полномочий субъектов доступа по отношению к защищаемым ресурсам АС СФЗ при коллективной обработке данных в СФЗ, включая использование правила «двух и более лиц» при выполнении действий в особо важных и локальных высокоопасных зонах;
- категория обслуживаемой зоны (зон) физической защиты;
- режим обработки данных в АС СФЗ (автоматический, полуавтоматический).

Различаются четыре уровня чувствительности ресурсов АС СФЗ по отношению к несанкционированному доступу и воздействиям:

4-й – раскрытие, уничтожение (искажение) информации или блокировка работы АС СФЗ могут создать условия для несанкционированного проникновения внешнего нарушителя в защищенную зону (ЗЗ) или несанкционированных действий внутреннего нарушителя в этой зоне;

3-й – раскрытие, уничтожение (искажение) информации или блокировка работы АС СФЗ могут создать условия для несанкционированного проникновения внешнего нарушителя во внутреннюю зону (ВЗ) или несанкционированных действий внутреннего нарушителя в этой зоне;

2-й – раскрытие, уничтожение (искажение) информации или блокировка работы АС СФЗ могут создать условия для несанкционированного проникновения внешнего нарушителя в особо важную зону (ОВЗ) или несанкционированных действий внутреннего нарушителя в этой зоне;

1-й – раскрытие, уничтожение (искажение) информации или блокировка работы АС СФЗ могут создать условия для несанкционированного проникновения внешнего нарушителя в локальную высокоопасную зону (ЛВОЗ) или несанкционированных действий внутреннего нарушителя в этой зоне.

Различаются два основных режима обработки данных в АС СФЗ. Они характеризуются степенью автоматизма при выполнении прикладных программ СФЗ, а также использованием фиксированной или изменяемой программной среды, условием постоянного резидентного размещения штатных ресурсов:

а) автоматический (специализированный, замкнутый), характеризующийся строго фиксированной программной средой, непосредственно относящейся к управлению оборудованием СФЗ, когда штатные ресурсы являются постоянными резидентами АС СФЗ и в системе может выполняться только строго заданный перечень программ и процессов, а программные процессы инициализируются (запускаются) автоматически без участия оператора;

б) полуавтоматический (общий), характеризующийся фиксированной программной средой, непосредственно относящейся к управлению оборудованием СФЗ, но штатные ресурсы не являются постоянными резидентами АС, а программные процессы инициализируются (запускаются) как автоматически, так и по командам оператора.

Устанавливаются восемь классов защищенности информации АС СФЗ по отношению к несанкционированному доступу и воздействиям. Каждый класс характеризуется определенной минимальной совокупностью требований по обеспечению безопасности информации. Классы подразделяются на четыре группы, отличающиеся уровнем чувствительности используемых в АС СФЗ ресурсов, связанных с информацией о физической защите соответствующей зоны. Каждая группа характеризуется определенной минимальной совокупностью требований по обеспечению безопасно-

сти информации. Каждая группа состоит из двух классов, отличающихся по режиму обработки данных (автоматический – [А], полуавтоматический – [П]). В пределах каждой группы соблюдается иерархия требований по обеспечению безопасности информации в зависимости от режима ее обработки и, следовательно, иерархия классов защищенности АС СФЗ от несанкционированного доступа и воздействий.

Минимальные требования по обеспечению безопасности информации предъявляются к 4-й группе, максимальные – к 1-й группе, при этом внутри группы более высокие требования предъявляются к полуавтоматическому режиму обработки данных.

Четвертая группа включает АС СФЗ, в которых используются ресурсы, раскрытие, модификация, уничтожение или блокировка доступа к которым могут создать условия для проникновения и (или) действий в ЗЗ. Группа содержит два класса – 4А, 4П. Класс 4А относится к автоматическому (специализированному) режиму обработки данных, класс 4П – к полуавтоматическому (общему) режиму обработки.

Третья группа включает АС СФЗ, в которых используются ресурсы, раскрытие, модификация, уничтожение или блокировка доступа к которым могут создать условия для проникновения и (или) действий во ВЗ. Группа содержит два класса – 3А, 3П. Класс 3А относится к автоматическому (специализированному) режиму обработки данных, класс 3П – к полуавтоматическому (общему) режиму обработки.

Вторая группа включает АС СФЗ, в которых используются ресурсы, раскрытие, модификация, уничтожение или блокировка доступа к которым могут создать условия для проникновения и (или) действий в ОВЗ. Группа содержит два класса – 2А, 2П. Класс 2А относится к автоматическому (специализированному) режиму обработки данных, класс 2П – к полуавтоматическому (общему) режиму обработки.

Первая группа включает АС СФЗ, в которых используются ресурсы, раскрытие, модификация, уничтожение или блокировка доступа к которым могут создать условия для проникновения и (или) действий в ЛВОЗ. Группа содержит два класса – 1А, 1П. Класс 1А относится к автоматическому (специализированному) режиму обработки данных, класс 1П – к полуавтоматическому (общему) режиму обработки.

Общие требования, учитываемые при классификации

Обеспечение безопасности информации в АС СФЗ от несанкционированного доступа и воздействий является составной частью общей проблемы информационной безопасности и обеспечения физической защиты ЯО. Мероприятия по защите ресурсов АС СФЗ от НСД должны осуществляться взаимосвязано с организационными и техническими мероприятиями по защите информации и физической защите ядерных материалов и установок.

В общем случае, комплекс программно-технических средств и организационных решений по защите чувствительных ресурсов АС СФЗ от НСД реализуется в рамках системы защиты информации от НСД, состоящей из четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности.

В зависимости от класса защищенности АС СФЗ в рамках этих подсистем должны быть реализованы требования в соответствии с приведенной ниже табл. 12.1 со следующими обозначениями:

« - »– нет требований к данному классу;

« + » – есть требования к данному классу;

« = » – требования совпадают с требованиями предшествующего класса.

Таблица 12.1. Классы защищенности АС СФЗ

№ п/п	Подсистемы и требования	ГРУППЫ / КЛАССЫ							
		4		3		2		1	
		4А	4П	3А	3П	2А	2П	1А	1П
1	**ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ**								
1.1	***Проверка подлинности (аутентификация)***								
	Персонала	+	=	+	=	+	=	+	=
	Системы	-	-	-	+	=	=	=	=
	Программ/процессов	-	+	=	+	=	+	=	=
	Рабочих станций/терминалов/узлов	+	=	+	=	=	+	=	=
	Внешних устройств	+	=	=	=	+	=	+	=
1.2	***Контроль доступа субъектов***								
	К загрузке/останову системы	+	=	+	=	+	=	+	=
	К системе	+	=	+	=	+	=	+	=
	К программам/командам	-	+	=	+	=	+	=	=
	К томам/каталогам/файлам/записям	-	+	=	+	=	+	=	+
	К рабочим станциям/терминалам/ узлам сети	-	-	+	=	=	+	=	=
	К внешним устройствам	-	+	=	+	+	=	+	=
1.3	***Управление потоками по уровню конфиденциальности информации***								
	Разделение накопителей	-	-	+	=	+	=	=	=
	Разделение файлов	-	-	+	=	=	=	=	=
	Разделение пакетов данных	-	-	+	=	+	=	=	=
2	**ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЁТА**								
2.1	***Регистрация и учёт***								
	Загрузки/останова системы/ рабочих станций/терминалов	+	=	=	=	=	=	=	=
	Доступа персонала к системе	+	=	=	=	=	=	+	=
	Доступа персонала к рабочим станциям/терминалам/узлам сети	-	-	+	=	=	+	=	=
	Завершения сеанса работы/выхода из системы	-	-	+	=	=	=	=	=
	Доступа к программам/командам	-	+	=	+	=	+	=	=

Окончание табл.12.1

№ п/п	Подсистемы и требования	ГРУППЫ / КЛАССЫ							
		4		3		2		1	
		4А	4П	3А	3П	2А	2П	1А	1П
	Доступа к томам/ каталогам/ файлам/записям	-	+	=	+	=	+	=	+
	Доступа к внешним устройствам	-	+	=	+	+	=	+	=
	Изменения параметров (конфигурации) системы/ полномочий субъектов доступа	-	+	+	=	+	=	+	=
2.2	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ПЭВМ и внешних накопителей	-	-	-	+	=	=	=	=
2.3	Учёт носителей информации	+	=	+	=	=	=	+	=
2.4	Сигнализация попыток нарушения защиты	-	-	+	=	+	=	+	=
3	КРИПТОГРАФИЧЕСКАЯ ПОДСИСТЕМА								
3.1	Шифрование служебной информации СЗИ НСД	-	-	-	-	+	=	+	=
3.2	Шифрование чувствительных данных	-	-	-	-	+	=	+	=
3.3	Использование сертифицированных криптографических средств	-	-	-	-	+	=	=	=
4	ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ								
4.1	Обеспечение целостности программно-аппаратных средств и циркулирующей информации	+	=	+	=	+	=	+	=
4.2	Наличие администратора	+	=	+	=	+	=	+	=
4.3	Резервирование	-	-	+	=	+	=	+	=
4.4	Восстановление	+	=	+	=	+	=	+	=
4.5	Тестирование	+	=	+	=	+	=	+	=
4.6	Физическая защита оборудования системы и носителей данных	+	=	+	=	+	=	+	=
4.7	Использование сертифицированных СЗИ НСД	+	=	=	=	=	=	=	=

Требования к четвертой группе

При этом указанные требования к локальным АС СФЗ, отнесенным к 4-й группе защищенности, предъявляются только в случае отсутствия в этой АС информации, составляющей государственную тайну. В противном случае к таким АС СФЗ должны быть применены требования, предъявляемые к 3-й группе защищенности.

Требования к автономным средствам, использующим микропроцессорную технику и реализующим отдельные элементы подсистем СФЗ, определяются отдельно.

Класс «4А». Подсистема управления доступом. Должна проводиться проверка подлинности и контроль доступа в систему операторов (администраторов) по их идентификаторам (имени, номеру) и паролям условно-постоянного действия длиной не менее 6 алфавитно-цифровых символов. Все операторы и администраторы должны иметь уникальные идентификаторы и пароли. Должен проводится контроль доступа администратора к программной загрузке и останову системы по паролю и списку доступа. Доступ к загрузке и останову системы должен иметь только администратор (администраторы) системы. Должна проводиться проверка подлинности (аутентификация) терминалов и внешних устройств системы по их логическим (физическим) адресам во время загрузки системы.

Класс «4А». Подсистема регистрации и учета. Должна осуществляться регистрация загрузки/останова системы, рабочих станций, терминалов. В параметрах регистрации указываются:

- время и дата загрузки/останова (shutdown) системы, рабочих станций, терминалов;
- идентификатор оператора (администратора);

•результат попытки загрузки/останова: успешный или неуспешный – несанкционированный, причина неуспешной попытки (неправильный идентификатор, пароль и т.п.

Должна осуществляться регистрация входа субъектов доступа (операторов, администратора) в систему. В параметрах регистрации указываются:

•время и дата входа субъекта доступа в систему;

•идентификатор субъекта доступа;

•результат попытки входа: успешный или неуспешный – несанкционированный, причина неуспешной попытки (неправильные идентификатор, пароль, время доступа и тому подобное).

Должен проводиться учет всех носителей информации с помощью их маркировки, учет носителей должен проводиться в журнале с регистрацией их выдачи/приема.

Класс «4А». ***Подсистема обеспечения целостности.*** Должен проводиться контроль целостности СЗИ НСД при загрузке системы с помощью проверки наличия имен программ (файлов) и данных СЗИ НСД.

В системе должны:

•присутствовать администратор, ответственный за ведение СЗИ НСД, загрузку и останов системы, ее восстановление и тестирование;

•иметься средства восстановления СЗИ НСД;

•быть регламентированы средства и порядок тестирования СЗИ НСД;

•осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС СФЗ посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище (помещение, шкаф, сейф) носителей информации;

•использоваться сертифицированные СЗИ НСД.

Класс «4П». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «4А». Дополнительно СЗИ НСД должна обеспечивать:

1. Проверку подлинности программ по эталонному размеру соответствующих файлов во время загрузки системы.
2. Контроль доступа персонала к программам, командам по таблицам санкционирования.
3. Контроль доступа персонала к томам, каталогам по таблицам санкционирования.
4. Контроль доступа персонала к внешним устройствам системы по таблицам санкционирования.

Класс «4П». Подсистема регистрации и учета. Требования совпадают с аналогичными требованиями класса «4А». Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию доступа персонала к программам и командам системы. В параметрах регистрации указываются:

•время и дата попытки доступа;

•идентификатор оператора;

•спецификация (имя) программы, команды;

•результат попытки: успешный или неуспешный – несанкционированный.

2. Регистрацию доступа персонала к томам, каталогам. В параметрах регистрации указываются:

•время и дата попытки доступа;

•идентификатор оператора;

•спецификация (имя) тома, каталога;

•вид запрошенной операции (чтение, запись, удаление);

•результат попытки: успешный или неуспешный – несанкционированный.

3. Регистрацию включения/отключения внешних устройств системы. В параметрах регистрации указываются:

- время и дата включения/выключения устройства;
- идентификатор (адрес, имя) устройства;
- идентификатор оператора;
- результат попытки: успешный или неуспешный – несанкционированный.

4. Регистрацию изменения конфигурации и параметров системы. В параметрах регистрации указываются:

- время и дата внесения изменения;
- идентификатор оператора;
- тип и вид проведенного изменения.

Класс «4П». Подсистема обеспечения целостности. Требования совпадают с аналогичными требованиями класса «4А».

Требования к третьей группе

Класс «3А». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «4П». Дополнительно СЗИ НСД должна обеспечивать:

1. Проверку подлинности и контроль доступа в систему и доступа к загрузке/останову системы операторов (администраторов) по их идентификаторам (имени, номеру) и паролям временного действия (не более 3-х месяцев) длиной не менее 6 алфавитно-цифровых символов.

2. Проверку подлинности рабочих станций, терминалов, узлов по их логическим (физическим) адресам.

3. Контроль доступа операторов (администраторов) к рабочим станциям, терминалам, узлам сети по спискам доступа с учетом заданных привилегий.

4. Разделение (изолирование) ресурсов (накопителей и файлов), содержащих конфиденциальную информацию, от других ресурсов.

5. Разделение (изолирование) маршрутов/протоколов (логических, физических каналов) передачи по сети пакетов данных, содержащих конфиденциальную информацию, от маршрутов/протоколов других данных в целях защиты от активного/пассивного прослушивания сети.

Класс «3А». ***Подсистема регистрации и учета.*** Данные требования совпадают с аналогичными требованиями класса «4П». Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию доступа персонала к рабочим станциям, терминалам, узлам сети. В параметрах регистрации указываются:

- время и дата попытки доступа;
- идентификатор оператора (администратора);
- спецификация (имя, адрес) рабочей станции, терминала, узла сети;
- результат попытки: успешный или неуспешный – несанкционированный.

2. Регистрацию завершения сеанса работы/выхода из системы. В параметрах регистрации указываются:

- время и дата завершения работы;
- идентификатор оператора (администратора);
- спецификация (имя, адрес) рабочей станции, терминала, узла сети.

3. Регистрацию изменения полномочий персонала на доступ в систему. В параметрах регистрации указываются:

- время и дата внесения изменения;
- идентификатор администратора;
- идентификатор персонала, у которого изменены полномочия;

•вид изменения (внесение, исключение из списка доступа, изменение пароля и т.п.).

Должен проводиться учет всех носителей информации (томов) с помощью их защищенной маркировки, учет носителей должен проводиться в журнале с регистрацией их выдачи/приема.

Должна проводится сигнализация (оперативное отображение) попыток несанкционированного доступа в систему на рабочей станции (терминале) администратора системы. Данные сигнализации должны включать:

•идентификатор (имя, адрес) рабочей станции (терминала), с которой осуществлена несанкционированная попытка доступа в систему;

•идентификатор, заданный при такой попытке;

•причину отклонения доступа в систему (неправильный идентификатор, пароль, время входа и т.п.).

Класс «3А». Подсистема обеспечения целостности. Должен проводиться контроль целостности СЗИ НСД при загрузке системы по эталонным контрольным суммам всех файлов и данных СЗИ НСД. Должны резервироваться наиболее критичные ресурсы системы, связанные с управлением доступом.

В системе должно быть выделено отдельное рабочее место администратора (рабочая станция, терминал), с которого проводится ведение СЗИ НСД, загрузка и останов системы, ее восстановление и тестирование.

В системе должны иметься программные средства оперативного восстановления СЗИ НСД с резервных (архивных) носителей.

В системе должны использоваться программные средства тестирования СЗИ НСД.

Должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС СФЗ, с помощью

технических средств охраны и специального персонала, строгий пропускной режим, специальное оборудование помещений АС СФЗ, включающее использование автоматизированной системы контроля и управления доступом в помещения, либо автономных устройств.

Класс «3П». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «3А». Дополнительно СЗИ НСД должна обеспечивать:

1. Проверку подлинности системы по ее сообщениям. Должны быть установлены процедуры передачи системы между сменами, гарантирующие ее подлинность и целостность.

2. Проверку подлинности программ по эталонному размеру соответствующих файлов во время загрузки системы и перед каждым их запуском.

3. Контроль доступа персонала к программам, командам по таблицам санкционирования с учетом режима их выполнения (опций программ).

4. Контроль доступа персонала к файлам, записям по таблицам санкционирования.

5. Контроль доступа персонала к командам внешних устройств системы по таблицам санкционирования.

Класс «3П». Подсистема регистрации и учета. Требования совпадают с аналогичными требованиями класса «3А». Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию доступа персонала к режимам работы программ и команд системы. В параметрах регистрации указываются:

- время и дата попытки доступа;
- идентификатор оператора;
- спецификация (имя) запрошенной программы, команды;
- вид запрошенного режима программы, команды;

•результат попытки: успешный или неуспешный – несанкционированный.

2. Регистрацию доступа персонала к файлам, записям. В параметрах регистрации указываются:

•время и дата попытки доступа;

•идентификатор оператора;

•спецификация (имя) файла, записи;

•вид запрошенной операции (чтение, запись, удаление);

•результат попытки: успешный или неуспешный – несанкционированный.

3. Регистрацию доступа к командам внешних устройств системы. В параметрах регистрации указываются:

•время и дата попытки выдачи команды устройства;

•идентификатор (адрес, имя) устройства;

•идентификатор оператора;

•вид запрошенной команды,

•результат попытки: успешный или неуспешный – несанкционированный.

Должна проводиться очистка (обнуление, обезличивание, инициализация) освобождаемых областей оперативной памяти и внешних накопителей ПЭВМ. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Класс «3П». Подсистема обеспечения целостности. Требования совпадают с аналогичными требованиями класса «3А».

Требования ко второй группе

Класс «2А». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «3П». Дополнительно СЗИ НСД должна обеспечивать:

1. Проверку подлинности и контроль доступа в систему и доступа к загрузке/останову системы операторов (администраторов) по их идентификаторам (имени, номеру) и паролям кратковременного действия (не более 1-го месяца) длиной не менее 8 алфавитно-цифровых символов. Администратор не должен иметь доступ к паролям операторов. В системе должны использоваться программные средства для смены паролей самими операторами с соответствующей проверкой их уникальности и длины.

2. Проверку подлинности (аутентификацию) внешних устройств системы по их логическим (физическим) адресам при каждом доступе к устройству.

3. Контроль доступа операторов к командам управления внешними устройствами (подсистемы управления доступом СФЗ) по принципу «в две руки» по паролям и таблицам санкционирования. Одним из операторов должен быть администратор.

4. Разделение (изолирование) накопителей, содержащих конфиденциальную информацию по их уровню конфиденциальности (грифу секретности).

5. Разделение (изолирование) маршрутов/протоколов (логических, физических каналов) передачи по сети пакетов данных, содержащих конфиденциальную информацию, по их уровню конфиденциальности (грифу секретности) в целях защиты от активного/пассивного прослушивания сети.

Класс «2А». Подсистема регистрации и учета. Требования совпадают с аналогичными требованиями класса «3П». Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию доступа «в две руки» к командам управления внешними устройствами системы. В параметрах регистрации указываются:

- время и дата попытки выдачи команды устройства;
- идентификатор (адрес, имя) устройства;
- идентификаторы (имена) операторов-участников;
- вид запрошенной команды;
- результат попытки: успешный или неуспешный – несанкционированный.

2. Регистрацию изменения полномочий персонала на доступ к ресурсам системы. В параметрах регистрации указываются:

- время и дата внесения изменения;
- идентификатор администратора;
- идентификатор персонала, у которого изменены полномочия,
- вид (тип) ресурса – объекта доступа,
- вид изменения (тип доступа, добавление, исключение и тому подобное).

Должна проводиться сигнализация (оперативное отображение) попыток несанкционированного доступа к ресурсам системы (внешним устройствам, томам, каталогам, файлам, программам) на рабочей станции (терминале) администратора системы. Данные сигнализации должны включать:

- идентификатор (имя, адрес) рабочей станции (терминала), с которой осуществлена несанкционированная попытка доступа к ресурсу;
- идентификатор оператора;
- идентификатор (имя) ресурса;
- вид запрошенной операции с ресурсом;

•причину отклонения доступа к ресурсу (нет привилегий, недостаточно привилегий и т.п.).

Класс «2А». ***Криптографическая подсистема.*** Должно осуществляться шифрование (преобразование) служебной информации СЗИ НСД (идентификаторов, паролей, таблиц санкционирования) при их записи на накопители, исключающее их прямое чтение (восстановление). Должно осуществляться шифрование (преобразование) чувствительных данных системы при их записи на накопители. Должны использоваться сертифицированные криптографические средства.

Класс «2А». ***Подсистема обеспечения целостности.*** Должен проводиться контроль целостности СЗИ НСД, программ и чувствительных данных системы при загрузке системы и по командам по эталонным контрольным суммам длиной не менее 8 байт. Должны резервироваться в «горячем режиме» наиболее критичные ресурсы системы. В системе должно быть выделено резервное рабочее место администратора (рабочая станция, терминал), с которого проводится ведение СЗИ НСД, загрузка и останов системы, ее восстановление и тестирование. В системе должны иметься средства автоматического восстановления СЗИ НСД. Программные средства тестирования СЗИ НСД должны постоянно присутствовать в системе и запускаться при каждой загрузке системы и по командам администратора. Должна осуществляться многоуровневая физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС СФЗ, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС СФЗ, включающее использование автоматизированной системы контроля и управления доступом в помещения, либо автономных устройств.

Класс «2П». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «3П». Дополнительно СЗИ НСД должна обеспечивать:

1. Проверку подлинности программ по эталонным контрольным суммам соответствующих файлов во время загрузки системы и перед каждым их запуском.

2. Проверку подлинности рабочих станций, терминалов, узлов по специальному аутентификационному протоколу.

3. Контроль доступа операторов к программам, командам управления системой и режимам их выполнения по принципу «в две руки» по паролям и таблицам санкционирования. Одним из операторов должен быть администратор.

4. Контроль доступа персонала к операциям над томами, каталогами, файлами, записями по таблицам санкционирования.

5. Контроль доступа операторов (администраторов) к ресурсам (томам, каталогам, файлам, программам) рабочих станций, терминалов, узлов сети по спискам доступа с учетом заданных привилегий.

Класс «2П». Подсистема регистрации и учета. Требования совпадают с аналогичными требованиями класса «2А». Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию доступа персонала к ресурсам рабочих станций, терминалов, узлов сети. В параметрах регистрации указываются:

- время и дата попытки доступа;
- идентификатор оператора (администратора);
- спецификация (имя, адрес) рабочей станции, терминала, узла сети;
- спецификация (имя) ресурса (том, каталог, файл, программа);
- вид запрошенного доступа;

•результат попытки: успешный или неуспешный – несанкционированный.

2. Регистрацию доступа «в две руки» к программам, командам системы и режимам их выполнения. В параметрах регистрации указываются:

•время и дата попытки доступа к программе, команде;

•идентификатор (имя) программы, команды, их режима (ключа);

•идентификаторы (имена) операторов-участников;

•результат попытки: успешный или неуспешный – несанкционированный.

3.Регистрацию доступа персонала к операциям над томами, каталогами, файлами, записями. В параметрах регистрации указываются:

•время и дата попытки доступа;

•идентификатор оператора;

•спецификация (имя) тома, каталога, файла, записи;

•вид запрошенной операции (чтение, запись, удаление и т.п.);

•результат попытки: успешный или неуспешный – несанкционированный.

Класс «2П». Криптографическая подсистема. Требования совпадают с аналогичными требованиями класса «2А».

Требования к первой группе

Класс «1А». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «2П». Дополнительно СЗИ НСД должна обеспечивать:

1. Проверку подлинности и контроль доступа в систему и доступа к загрузке/останову системы операторов (администраторов)

по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролям кратковременного действия (не более 1-го месяца) длиной не менее 8 алфавитно-цифровых символов. Администратор не должен иметь доступ к паролям операторов. В системе должны использоваться программные средства для смены паролей самими операторами с соответствующей проверкой их уникальности и длины.

2. Проверку подлинности (аутентификацию) внешних устройств системы по специальным тестам и протоколам аутентификации при каждом доступе к устройству.

3. Контроль доступа операторов к командам управления внешними устройствами по принципу «в три руки» по паролям и таблицам санкционирования. Одним из операторов должен быть администратор.

Класс «1А». Подсистема регистрации и учета. Требования совпадают с аналогичными требованиями класса «2П». Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию входа субъектов доступа (операторов, администратора) в систему с учетом снятых биометрических характеристик или специальных устройств (жетонов, карт, электронных ключей) и паролей. В параметрах регистрации указываются:

- время и дата входа/выхода субъекта доступа в систему/из системы;
- идентификатор (имя) субъекта доступа;
- результат попытки входа: успешный или неуспешный – несанкционированный, причина неуспешной попытки (неправильные биометрические характеристики, специальное устройство, пароль, время доступа и т.п.).

2. Регистрацию доступа «в три руки» к командам управления внешними устройствами системы. В параметрах регистрации указываются:

•время и дата попытки выдачи команды устройства;

•идентификатор (адрес, имя) устройства;

•идентификаторы (имена) операторов-участников (3-х);

•вид запрошенной команды;

•результат попытки: успешный или неуспешный – несанкционированный.

3. Регистрацию изменения конфигурации системы. В параметрах регистрации указываются:

•время и дата внесения изменения;

•идентификатор администратора;

•вид изменения конфигурации (добавление, исключение внешних устройств, изменение режимов функционирования и т.п.).

Должен проводиться учет всех носителей информации (томов) с помощью их защищенной маркировки с использованием сертифицированных специальных защитных знаков, учет носителей должен проводиться в журнале с регистрацией их выдачи/приема.

Должна проводиться сигнализация (оперативное отображение и звуковое оповещение) попыток несанкционированного доступа к ресурсам системы (внешним устройствам, томам, каталогам, файлам, программам) на основной и резервной рабочей станции (терминале) администратора системы и на звуковом устройстве ближайшего пункта охраны. Данные сигнализации должны включать:

•идентификатор (имя, адрес) рабочей станции (терминала), с которой осуществлена несанкционированная попытка доступа к ресурсу;

•идентификатор оператора;

•идентификатор (имя) ресурса;

•вид запрошенной операции с ресурсом;

•причина отклонения доступа к ресурсу (нет привилегий, недостаточно привилегий и тому подобное).

Класс «1А». Криптографическая подсистема. Требования совпадают с аналогичными требованиями класса «2П». Дополнительно СЗИ НСД должна обеспечивать шифрование служебной информации СЗИ НСД (идентификаторов, паролей, таблиц санкционирования) и конфиденциальных (секретных) данных системы при их записи на накопители с использованием алгоритма ГОСТ 28147—89.

Класс «1А». Подсистема обеспечения целостности. Требования совпадают с аналогичными требованиями класса «2П». Дополнительно СЗИ НСД должна обеспечивать следующее.

Контроль целостности СЗИ НСД, программ и чувствительных данных системы при загрузке системы и по командам по эталонным контрольным суммам с использованием имитовставки алгоритма ГОСТ 28147–89.

Многократно резервироваться в «горячем режиме» должны наиболее критичные ресурсы системы (устройства, каналы связи и данные) и архивироваться в автоматическом режиме все данные и программы системы.

В системе должно быть выделено дополнительное мобильное рабочее место администратора (рабочая станция, терминал), с которого может проводиться ведение СЗИ НСД, загрузка и останов системы, ее конфигурирование, восстановление и тестирование в любой точке системы.

В системе должны иметься средства автоматического восстановления программных средств и данных всей системы.

Программные средства тестирования СЗИ НСД и системы должны постоянно присутствовать в системе и запускаться автоматически при каждой несанкционированной попытке доступа к ресурсам системы для проверки их целостности.

Класс «1П». Подсистема управления доступом. Требования совпадают с аналогичными требованиями класса «1А». Дополнительно СЗИ НСД должна обеспечивать контроль доступа операторов к операциям по изменению наиболее чувствительных томов, каталогов, файлов, записей системы по принципу «в две руки» по паролям и таблицам санкционирования. Одним из операторов должен быть администратор.

Класс «1П». Подсистема регистрации и учета. Требования совпадают с аналогичными требованиями класса «1А». Дополнительно СЗИ НСД должна обеспечивать:

1.Регистрацию доступа «в две руки» персонала к операциям по изменению наиболее чувствительных томов, каталогов, файлов, записей. В параметрах регистрации указываются:

- время и дата попытки доступа;
- идентификаторы операторов;
- спецификация (имя) тома, каталога, файла, записи;
- вид запрошенного изменения (запись, модификация, удаление и тому подобное);
- результат попытки: успешный или неуспешный – несанкционированный.

Класс «1П». Криптографическая подсистема. Требования совпадают с аналогичными требованиями класса «1А».

Класс «1П». Подсистема обеспечения целостности. Требования совпадают с аналогичными требованиями класса «1А».

12.11. Информационная безопасность систем радиосвязи, используемых на ЯО

Безопасность информации при использовании средств и систем радиосвязи на ЯО обеспечивается комплексом организационно-технических мер, проводимых на этапах проектирования, создания

и эксплуатации и направленных на исключение возможности передачи по открытому радиоканалу сведений ограниченного доступа, прямо или косвенно раскрывающих основную деятельность ЯО, его систему безопасности, в том числе СФЗ, исключение возможности несанкционированного доступа к этим радиосистемам и их информационным ресурсам, на предотвращение нарушения работоспособности и дезорганизацию систем радиосвязи.

Все переговоры между радиоабонентами должны проводиться исключительно в рамках «Перечня сведений, разрешенных к открытой передаче», утверждаемого руководителями предприятий.

При необходимости передачи по системам радиосвязи секретной и другой информации ограниченного доступа должны быть реализованы методы защиты этой информации на основе кодирования, шифрования или скремблирования. Выбор конкретных методов и способов защиты информации осуществляется предприятием с учетом степени важности информации ограниченного доступа и по согласованию с вышестоящей организацией.

Технические и программно-аппаратные средства, реализующие указанные способы защиты, должны иметь соответствующие сертификаты соответствия по требованиям безопасности информации.

Комплекс программно-технических средств и мер по защите систем радиосвязи и циркулирующей в них информации от несанкционированного доступа и воздействия должен включать подсистемы управления доступом, регистрации и учета, преобразования информации и обеспечения целостности информации.

Объем и содержание требуемых мер защиты от НСД устанавливается в соответствии с классом защищенности системы радиосвязи и определяется на этапе проектирования системы радиосвязи на основании отраслевого руководящего документа «Классификация систем транкинговой радиосвязи, используемых в СФЗ, по требованиям безопасности информации» [12.13].

Определение класса защищенности от НСД системы радиосвязи осуществляется комиссией, назначаемой руководством предприятия, с обязательным привлечением специалистов службы безопасности предприятия.

Мероприятия по защите информации от НСД реализуются в ходе развертывания и эксплуатации радиосистемы.

Программно-аппаратные и технические средства защиты информации, применяемые в средствах и системах радиосвязи предприятий и организаций, должны иметь соответствующие сертификаты соответствия по требованиям безопасности информации. Сертификация указанных средств осуществляется в Системе сертификации средств защиты информации.

При использовании криптографических средств защиты, их сертификация проводится в системе сертификации средств защиты.

Обеспечению установленных требований, предъявляемых к системам радиосвязи, содействует система контроля, которая должна быть обязательно создана и использоваться. Основными задачами органов, осуществляющих контроль, являются предупреждение, своевременное выявление и пресечение нарушений установленных требований, контроль за устранением выявленных нарушений и недостатков. Все средства и системы радиосвязи предприятий атомной отрасли подлежат государственному надзору со стороны органов Госсвязьнадзора России, представители которого имеют право доступа ко всем радиосредствам в установленном порядке по предъявлению соответствующего удостоверения. Ведомственный контроль за соблюдением установленных режимов работы систем и средств радиосвязи и обеспечением порядка передачи информации по каналам радиосвязи на ЯО осуществляется вышестоящей организацией.

12.12. Классификация систем радиосвязи, используемых на ЯО, по требованиям безопасности информации

Классификацию систем радиосвязи, используемых на ЯО, по требованиям информационной безопасности рассмотрим на примере классификации наиболее распространенных в данном случае систем транкинговой радиосвязи (СТРС), предназначенных для использования в системах физической защиты ЯО [12.13].

Рассматриваемая в данном случае классификация не распространяется на обычные системы мобильной радиосвязи, обеспечивающие непосредственное взаимодействие мобильных радиостанций (радиотелефонов) между собой.

В современных СТРС широко применяются микропроцессорные технологии и средства вычислительной техники, обеспечивающие их функционирование, включая управление соединениями и каналами связи, администрирование и обеспечение безопасности системы.

Безопасность СТРС направлена на предупреждение несанкционированного доступа к ресурсам СТРС (транкинговым контроллерам (ТК), терминалам технического обслуживания, диспетчерским пультам, мобильным радиостанциям) и циркулирующей в ней информации, а также отказа или прерывания в обслуживании абонентов.

Секретная информация, циркулирующая и хранящаяся в СТРС, не должна передаваться по радиоканалам в открытом виде.

Одним из важных аспектов безопасности информации для СТРС, предназначенных для критических условий применения, является противодействие навязыванию ложной информации – предупреждение (выявление) ложных посылок и информационных сообщений, несанкционированных управляющих СТРС команд (телеграмм), посылаемых в систему нарушителем от имени легаль-

ного пользователя (администратора) в целях нарушения или блокирования радиосвязи.

Применительно к СТРС НСД определяется как доступ к ресурсам и информации СТРС, нарушающий установленные правила разграничения доступа, с использованием как штатных средств СТРС, так и нештатных технических средств. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения абонентских мобильных радиостанций и управляющих устройств базовых радиостанций (транкинговых контроллеров) СТРС и входящих в их состав СВТ. Под нештатными средствами понимаются произвольные технические средства и программно-технические комплексы (в частности, измерительная аппаратура, средства регистрации и анализа информации, формирования и передачи радиосигналов и сообщений), не входящие в состав СТРС. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по физической защите и специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

Неотъемлемой частью системы защиты информации является комплекс организационных мер по обучению персонала, разграничению обязанностей и ответственности должностных лиц, созданию и сопровождению системы контроля доступа к техническим средствам системы и санкционирования их использования.

Безопасность информации и непрерывность функционирования СТРС должны поддерживаться также комплексом технических мер, обеспечивающих работоспособность и нормальные условия эксплуатации основных компонент системы в неблагоприятных условиях и при воздействии дестабилизирующих внешних факторов. К наиболее важным из них относятся: обеспечение гарантиро-

ванного (бесперебойного) электропитания, аппаратное резервирование наиболее критичных для работоспособности системы узлов, средства диагностики и восстановления функций при сбоях и нарушении работоспособности элементов системы, средства резервного копирования и восстановления информационных данных и программного обеспечения.

Для оценки полноты и качества реализованного в СТРС комплекса средств защиты проводится на основе классификации СТРС по требованиям безопасности информации выбор соответствующего класса защищенности (с учетом определенных условий применения СТРС). Отнесение СТРС к определенному классу защищенности по требованиям безопасности информации необходимо также в целях разработки и применения обоснованных средств и мер защиты, а также оценки их достаточности для достижения требуемого уровня защищенности ресурсов СТРС, включая циркулирующую в СТРС информацию.

Выбор конкретного класса защищенности СТРС, средств и методов защиты ресурсов СТРС осуществляется на основе анализа условий применения, уровня конфиденциальности (секретности) циркулирующей информации и важности поддержания постоянной работоспособности СТРС с учетом возможности реализации угроз безопасности информации в конкретных условиях эксплуатации системы.

Основными этапами классификации СТРС являются:

- анализ исходных данных;
- выявление основных признаков СТРС, существенных для ее классификации;
- сравнение выявленных признаков СТРС с требованиями классификации;
- проведение сертификации СТРС по требованиям безопасности информации и присвоение СТРС класса защищенности, соот-

ветствующего качеству реализованного комплекса средств и мер защиты ресурсов от НСД.

Необходимыми исходными данными для классификации СТРС являются:

- уровень защищенности от НСД ресурсов СТРС (базовых станций, транкинговых контроллеров, терминалов технического обслуживания, диспетчерских пультов, мобильных радиостанций – радиотелефонов) и циркулирующей в системе информации (речевой, цифровых информационных и управляющих данных);
- уровень защищенности СТРС от отказа или прерывания обслуживания абонентов;
- режим функционирования (автономный, комплексный – с выходом на другие системы связи, включая телефонную сеть общего пользования);
- средства и методы администрирования СТРС.

Выбор класса СТРС производится заказчиком и/или разработчиком с привлечением квалифицированных специалистов (компетентных организаций) по защите информации.

Подтверждение соответствия СТРС определенному классу защищенности производится при сертификации СТРС по требованиям безопасности информации. Сертификация производится аккредитованными установленным порядком сертификационными центрами и испытательными лабораториями.

Устанавливаются три класса защищенности СТРС, различающихся условиями их эксплуатации и уровнем защиты. Низший класс защищенности третий, высший – первый.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите. СТРС, к которым не предъявляется требований по защите информации, а также СТРС, не удовлетворяющие требованиям третьего класса защищенности, не классифицируются по требованиям безопасности информации. Все

классы защищенности СТРС предполагают использование подключений к другим (внешним) коммуникационным системам, включая ТфОП.

Третий класс характеризуется требованиями по санкционированности использования абонентского оборудования СТРС и авторизованному администрированию с соответствующей регистрацией в системе событий, способных повлиять на безопасность информации в СТРС и надежность функционирования СТРС.

Применение СТРС третьего класса защищенности рекомендуется, если кратковременное нарушение непрерывности связи не является критичным (например, при наличии дублирующих каналов связи), в условиях, не требующих обязательной защиты передаваемой речевой информации и надежной аутентификации абонентов.

Такие условия характерны для систем охраны удаленных объектов, их внутренних технологических и коммуникационных систем, для организации оперативной связи обслуживающих подразделений.

Второй класс дополнительно допускает хранение в СВТ базовых станций (транкинговых контроллерах, локальных терминалах технического обслуживания) учетной и регистрационной информации с грифом не выше «секретно». Второй класс СТРС содержит два подкласса: 2Б и 2А. СТРС второго класса защищенности должны обеспечивать возможность фильтрации управляющих сообщений (команд) как на уровне управляющих устройств базовых станций – транкинговых контроллеров (подкласс 2Б), так и на уровне СВТ абонентских мобильных радиостанций (радиотелефонов) СТРС (подкласс 2А). К механизмам идентификации, аутентификации, регистрации и надежности функционирования оборудования для систем второго класса предъявляются более жесткие требования, в частности, дополнительно требуется наличие в системе воз-

можности активной аутентификации пользователя при инициировании сеанса связи.

Область использования СТРС второго класса – оперативная связь подразделений обеспечения и охраны при транспортировке ядерных материалов и другие подобные условия применения, в которых важна надежная аутентификация абонентов (в том числе по инициативе базовой станции) с целью исключения возможности несанкционированного использования абонентского оборудования для навязывания ложных сообщений.

СТРС второго класса рекомендуется использовать в тех случаях, когда критичны аспекты защищенности каналов связи на относительно короткие промежутки времени и важна санкционированная доступность (непрерывность функционирования) средств связи.

В СТРС первого класса допускается возможность хранения учетной и регистрационной информации на управляющих устройствах СТРС (транкинговых контроллерах, локальных терминалах технического обслуживания) и передачи по эфиру зашифрованной информации с грифом «секретно» для подкласса 1Б и «совершенно секретно» для подкласса 1А с использованием средств криптографической защиты передаваемой информации (СКЗИ), сертифицированных для соответствующего грифа секретности информации. Использование СКЗИ должно проводиться в соответствии с установленными правилами эксплуатации СКЗИ. Для оборудования базовых станций (транкинговых контроллеров, коммутаторов, интерфейсов) должно быть предусмотрено аппаратное резервирование средств, выполняющих основные функции коммутации и управления; в состав СТРС должны входить средства преобразования передаваемой информации к виду, исключающему возможность прослушивания передаваемых по эфиру сообщений, а для подклассов 1Б и 1А – гарантированной стойкости; аутентификация пользователей в СТРС является обязательной; должна быть преду-

смотрена возможность реализации обратного вызова при инициализации сеанса связи. Подклассы 1В, 1Б, 1А различаются по средствам аутентификации и преобразования информации.

СТРС первого класса, обеспечивающие высокую достоверность идентификации и аутентификации абонентов и гарантированную стойкость защиты радиоканалов, целесообразно использовать в системах принятия решений и управления верхнего уровня и, в случае необходимости, в системах оперативного управления при ликвидации последствий и угрозы возникновения аварийных ситуаций.

Комплекс программно-технических средств и мер по защите СТРС от НСД реализуется в рамках единой системы защиты информации от НСД (СЗИ НСД), функционально подразделяемой на следующие подсистемы:

- управления доступом;
- администрирования;
- регистрации и учета;
- преобразования информации;
- обеспечения целостности.

В зависимости от класса защищенности СТРС в рамках этих подсистем реализуются определенные требования, которые представлены в табл. 12.2 со следующими обозначениями:

« - » – нет требований к данному классу;

« + » – есть требования к данному классу.

« = » – требования совпадают с требованиями предшествующего класса.

Рассмотрим требования по информационной безопасности СТРС отдельно по классам:

Требования к третьему классу

Подсистема управления доступом. Все мобильные радиостанции должны иметь уникальные идентификаторы (номера, адреса). Базовой станцией (транкинговым контроллером – ТК) СТРС должна проводиться автоматическая аутентификация мобильных радиостанций по идентификатору (номеру, адресу) при инициализации сеанса связи.

При этом должен проводиться контроль:

- доступа мобильных радиостанций абонентов к базовой станции по спискам доступа;
- доступа мобильных радиостанций абонентов СТРС к режиму экстренных сообщений по спискам доступа (при наличии в СТРС такого режима);
- доступа мобильных радиостанций абонентов СТРС к сервису «групповой вызов» по спискам доступа (при наличии в СТРС такого режима);
- вызова мобильными радиостанциями абонентов СТРС абонентов телефонной сети общего пользования (ТфОП), а также доступа к СТРС со стороны абонентов ТфОП по спискам доступа.

Таблица 12.2. Классификация СТРС

№ п/п	Подсистемы и требования	Классы защищенности СТРС					
		3	2Б	2А	1В	1Б	1А
	1. Подсистема управления доступом						
	Проверка подлинности (аутентификация)						
1.1	Проверка подлинности мобильной радиостанции, телефона (радиотелефона)	+	=	=	+	=	+
1.2	Проверка подлинности абонента со стороны базовой станции	-	+	+	+	=	+
1.3	Проверка подлинности вызывающего абонента со стороны вызываемого	-	-	-	+	=	+
1.4	Проверка подлинности базовой станции со стороны абонента	-	-	+	=	+	=
	Управление доступом субъектов:						
1.5	К мобильной радиостанции	-	-	+	=	=	+
1.6	Абонентов к базовой станции	+	=	=	+	=	=
1.7	К выходу на другие системы связи (АТС) и входу из них	+	=	=	+	=	+
1.8	К режиму экстренных сообщений	+	=	=	=	+	=
1.9	К групповому вызову	+	=	=	=	+	=
	Фильтрация управляющих данных						
1.10.	Фильтрация управляющих данных, принимаемых базовой станцией	-	+	=	+	=	=
1.11	Фильтрация управляющих данных, принимаемых мобильной радиостанцией	-	-	+	=	+	=
	2. Подсистема администрирования						
	Аутентификация						
2.1	Проверка подлинности администратора (оператора) базовой станции	+	+	=	+	=	+
2.2	Проверка подлинности канала (устройства) доступа к функциям администрирования базовой станции	-	+	+	=	=	=

Окончание табл. 12.2

№ п/п	Подсистемы и требования	Классы защищенности СТРС					
		3	2Б	2А	1В	1Б	1А
	Управление доступом:						
2.3	Администратора к базовой станции	+	+	=	=	=	=
2.4	К функциям управления базовой станции	+	=	=	+	=	=
2.5	К регистрационной информации	-	+	=	=	=	=
	3. Подсистема регистрации и учета						
3.1	Включения/отключения базовой станции	+	=	=	=	=	=
3.2	Начала/завершения сеанса связи	+	=	=	=	=	=
3.3	Результатов проверки подлинности абонентов (радиостанций)	+	=	=	+	=	=
3.4	Доступа к внешним системам связи (АТС)	+	=	=	=	=	=
3.5	Доступа администратора к базовой станции	+	=	=	=	=	=
3.6	Изменения параметров настройки (конфигурации) базовой станции и полномочий абонентов	-	+	=	+	=	=
3.7	Доступа к регистрационной информации	-	+	=	=	=	=
3.8	Сигнализация попыток нарушения защиты	-	-	-	-	+	=
3.9	Блокирования управляющих данных при их фильтрации	-	+	+	=	=	=
	4. Подсистема преобразования информации						
4.1	Преобразование передаваемой информации	-	+	=	+	+	+
	5. Подсистема обеспечения целостности						
5.1	Обеспечение целостности программно-аппаратных средств и управляющей информации	+	+	+	+	=	+
5.2	Восстановление и тестирование	+	+	+	+	+	+
5.3	Документация	+	+	+	+	+	+

Подсистема администрирования. Для систем данного класса должны:

•проводиться проверка подлинности администратора при доступе к базовой станции (терминалу технического обслуживания, ТК) по идентификатору и паролю временного действия;

•проводиться контроль доступа администраторов к базовой станции (ТК, терминалу технического обслуживания) по спискам доступа к функциям управления;

•быть предусмотрены средства, либо предприняты меры, исключающие возможность удаленного администрирования СТРС абонентами внешних сетей связи, включая ТфОП.

Подсистема регистрации и учета. Для систем данного класса:

1.Должна проводиться регистрация загрузки, инициализации управляющего устройства СТРС (ТК, терминала технического обслуживания) и его останова. В параметрах регистрации указываются дата, время включения/выключения ТК (терминала технического обслуживания).

Регистрация даты, времени выключения управляющего устройства СТРС не производится при аварийном отключении базовой станции.

2.Должна проводиться регистрация результатов проверки подлинности мобильных радиостанций при их подключении к базовой станции (регистрации). В параметрах регистрации указываются:

•дата и время попытки подключения;

•идентификатор (номер, адрес) мобильной радиостанции (радиотелефона);

•результат проверки подлинности мобильной радиостанции (радиотелефона): успешная, неуспешная – несанкционированная (посторонняя) радиостанция.

3.Должна проводиться регистрация соединений абонентов. В параметрах регистрации указываются:

•дата и время попытки установления соединения;

•идентификаторы вызывающего и вызываемого абонента (номер, адрес устройства);

•результат попытки установления соединения: успешная, неуспешная;

•причина неуспешной и/или несанкционированной попытки установления соединения: несанкционированный номер, абонент отсутствует, занят и т.д.;

•длительность соединения;

•тип вызова (индивидуальный, групповой, экстренный и тому подобное);

•приоритет вызова.

4.Должна осуществляться регистрация доступа администратора к базовой станции (ТК, терминалу технического обслуживания). В параметрах регистрации указываются:

•дата и время попытки доступа к средствам управления базовой станцией;

•идентификатор, предъявленный при попытке доступа;

•вид доступа (локальный, удаленный);

•идентификатор (номер, адрес, порт) оборудования, используемого при доступе;

•результат попытки: успешный, неуспешный – несанкционированный.

5.Должна проводиться регистрация доступа мобильных радиостанций абонентов СТРС к внешним системам связи (ТфОП) и абонентов ТфОП к базовой станции. В параметрах регистрации указываются:

•дата и время попытки доступа;

•идентификатор (номер) вызывающего абонента;

•идентификатор (номер) вызываемого абонента;

•результат попытки доступа: успешная, неуспешная – несанкционированная.

Подсистема обеспечения целостности. Устройства управления базовой станции (ТК, терминал технического обслуживания) должны содержать средства контроля за целостностью своей программной и информационной части.

Для базовой станции должна быть предусмотрена процедура восстановления после сбоев и отказов оборудования, обеспечивающая восстановление эксплуатационных свойств технических средств СТРС.

В базовой станции должны быть предусмотрены средства восстановления программной и информационной (управляющей) части, доступные администратору.

В базовой станции должна обеспечиваться возможность регламентного тестирования:

•процесса проверки подлинности мобильных радиостанций и администраторов;

•процесса регистрации доступа к базовой станции и внешним системам связи;

•реализации правил разграничения доступа мобильных радиостанций абонентов к разрешенным видам сервиса;

•процесса контроля за целостностью программной и информационной части управляющих устройств базовой станции;

•процедуры восстановления программно-технической и информационной части базовой станции (транкингового контроллера, терминала технического обслуживания).

Требования к документации. Эксплуатационная документация на СТРС должна включать следующие документы:

1.Руководство пользователя, содержащее описание функций СТРС, инструкцию по использованию абонентской мобильной радиостанции и общий порядок работы с ней.

2.Руководство администратора базовой станции, содержащее:

•описание и порядок сопровождения функций, контролируемых базовой станцией (ТК);

•руководство по настройке и конфигурированию управляющего устройства базовой станции (ТК);

•описание старта базовой станции (ТК) и процедур проверки правильности старта;

•руководство по процедуре восстановления;

•описание средств и процесса контроля за целостностью программной и информационной части управляющих устройств базовой станции (ТК, терминала технического обслуживания).

3.Конструкторская (проектная) документация должна содержать процедуры восстановления свойств базовой станции (ТК, терминала технического обслуживания), а также спецификации, схемы, интерфейсы следующих средств:

•управляющих устройств базовой станции (ТК);

•аутентификации мобильных радиостанций и администратора;

•контроля доступа и регистрации;

•контроля за целостностью программной и информационной части базовой станции (ТК, терминала технического обслуживания);

4.Тестовая документация должна содержать описание тестов и испытаний, которым подвергалась СТРС и результаты тестирования.

Требования ко второму классу

Требования к техническим средствам. Технические средства базовой станции СТРС должны быть сертифицированы по требованиям безопасности информации по уровню защищенности, обеспечивающему возможность обработки и хранения информации с грифом «секретно», и иметь заключение об отсутствии специально внедренных средств несанкционированного съема (передачи) информации и сертификат, выданные аккредитованным органом.

Класс 2Б. Подсистема управления доступом. Должны быть выполнены требования к подсистеме управления доступом для СТРС класса 3. Дополнительно должны проводиться:

- аутентификация абонентов мобильных радиостанций по цифровому паролю временного действия;
- фильтрация управляющим устройством базовой станции (ТК) управляющих данных (команд, телеграмм). Механизм фильтрации должен обеспечивать блокирование неразрешенных (несанкционированных) управляющих воздействий на базовую станцию.

Класс 2Б. Подсистема администрирования. Должны быть выполнены требования к подсистеме администрирования для СТРС класса 3. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Должна проводиться аутентификация администратора при доступе к базовой станции (ТК, терминалу технического обслуживания) по идентификатору и паролю временного действия длиной не менее шести символов. Пароль не должен передаваться по эфиру и/или линиям связи в открытом виде (кроме случая локального подключения терминала администратора).

2.Должна проводиться проверка подлинности (санкционированности) канала доступа (порта, интерфейса базовой станции,

терминала технического обслуживания) администратора к базовой станции (ТК).

3.Вывод регистрационной и учетной информации СТРС, в том числе создание ее резервных копий, должен производиться только на учтенные носители информации соответствующего грифа, передача такой информации между базовыми станциями (в многозоновой конфигурации СТРС) должна осуществляться по защищенным линиям связи.

Класс 2Б. Подсистема регистрации и учета. Должны быть выполнены требования к подсистеме регистрации и учета для СТРС класса 3. Дополнительно должно быть предусмотрено выполнение следующих требований.

1.Должна проводиться регистрация следующих действий администратора:

- изменение режима функционирования СТРС;
- включение и исключение абонентов;
- изменение полномочий абонентов;
- вывод на терминал технического обслуживания (копирование, печать) регистрационной и учетной информации СТРС;
- очистка журнала (журналов) регистрации.

2.Должна осуществляться регистрация блокирования базовой станцией (ТК) фильтруемых управляющих данных. В параметрах регистрации указываются: дата, время, идентификатор абонента, тип и параметры отклоненной команды.

Класс 2Б. Подсистема преобразования информации. В СТРС должны быть реализованы средства преобразования передаваемой речевой информации, позволяющие исключить возможность ее прямого прослушивания по эфиру.

Передача секретной регистрационной и учетной информации между базовыми станциями должна осуществляться по защищенным линиям связи.

Класс 2Б. Подсистема обеспечения целостности. Должны быть выполнены требования к подсистеме обеспечения целостности для СТРС класса 3. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Процедура контроля целостности должна выполняться автоматически при каждом включении (инициализации) управляющего устройства базовой станции (ТК, терминала технического обслуживания).

2.В базовой станции (ТК, терминале технического обслуживания) должна дополнительно обеспечиваться возможность регламентного тестирования защищенных линий связи между базовыми станциями, а также тестирования следующих процессов:

- проверки подлинности абонентов;
- проверки санкционированности канала (интерфейса) доступа администратора к базовой станции;
- фильтрации управляющих данных (команд) базовой станцией (ТК);
- преобразования передаваемой речевой информации;
- автоматического контроля за целостностью программной и информационной части базовой станции (ТК, терминала технического обслуживания).

Класс 2Б. Требования к документации. Должны быть выполнены требования к документации для СТРС класса 3. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Руководство пользователя должно дополнительно содержать описание правил использования средств аутентификации по цифровому паролю и преобразования информации (скремблирования), порядок инициализации этого режима.

2.Руководство администратора базовой станции должно дополнительно содержать описание и порядок:

•сопровождения средств аутентификации абонентов по цифровому паролю;

•сопровождения средств проверки санкционированности канала (интерфейса) доступа администратора к базовой станции;

•сопровождения средств фильтрации управляющих сообщений (команд) базовой станцией (ТК) СТРС, описание режимов их использования и конфигурирования;

•сопровождения средств преобразования (скремблирования) передаваемой речевой информации;

•передачи, копирования и восстановления регистрационной и учетной информации базовой станции (ТК, терминала технического обслуживания) СТРС.

3.Конструкторская (проектная) документация должна дополнительно содержать спецификации, интерфейсы, алгоритмы следующих средств:

•аутентификации абонентов по цифровому паролю;

•проверки санкционированности канала (интерфейса) доступа администратора к базовой станции;

•фильтрации управляющих сообщений базовой станцией (ТК);

•автоматического контроля за целостностью программной и информационной части базовой станции (ТК, терминала технического обслуживания).

4.Тестовая документация должна дополнительно содержать описание и порядок проведения тестов следующих процессов:

•проверки подлинности абонентов;

•проверки санкционированности канала (интерфейса) доступа администратора к базовой станции;

•фильтрации управляющих данных (команд) базовой станцией (ТК);

•преобразования передаваемой речевой информации;

•автоматического контроля за целостностью программной и информационной части базовой станции (ТК, терминала технического обслуживания).

Класс 2А. Подсистема управления доступом. Должны быть выполнены требования к подсистеме управления доступом для СТРС класса 3 и 2Б. Дополнительно должны проводиться:

•автоматическая аутентификация базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) при инициализации сеанса связи;

•аутентификация абонентов по цифровому паролю временного действия по запросу. Пароль не должен передаваться по эфиру и линиям связи в открытом виде;

•контроль доступа абонентов к мобильной радиостанции (к ее включению/активизации) по условно-постоянному цифровому коду;

•фильтрация принимаемой мобильной радиостанцией управляющей информации (команд). Механизм фильтрации должен обеспечивать блокирование неразрешенных (несанкционированных) управляющих воздействий (команд) на мобильную радиостанцию.

Класс 2А. Подсистема администрирования. Должны быть полностью выполнены требования к подсистеме администрирования для СТРС класса 3, 2Б. Дополнительно должны иметься в наличии технические, программные или программно-технические средства, либо быть приняты организационно-технические меры, обеспечивающие контроль удаленного администрирования по телефонным и радиоканалам, доступным базовой станции СТРС.

Класс 2А. Подсистема регистрации и учета. Данные требования полностью включают требования к подсистеме регистрации

и учета для СТРС класса 3, 2Б. Дополнительно должна осуществляться регистрация (индикация) блокирования мобильной радиостанцией фильтруемых управляющих данных (команд). В параметрах регистрации указываются: дата, время, идентификатор абонента, тип и параметры отклоненной команды.

Класс 2А. Подсистема преобразования информации. Данные требования полностью включают требования к подсистеме преобразования информации для СТРС класса 2Б.

Класс 2А. Подсистема обеспечения целостности. Данные требования полностью включают требования к подсистеме обеспечения целостности для СТРС класса 3, 2Б. Дополнительно должно быть предусмотрено в базовой станции (транкинговом контроллере, терминале технического обслуживания) обеспечение возможность регламентного тестирования:

- процесса проверки подлинности базовой станции со стороны мобильной радиостанции;
- процесса аутентификации абонентов по цифровому паролю временного действия по запросу;
- контроля доступа абонентов к мобильной радиостанции по условно-постоянному цифровому коду;
- процесса фильтрации принимаемой мобильной радиостанцией управляющей информации (команд).

Класс 2А. Требования к документации. Должны быть выполнены требования к документации для СТРС класса 3, 2Б. Дополнительно должно быть предусмотрено выполнение следующих требований.

1.Руководство пользователя должно дополнительно содержать описание правил:

- аутентификации абонентов по цифровому паролю временного действия по запросу;

•доступа абонентов к мобильной радиостанции (к ее включению/активизации) по условно-постоянному цифровому коду;

•проверки подлинности базовой станции со стороны мобильной радиостанции.

2.Руководство администратора базовой станции должно дополнительно содержать описание и порядок сопровождения следующих средств:

•аутентификации абонентов по цифровому паролю временного действия по запросу;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по условно-постоянному цифровому коду;

•проверки подлинности базовой станции со стороны мобильной радиостанции;

•фильтрации принимаемой мобильной радиостанцией управляющей информации (команд).

3.Конструкторская (проектная) документация должна дополнительно содержать спецификации, интерфейсы следующих средств:

•аутентификации абонентов по цифровому паролю временного действия по запросу;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по условно-постоянному цифровому коду;

•проверки подлинности базовой станции со стороны мобильной радиостанции;

•фильтрации принимаемой мобильной радиостанцией управляющей информации (команд).

4.Тестовая документация должна дополнительно содержать описание и порядок проведения тестов следующих процесса (средств):

•аутентификации абонентов по цифровому паролю временного действия по запросу;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по условно-постоянному цифровому коду;

•проверки подлинности базовой станции со стороны мобильной радиостанции;

•фильтрации принимаемой мобильной радиостанцией управляющей информации (команд).

Требования к первому классу

Требования к техническим средствам. Для технических средств базовой станции СТРС класса 1В должны быть полностью выполнены аналогичные требования для класса 2.

Технические средства базовой станции СТРС, абонентские мобильные радиостанции и оконечные устройства (терминалы), при применении которых допускается обработка и передача секретной информации, должны быть сертифицированы по требованиям безопасности информации по уровню защищенности, обеспечивающему возможность обработки и передачи информации с грифом «секретно» для СТРС класса 1Б и «совершенно секретно» для СТРС класса 1А и иметь заключение об отсутствии специально внедренных средств несанкционированного съема (передачи) информации и сертификат, выданные аккредитованным органом.

Класс 1В. Подсистема управления доступом. Должны быть выполнены требования к подсистеме управления доступом для СТРС класса 3, 2Б, 2А. Дополнительно должны проводиться:

•автоматическая аутентификация мобильной радиостанции, телефона ТфОП по их идентификатору (номеру, адресу) и цифровому паролю временного действия длиной не менее шести цифр при инициализации связи, пароль не должен передаваться по эфиру и/или физическим линиям связи в открытом виде;

•аутентификация абонента мобильной радиостанции со стороны базовой станции (ТК) по специальному сигналу (бипера);

•автоматическая аутентификация вызывающего абонента со стороны вызываемого через базовую станцию (ТК).

4.Должна проводиться фильтрация управляющих данных (команд), принимаемых базовой станцией (ТК), по таблице санкционирования управляющих команд для абонентов и администратора (администраторов).

Класс 1В. Подсистема администрирования. Должны быть полностью выполнены требования к подсистеме администрирования для СТРС класса 3, 2Б, 2А. Дополнительно должны проводиться:

•аутентификация администратора при доступе к базовой станции (ТК, терминалу технического обслуживания) по идентификатору и паролю временного действия, длиной не менее восьми буквенно-цифровых символов;

•контроль доступа администратора к критичным функциям управления базовой станцией (ТК) по дополнительному паролю.

Класс 1В. Подсистема регистрации и учета. Данные требования полностью включают требования к подсистеме регистрации и учета для СТРС класса 3, 2Б. Дополнительно должна осуществляться регистрация:

•неуспешных проверок подлинности вызывающего абонента со стороны вызываемого. В параметрах регистрации указываются:

дата, время, идентификаторы вызывающего и вызываемого абонентов (мобильных станций, номеров телефонов);

•изменения параметров (конфигурации) базовой станции (ТК) со стороны администратора. В параметрах регистрации указываются: дата, время, идентификатор администратора, наименование измененных параметров, их старое и новое значение.

Класс 1В. Подсистема преобразования информации. Данные требования полностью включают аналогичные требования класса 2Б. Дополнительно должно осуществляться автоматическое динамическое перераспределение передаваемой информации сеанса связи по различным частотным каналам.

Класс 1В. Подсистема обеспечения целостности. Данные требования полностью включают требования к подсистеме обеспечения целостности для СТРС класса 3, 2Б, 2А. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Взаимодействие между базовыми станциями (ТК, коммутаторами) в многозоновых транкинговых системах должно осуществляться по защищенным каналам связи, либо с использованием защищенного протокола обмена.

2.Базовая станция (ТК, терминал технического обслуживания) должна содержать средства автоматического контроля за целостностью своей программной и информационной части, а также постоянной части управляющей информации с помощью контрольных сумм.

3.Базовая станция (ТК, терминал технического обслуживания) должна предусматривать процедуру автоматического восстановления после сбоев и отказов оборудования, которая должна обеспечивать восстановление свойств СТРС, а также после выявления нарушения целостности программных и информационных ресурсов.

4.В базовой станции (ТК) должна обеспечиваться возможность дополнительного регламентного тестирования:

•процесса проверки подлинности абонента мобильной радиостанции со стороны базовой станции (ТК) по специальному сигналу (бипера);

•автоматической проверки подлинности вызывающего абонента со стороны вызываемого через базовую станцию (ТК);

•процесса контроля доступа администратора к функциям управления базовой станции (ТК) по дополнительному паролю;

•процедур регистрации изменения параметров (конфигурации) базовой станции (ТК) со стороны администратора.

Класс 1В. Требования к документации. Должны быть выполнены требования к документации для СТРС класса 3, 2Б, 2А. Кроме этого должно быть предусмотрено выполнение следующих требований:

1.Руководство пользователя должно содержать следующие описания.

•применения средств аутентификации абонентов по специальному сигналу (бипера);

•автоматической аутентификации мобильной радиостанции, телефона ТфОП;

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК).

2.Руководство администратора базовой станции должно содержать:

•описание и порядок сопровождения средств аутентификации абонентов по специальному сигналу (бипера);

•описание и порядок сопровождения средств автоматической аутентификации мобильных радиостанций, телефонов ТфОП;

•описание и порядок сопровождения средств автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК);

•описание и порядок сопровождения таблиц санкционирования при фильтрации управляющих команд.

3.Конструкторская (проектная) документация должна содержать спецификации, интерфейсы следующих средств:

•аутентификации абонентов по специальному сигналу (бипера);

•автоматической аутентификации мобильных радиостанций, телефонов;

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК);

•фильтрации и таблиц санкционирования.

4.Тестовая документация должна содержать описание и порядок проведения тестов следующих процессов (средств):

•аутентификации абонентов по специальному сигналу (бипера);

•автоматической аутентификации мобильных радиостанций, телефонов ТФОП;

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК);

•фильтрации по таблицам санкционирования.

Класс 1Б. Подсистема управления доступом. Должны быть выполнены требования к подсистеме управления доступом для СТРС класса 3, 2Б, 2А, 1В. Дополнительно должны проводиться:

1.Автоматическая проверка подлинности базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) и изменяемому коду при инициализации связи.

2.Контроль доступа абонентов СТРС к режиму экстренных сообщений по спискам доступа.

3.Контроль доступа абонентов СТРС к сервису «групповой вызов» по спискам доступа.

4.Фильтрация управляющих данных, принимаемых базовой станцией (ТК), по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов).

5.Фильтрация управляющих данных, принимаемых мобильной абонентской радиостанцией, по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов).

Класс 1Б. Подсистема администрирования. Данные требования включают требования к подсистеме администрирования для СТРС класса 3, 2Б, 2А, 1В.

Класс 1Б. Подсистема регистрации и учета. Данные требования полностью включают требования к подсистеме регистрации и учета для СТРС класса 3, 2Б, 1В. Дополнительно должна осуществляться оперативная (в реальном масштабе времени) сигнализация попыток нарушения защиты на дисплей оператора СТРС. В параметрах сигнализации должны указываться: дата, время, идентификатор (номер) абонента, вид попытки нарушения.

Класс 1Б. Подсистема преобразования информации. Должно осуществляться преобразование всей передаваемой по эфиру и линиям связи между базовыми станциями информации с помощью криптографических средств гарантированной стойкости, устойчивых к пассивному и активному прослушиванию эфира и линий связи, сертифицированных для закрытия информации с грифом «секретно».

Класс 1Б. Подсистема обеспечения целостности. Данные требования полностью включают требования к подсистеме обеспечения целостности для СТРС класса 3, 2Б, 2А, 1В. Дополнительно в базовой станции должна обеспечиваться возможность дополнительного регламентного тестирования следующих процессов (средств):

•автоматической проверки подлинности базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) и изменяемому коду при инициализации связи;

•контроля доступа абонентов СТРС к режиму экстренных сообщений по спискам доступа;

•контроля доступа абонентов СТРС к сервису «групповой вызов» по спискам доступа;

•фильтрации управляющих данных, принимаемых базовой станцией (ТК), по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов);

•процесса (средств) фильтрации управляющих данных, принимаемых мобильной абонентской радиостанцией, по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов);

•оперативного оповещения администратора базовой станции (ТК) о попытках нарушения правил защиты информации в СТРС.

Класс 1Б. Требования к документации. Должны быть выполнены требования к документации для СТРС класса 3, 2Б, 2А, 1В. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Руководство пользователя должно содержать следующие описания:

•автоматической проверки подлинности базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) и изменяемому коду при инициализации связи;

•порядка доступа абонентов СТРС к режиму экстренных сообщений по спискам доступа;

•порядка доступа абонентов СТРС к сервису «групповой вызов» по спискам доступа.

2.Руководство администратора базовой станции должно содержать описание и порядок сопровождения следующих средств:

•автоматической проверки подлинности базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) и изменяемому коду при инициализации связи;

•контроля доступа абонентов СТРС к режиму экстренных сообщений по спискам доступа;

•контроля доступа абонентов СТРС к сервису «групповой вызов» по спискам доступа;

•фильтрации управляющих данных, принимаемых базовой станцией (ТК) и мобильной радиостанцией, по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов);

•преобразования информации;

•оперативного оповещения администратора базовой станции (ТК) о попытках нарушения правил защиты информации в СТРС.

3.Конструкторская (проектная) документация должна дополнительно содержать спецификации, интерфейсы следующих средств:

•автоматической проверки подлинности базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) и изменяемому коду при инициализации связи;

•контроля доступа абонентов СТРС к режиму экстренных сообщений и групповому вызову по спискам доступа;

•фильтрации управляющих данных, принимаемых базовой станцией (ТК) и мобильной радиостанцией, по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов);

•оперативного оповещения администратора базовой станции (ТК) о попытках нарушения правил защиты информации в СТРС.

4.Тестовая документация должна дополнительно содержать описание и порядок проведения тестов следующих процессов (средств):

•автоматической проверки подлинности базовой станции (ТК) со стороны мобильной радиостанции по ее идентификатору (номеру, адресу) и изменяемому коду при инициализации связи;

•контроля доступа абонентов СТРС к режиму экстренных сообщений и групповому вызову по спискам доступа;

•фильтрации управляющих данных, принимаемых базовой станцией (ТК) и мобильной радиостанцией, по встроенной таблице разрешенных управляющих команд для заданных исходных источников (адресов);

•оперативного оповещения администратора базовой станции (ТК) о попытках нарушения правил защиты информации в СТРС.

Класс 1А. Подсистема управления доступом. Должны быть выполнены требования к подсистеме управления доступом для СТРС класса 3, 2Б, 2А, 1В, 1Б. Дополнительно должны проводиться:

1.Аутентификация абонента мобильной радиостанции со стороны базовой станции (ТК) по специальным устройствам авторизации доступа (магнитным, смарт-картам и т.п.).

2.Автоматическая аутентификация вызывающего абонента со стороны вызываемого через базовую станцию (ТК) с использованием специальных устройств авторизации доступа.

3.Автоматическая аутентификация мобильной радиостанции, телефона по их конфиденциальному идентификатору (номеру, адресу) по специальному защищенному протоколу при инициализации сеанса связи.

4.Контроль доступа абонентов к мобильной радиостанции (к ее включению/активизации) по специальным устройствам авторизации доступа.

5.Контроль доступа абонентов СТРС к внешним сетям связи и абонентов из внешних сетей в СТРС по цифровым паролям и спискам доступа.

Класс 1А. Подсистема администрирования. Данные требования включают требования к подсистеме администрирования для СТРС класса 3, 2Б, 2А, 1В. Дополнительно должна проводиться аутентификация администратора при доступе к:

- базовой станции (ТК) по идентификатору, паролю временного действия и специальному устройству авторизации доступа по защищенному протоколу (интерфейсу);
- базовой станции (ТК, терминалу технического обслуживания) и к функциям управления базовой станции по дополнительному временному паролю длиной не менее восьми символов с использованием защищенного протокола (интерфейса).

Класс 1А. Подсистема регистрации и учета. Данные требования полностью включают требования к подсистеме регистрации и учета для СТРС класса 3, 2Б, 1В, 1Б.

Класс 1А. Подсистема преобразования информации. Должно осуществляться преобразование всей передаваемой по эфиру и линиям связи между базовыми станциями информации с помощью криптографических средств гарантированной стойкости, устойчивых к пассивному и активному прослушиванию эфира и линий связи, сертифицированных для закрытия информации с грифом «совершенно секретно».

Класс 1А. Подсистема обеспечения целостности. Данные требования полностью включают требования к подсистеме обеспечения целостности для СТРС класса 3, 2Б, 2А, 1В. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Должна осуществляться периодическая автоматическая проверка целостности всех программ и управляющих данных базовой

станции при ее функционировании и их автоматическое восстановление в случае выявления нарушения целостности.

2.В базовой станции должна обеспечиваться возможность дополнительного регламентного тестирования следующих процессов (средств):

•аутентификации абонента мобильной радиостанции со стороны базовой станции (ТК) по специальным устройствам авторизации доступа (магнитным, смарт-картам и т.п.);

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК) с использованием специальных устройств авторизации доступа;

•автоматической аутентификации мобильной радиостанции, телефона по их конфиденциальному идентификатору (номеру, адресу) по специальному защищенному протоколу при инициализации сеанса связи;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по специальным устройствам авторизации доступа;

•процесса (средств) контроля доступа абонентов СТРС к внешним сетям связи и абонентов из внешних сетей в СТРС по цифровым паролям и спискам доступа;

•периодической автоматической проверки целостности всех программ и управляющих данных базовой станции при ее функционировании и их автоматического восстановления в случае выявления нарушения целостности.

Класс 1А. Требования к документации. Должны быть выполнены требования к документации для СТРС класса 3, 2Б, 2А, 1В, 1Б. Дополнительно должно быть предусмотрено выполнение следующих требований:

1.Руководство пользователя должно содержать описания следующих правил:

•аутентификации абонента мобильной радиостанции со стороны базовой станции (ТК) по специальным устройствам авторизации доступа (магнитным, смарт-картам и т.п.);

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК) с использованием специальных устройств авторизации доступа;

•автоматической аутентификации мобильной радиостанции, телефона ТфОП по их конфиденциальному идентификатору (номеру, адресу) по специальному защищенному протоколу при инициализации сеанса связи;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по специальным устройствам авторизации доступа;

•проведения контроля доступа абонентов СТРС к внешним сетям связи (ТфОП) и абонентов из внешних сетей в СТРС по цифровым паролям и спискам доступа.

2.Руководство администратора базовой станции должно содержать описание и порядок сопровождения:

•средств аутентификации абонента мобильной радиостанции со стороны базовой станции (транкингового контроллера) по специальным устройствам авторизации доступа (магнитным, смарт-картам и т.п.);

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК) с использованием специальных устройств авторизации доступа;

•средств автоматической аутентификации мобильной радиостанции, телефона ТфОП по их конфиденциальному идентифика-

тору (номеру, адресу) по специальному защищенному протоколу при инициализации сеанса связи;

•средств контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по специальным устройствам авторизации доступа;

•средств контроля доступа абонентов СТРС к внешним сетям связи (ТфОП) и абонентов из внешних сетей в СТРС по цифровым паролям и спискам доступа.

3.Конструкторская (проектная) документация должна содержать спецификации и интерфейсы следующих средств:

•аутентификации абонента мобильной радиостанции со стороны базовой станции (транкингового контроллера) по специальным устройствам авторизации доступа (магнитным, смарт-картам и т.п.);

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК) с использованием специальных устройств авторизации доступа;

•автоматической аутентификации мобильной радиостанции, телефона ТфОП по их конфиденциальному идентификатору (номеру, адресу) по специальному защищенному протоколу при инициализации сеанса связи;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по специальным устройствам авторизации доступа;

•контроля доступа абонентов СТРС к внешним сетям связи (ТфОП) и абонентов из внешних сетей в СТРС по цифровым паролям и спискам доступа.

4.Тестовая документация должна содержать описание и порядок проведения тестов следующих процессов (средств):

•аутентификации абонента мобильной радиостанции со стороны базовой станции (ТК) по специальным устройствам авторизации доступа (магнитным, смарт-картам и т.п.);

•автоматической аутентификации вызывающего абонента со стороны вызываемого через базовую станцию (ТК) с использованием специальных устройств авторизации доступа;

•автоматической аутентификации мобильной радиостанции, телефона ТфОП по их конфиденциальному идентификатору (номеру, адресу) по специальному защищенному протоколу при инициализации сеанса связи;

•контроля доступа абонентов к мобильной радиостанции (к ее включению/активизации) по специальным устройствам авторизации доступа;

•контроля доступа абонентов СТРС к внешним сетям связи (ТфОП) и абонентов из внешних сетей в СТРС по цифровым паролям и спискам доступа.

Вопросы для самоконтроля

1. Дайте определение понятий «информационная безопасность», «защита информации».
2. Определите составляющие характеристики защищенности информации.
3. Дайте определение понятия «политика безопасности».
4. Назовите этапы выработки политики безопасности.
5. Назовите нормативные документы федерального уровня, определяющие политику информационной безопасности ЯО.
6. Назовите характерные свойства функционирования АС СФЗ ЯО с точки зрения информации и информационной безопасности.

7. Чем определяются основные требования по защите информации, составляющей государственную и служебную тайны?

8. Какие сведения необходимо защищать на ЯО?

9. Какие информационные объекты необходимо защищать на ЯО?

10. Определите роль подсистемы защиты информации в СФЗ ЯО.

11. Определите основные каналы утечки информации в СФЗ ЯО.

12. Определите основные источники угроз информационной безопасности СФЗ ЯО.

13. Какие угрозы связаны с непреднамеренной деятельностью человека?

14. Какие угрозы связаны с умышленной деятельностью человека?

15. Определите возможные способы нарушения информационной безопасности СФЗ ЯО.

16. Перечислите информационные способы нарушения информационной безопасности СФЗ ЯО.

17. Перечислите программно-математические способы нарушения информационной безопасности СФЗ ЯО.

18. Перечислите физические способы нарушения информационной безопасности СФЗ ЯО.

19. Перечислите радиоэлектронные способы нарушения информационной безопасности СФЗ ЯО.

20. Перечислите организационно-правовые способы нарушения информационной безопасности СФЗ ЯО.

21. Каковы составляющие модели потенциального нарушителя информационной безопасности СФЗ ЯО?

22. Определите методы получения защищенной информации о ЯО вероятным нарушителем.

23. Определите основные направления защиты информации на ЯО.

24. Определите основные меры защиты информации на ЯО.

25. Определите структуру подсистемы защиты информации в СФЗ ЯО.

26. Определите роль категорирования объектов в обеспечении информационной безопасности ЯО.

27. Определите роль классификации систем в обеспечении информационной безопасности ЯО.

28. Определите роль аттестации СФЗ в обеспечении информационной безопасности ЯО.

29. Определите роль контроля в обеспечении информационной безопасности ЯО.

30. Определите порядок организации на ЯО работ по созданию и эксплуатации СФЗ и ее подсистемы защиты информации.

31. Определите стадии создания подсистемы защиты информации СФЗ.

32. Сформулируйте требования и рекомендации по защите речевой информации.

33. Сформулируйте требования и рекомендации по защите информации от утечки за счет побочных электромагнитных излучений и наводок.

34. Сформулируйте требования и рекомендации по защите информации от несанкционированного доступа.

35. Сформулируйте требования и рекомендации по защите информации от фотографических и оптико-электронных средств разведки.

36. Сформулируйте требования к персоналу СФЗ ЯО.

37. Определите общие принципы классификации АС СФЗ ЯО.

38. Какие исходные данные необходимы для классификации АС СФЗ ЯО?

39. Перечислите классы АС СФЗ ЯО, дайте их краткую характеристику.

40. Перечислите подсистемы системы защиты информации СФЗ ЯО.

41. Определите принципы обеспечения информационной безопасности систем радиосвязи ЯО.

42. Сформулируйте принципы обеспечения информационной безопасности СТРС при их использовании на ЯО.

43. Перечислите основные этапы классификации СТРС.

44. Перечислите основные данные, необходимые для классификации СТРС.

45. Перечислите классы защищенности СТРС и дайте их краткую характеристику.

46. Перечислите подсистемы системы защиты информации СТРС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК
(жирным шрифтом выделены основные источники)

К предисловию

П.1. Методика проектирования систем физической защиты/ Сандийская национальная лаборатория, 1997.

П.2. Системы физической защиты ядерно-опасных объектов. Учебное пособие/ Под ред. Н.С. Погожина. Авторы: П.В. Бондарев, К.А. Каширин, М.А. Костиков, А.И. Толстой. М.: МИФИ, 2001.

П.3. Информационная безопасность систем физической защиты, учета и контроля ядерных материалов: Учебное пособие/ К.А. Каширин, А.С. Пискарев, Н.С. Погожин, А.И. Толстой, А.В. Шеин. М.: МИФИ, 2002.

П.4. Измайлов А.В. Методы проектирования и анализ эффективности систем физической защиты ядерных материалов и установок: Учебное пособие. М.: МИФИ, 2002.

К главе 1

1.1. Интегрированные системы физической защиты. Обнинск: МСУЦ, 1999.

1.2. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. М.: Гелиос АРВ, 2005.

1.3. Алексеенко В.Н., Древс Ю.Г. Основы построения систем защиты производственных предприятий и банков. М.: МИФИ, 1996.

К главе 2

2.1 Основы физической защиты. Компьютерный обучающий курс, версия 2.0. Обнинск: МСУЦ, 2002.

2.2. Иванов И.В. Охрана периметров – 2. М.: Паритет Граф, 2000.

2.3. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. М.: Горячая линия-Телеком, 2004.

К главе 3

3.1. ГОСТ Р 51241-98. Технические средства защиты и охраны. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

3.2. Системы управления доступом/ А. М. Абрамов, О.Ю. Никулин, А.Н. Петрушин. М.: ОБЕРЕГ- РБ, 1998.

3.3. Biometrics in Physical Access Control. Issues, Status and Trends. Англ. / Bill Spence. - Recognition Systems, Inc. 1996.

3.4. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Гостехкомиссия России. М., 1992.

3.5. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссия России. М., 1997.

3.6. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требований по защите информации. Гостехкомиссия России. М., 1992.

К главе 4

4.1. Никулин О.Ю., Петрушин А.Н. Системы телевизионного наблюдения. М.: ОБЕРЕГ-РБ, 1997.

4.2. Яворский Б.М., Детлаф А.А. Справочник по физике для инженеров и студентов вузов. М.: Наука, 1977.

4.3. Андрианов В.И., Соколов А.В. Охранные устройства для дома и офиса. СПб.: Лань, 1997.

4.4. Дамьяновски В. Библия охранного телевидения/ Пер. с англ. М.: ООО «Ай-Эс-Эс пресс», 2003.

К главе 5

5.1. Технические средства безопасности. Часть 1: Учебно-методическое пособие/ Т.Г. Кирюхина, А.Н. Членов. М.: НОУ «Такир», 2002.

5.2. Лабораторный практикум «Системы физической защиты». Часть 1. М.: МИФИ, 2002.

К главе 6

6.1. Интегрированные системы физической защиты. Обнинск: МСУЦ, 1999.

6.2. Брюховецкий Р.И. Технические средства охраны периметров. М.: Научно-производственный центр Барьер-3, 2003.

6.3. По материалам фирмы «Эксперт» (www.fzekspert.ru).

6.4. По материалам компании «ЭЛИКС» (www.elics.ru/company/main.html).

6.5. По материалам компании GUNNEBO ITALDIS (www.gunnebo italdis.com).

6.6. По материалам компании «ООО Полипром» (www.polp-2.ru).

6.7. По материалам компании «ООО Спецэффект» (www.spec.ru).

6.8. По материалам компании «ООО Блок-Плюс» (www.Blok-Plus.ru).

К главе 7

7.1. Технические средства безопасности. Часть 1: Учебно-методическое пособие/ Т.Г. Кирюхина, А.Н. Членов. М.: НОУ «Такир», 2002.

7.2. Лабораторный практикум «Системы физической защиты». Часть 1. М.: МИФИ, 2002.

7.3. Отраслевой документ «Положение о порядке использования систем радиосвязи на предприятиях Минатома России». М.: Минатом России, 1999.

К главе 8

8.1. Терминологический словарь по учету, контролю и физической защите ядерных материалов. М.: ЦНИИАтоминформ, 2000.

8.2. Закон Российской Федерации по использованию атомной энергии от 21.10.1995, № 170-ФЗ.

8.3. Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов, утвержденные постановлением Правительства Российской Федерации от 19.07.2007, № 456.

К главе 9

9.1. Методические рекомендации по анализу уязвимости ядерно-опасных объектов. Отраслевой нормативный документ Минатома России. 2000.

9.2. Системы физической защиты ядерно-опасных объектов. Методические рекомендации по концептуальному проектированию. Отраслевой нормативный документ Минатома России. 1993.

9.3. Системы физической защиты ядерно-опасных объектов. Методические рекомендации по оценке эффективности. Отраслевой нормативный документ Минатома России. 2004.

9.4. Инструкция о порядке разработки, согласования, утверждения и составе проектной документации на строительство предприятий, зданий и сооружений. СНиП 11-01-95. Минстрой России. 1995.

9.5. Системы физической защиты ядерно-опасных объектов. Инструкция по проектированию. Отраслевой нормативный документ Минатома России. 2001.

9.6. Системы физической защиты ядерно-опасных объектов. Требования к проектным решениям. Отраслевой нормативный документ Минатома России. 2001.

К главе 10

10.1. Автоматизированная система безопасности транспортировки ядерных материалов (АСБТ).— ФГУП «СНПО «Элерон»», Росатом 2005.

10.2. Методика пошагового моделирования «Table Top».— Окриджская национальная лаборатория, США. 2002.

10.3. Компьютерная программа моделирования боестолкновений в процессе перевозок ядерных материалов «Полигон».— ФГУП «СНПО «Элерон»», Росатом. 2005.

К главе 11

11.1. Системы физической защиты ЯОО. Методические рекомендации по анализу уязвимости ЯОО. Минатом РФ (проект). 2001.

11.2. Системы физической защиты ЯОО. Методические рекомендации по оценке эффективности. Минатом РФ (проект). 2001.
11.3. Описание компьютерной программы SAVI.— Sandia NL, США. 1998.
11.4. Описание компьютерной программы ASSESS. Материалы тренинг-курса по обучению пользованию программой.— LLNL, США. 1995.
11.5. Описание компьютерной программы «Вега-2».— ФГУП «СНПО «Элерон»», Минатом России. 1999.

К главе 12

12.1. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». М., 1995.
12.2. Герасименко В.А., Малюк А.А. Основы защиты информации. Учебник. М.: МИФИ, 1997.
12.3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Книга 1. М.: Энергоатомиздат, 1994.
12.4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Книга 2. М.: Энергоатомиздат, 1994.
12.5. Скородумов Б.И. Информационная безопасность. Обеспечение безопасности информации электронных банков. М.: МИФИ, 1995.
12.6. Отраслевые методические рекомендации «Концепция информационной безопасности СФЗ ЯОО». М.: Минатом России, 1999.
12.7. Руководящий документ «Общие требования по защите информации в СФЗ ЯОО». М.: Минатом России, 1999.
12.8. Руководящий документ «СФЗ ЯОО. Автоматизированные системы управления и обеспечения физической защиты. Защита информации от несанкционированного доступа. Классификация автоматизированных систем и требования по безопасности информации». М.: Минатома России, 1999.
12.9. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».1992.

12.10. Положение о сертификации средств защиты информации по требованиям безопасности информации. Гостехкомиссия России, 1995.
12.11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Гостехкомиссия России, 1995.
12.12. Отраслевой документ «Положение о порядке использования систем радиосвязи на предприятиях Минатома России». М.: Минатом России, 1999.
12.13. Временный руководящий документ «Классификация систем транкинговой радиосвязи, используемых в системах физической защиты, по требованиям безопасности информации». М.: Минатом России, 1999.

Павел Викторович Бондарев
Александр Владимирович Измайлов
Александр Иванович Толстой

ФИЗИЧЕСКАЯ ЗАЩИТА ЯДЕРНЫХ ОБЪЕКТОВ

Учебное пособие
Под редакцией Н.С. Погожина

Редактор *Е.Е. Шумакова*

Оригинал-макет выполнен:
П.В. Бондаревым, А.И. Толстым

Подписано в печать 24.11.2008. Формат 60×84 1/16
Печ.л. 36,5. Уч.-изд.л. 36,5. Тираж 150 экз.
Изд. № 1/52. Заказ № ____

Московский инженерно-физический институт
(государственный университет)
115409, Москва, Каширское ш., 31.
Типография издательства «ТРОВАНТ»,
г. Троицк Московской области

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК