Л. М. Лыньков, Т. В. Борботько, Н. И. Мухуров

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Рекомендовано Учебно-методическим объединением вузов Республики Беларусь по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия по курсам «Защита объектов связи и речевых сообщений от несанкционированного перехвата» и «Методы и средства ЗОС от несанкционированного доступа» для студентов учреждений, обеспечивающих получение высшего образования по специальностям I-98 01 02 «Защита информации в телекоммуникациях» и I-45 01 03 «Сети телекоммуникаций»

Минск БГУИР 2007

УДК 621.391.25 (075.8)
ББК 32.889 я 7
Л 88

Р е ц е н з е н т ы :
начальник кафедры «Автоматизированных систем управления»
УО «Военная академия Республики Беларусь»,
доц., канд. техн. наук, А. В. Хижняк;
зав. кафедрой радиоэлектронных средств УО «Белорусский
государственный университет информатики и радиоэлектроники»,
проф., канд. техн. наук, Н. С. Образцов

Лыньков, Л. М.

Л 88 Методы и средства защиты объектов от несанкционированного доступа : учеб.-метод. пособие / Л. М. Лыньков, Т. В. Борботько, Н. И. Муху-ров. – Минск : БГУИР, 2007. – 139 с.

ISBN 978-985-488-232-1

В пособии рассмотрена система информационной безопасности объекта связи. Особое внимание уделено организационным мероприятиям, позволяющим поддерживать необходимый уровень безопасности объекта связи, а также изложены вопросы технического контроля защищенности объектов от утечки информации по техническим каналам.

УДК 621.391.25 (075.8)
ББК 32.889 я 7

ISBN 978-985-488-232-1

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современных условиях информация представляет собой товар, цена которого может превышать стоимость самых дорогих образцов продукции. Защита ее от изменения, уничтожения и несанкционированного доступа представляет собой сложную проблему, обусловленную, прежде всего, тем, что в условиях информационной открытости наблюдается размывание границы между свободно распространяемой и конфиденциальной информацией.

Таким образом, защита информации представляет собой сложную многогранную проблему, часть которой на данный момент времени не имеет четкой целевой постановки.

В настоящее время в информационном обмене посредством телекоммуникационных сетей насчитывается большое число субъектов, участвующих в нем. Все информационные потоки, передаваемые от отправителя к получателю, проходят через объекты связи, надежность работы которых гарантирует своевременный и качественный прием и передачу этих данных. В результате этого, безопасность информационной телекоммуникационной системы напрямую зависит от безопасности объекта связи, стабильности его работы. Поэтому обеспечение контроля доступа на объект связи и в отдельные его категорированные помещения как его сотрудников, так и посетителей является актуальной проблемой.

1. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА СВЯЗИ

1.1. Цели и задачи системы информационной безопасности

Основной целью системы информационной безопасности (СИБ) является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта.

Не менее значимой целью СИБ является повышение качества предоставляемых услуг и гарантий безопасности, имущественных прав и интересов клиентов.

Достижение заданных целей возможно в ходе решения следующих основных задач:

- отнесение информации к категории ограниченного доступа (служебной тайне);

- прогнозирование и своевременное выявление угроз безопасности информационных ресурсов, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению их нормального функционирования и развития;

- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения различных видов ущерба;

- создание механизма и условий оперативного реагирования на угрозы информационной безопасности (ИБ) и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на

основе правовых, организационных и технических мер и средств обеспечения безопасности;

- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Рассмотрим модель построения СИБ, представленную на рис. 1.1.

Рис. 1.1. Модель построения системы информационной безопасности

Эта модель соответствует международному стандарту ISO/IEC 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью» и учитывает тенденции развития нормативной базы по вопросам информационной безопасности.

Представленная модель информационной безопасности – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

В ней отражены следующие объективные факторы:

- угрозы ИБ, характеризующиеся вероятностью возникновения и вероятностью реализации;

- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

- риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы ИБ: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной СИБ предполагается первоначально провести анализ рисков в области ИБ. Затем определить оптимальный уровень риска для объекта связи на основе заданного критерия. СИБ (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

1.2. Методика проведения аналитических работ

Данная методика позволяет:

- полностью проанализировать и документально оформить требования, связанные с обеспечением ИБ;

- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;

- оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;

- обеспечить проведение работ в сжатые сроки;

- представить обоснование для выбора мер противодействия;

- оценить эффективность контрмер, сравнить их различные варианты.

Этап 1. Определение границ исследования

Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми

осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные.

Этап 2. Построение модели информационной технологии

При построении модели необходимо учитывать взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

В соответствии с предлагаемой методикой эта модель строится следующим образом: для выделенных ресурсов определяется их ценность как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

Этап 3. Выбор контрмер

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут являться рекомендации по проведению регулярных проверок эффективности системы защиты.

Этап 4. Управление рисками

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия

существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Этап 5. Оценка достигаемой защищенности

В завершение работ можно определить меру гарантии безопасности информационной среды объекта, основанную на оценке, при которой можно доверять информационной среде объекта.

Данный подход предполагает, что гарантия возрастает с применением больших усилий при проведении оценки безопасности. Приведем для адекватности оценки основания:

- вовлечение в процесс оценки большего числа элементов информационной среды объекта;
- глубина, достигаемая за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения;
- строгость, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

1.2.1. Методология анализа рисков

Цель процесса оценивания рисков состоит в определении их характеристик в информационной системе и ее ресурсах. На основе таких данных выбираются необходимые средства управления ИБ.

Процесс оценивания рисков содержит несколько этапов:

- описание объекта и мер защиты;
- идентификация ресурса и оценивание его количественных показателей;
- анализ угроз ИБ;
- оценивание уязвимостей;
- оценивание существующих и предполагаемых средств обеспечения ИБ;

- оценивание рисков.

Риск, характеризующий опасность, которой может подвергаться система и использующая ее организация, зависит:

- от показателей ценности ресурсов;

- от вероятностей нанесения ущерба ресурсам (выражаемых через вероятности реализации угроз для ресурсов);

- от степени легкости, с которой уязвимости могут быть использованы при возникновении угроз (уязвимости системы защиты);

- от существующих или планируемых средств обеспечения ИБ.

Расчет этих показателей выполняется на основе математических методов, имеющих такие характеристики, как обоснование и параметры точности метода.

1.3. Проектирование системы безопасности объекта связи

Данная методика позволяет оценить или переоценить уровень текущего состояния ИБ объекта связи, выработать рекомендации по обеспечению (повышению) его ИБ, снизить потенциальные потери путем повышения устойчивости функционирования корпоративной сети, разработать концепцию и политику безопасности объекта, а также предложить планы защиты конфиденциальной информации, передаваемой по открытым каналам связи, защиты информации от умышленного искажения (разрушения), несанкционированного доступа к ней, ее копирования или использования.

1.3.1. Построение профиля защиты

На этом этапе разрабатывается план проектирования системы защиты информационной среды объекта связи. Производится оценка доступных средств, осуществляется анализ и планирование разработки и интеграции средств защиты (рис. 1.2). Необходимым элементом работы является определение допустимого риска объекта защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

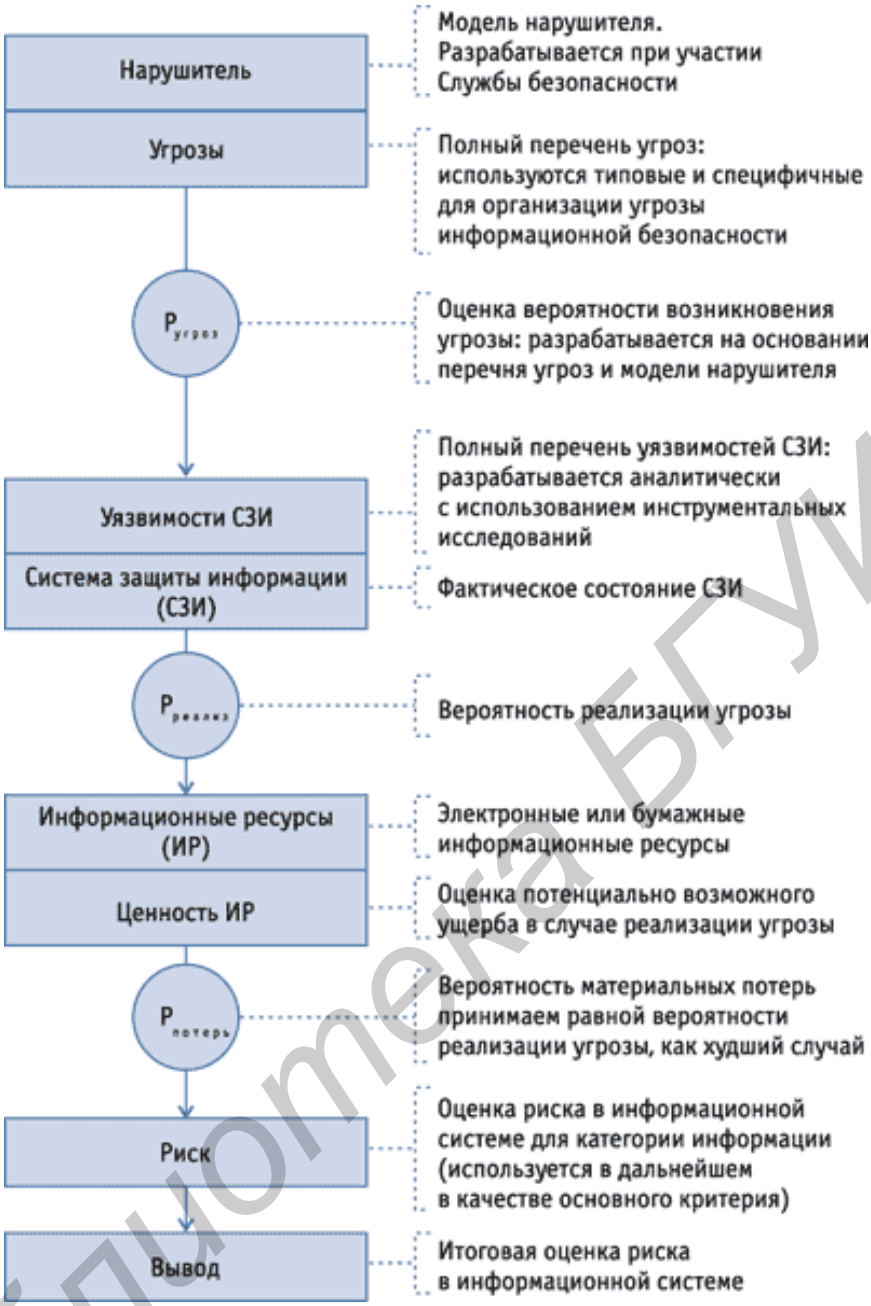

Рис. 1.2. Алгоритм оценки информационных рисков

Работа по построению плана защиты объекта начинается с построения профиля защиты. При этом часть этой работы уже была проделана при проведении анализа рисков.

Этап 1. Разработка организационной политики безопасности

Прежде чем предлагать какие-либо технические решения по СИБ объекта, предстоит разработать для него политику безопасности.

Собственно организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

СИБ объекта окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Шагами построения алгоритма организационной политики безопасности являются:

- внесение в описание объекта автоматизации структуры ценности и проведение анализа риска;

- определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается и утверждается.

Этап 2. Условия безопасного использования информационных технологий

Предполагается, что система обеспечения безопасности объекта связи, соответствующая выбранному профилю защиты, обеспечит требуемый уровень безопасности только в том случае, если она реализована, управляется и используется в соответствии с выработанными правилами. Операционная среда должна управляться согласно принятой для данного профиля защите нормативной документации, а также инструкциям администраторов и пользователей.

Выделяются следующие виды условий безопасного использования информационных технологий (ИТ):

- физические условия;

- условия для персонала;

- условия соединений.

Физические условия касаются размещения ресурсов объекта, а также защиты аппаратных средств и программного обеспечения, критичных к нарушению политики безопасности.

Условия для персонала содержат организационные вопросы управления безопасностью и отслеживания полномочий пользователей.

Условия соединений не содержат явных требований для сетей и распределенных систем, но, например, условие равенства положения означает наличие единой области управления всей сетью объекта.

Условия безопасного использования объекта автоматизации оформляются в виде отдельного документа, который согласовывается и утверждается.

Этап 3. Формулирование целей безопасности объекта

В данном разделе профиля защиты дается детализованное описание общей цели построения системы безопасности объекта связи, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив).

Факторы безопасности, в свою очередь, делят на технологические, технические и организационные.

Этап 4. Определение функциональных требований безопасности

Функциональные требования профиля защиты определяются на основе набора хорошо известных, отработанных и согласованных функциональных требований безопасности. Все требования к функциям безопасности можно разделить на два типа: управление доступом к информации и управление потоками информации.

На этом этапе предстоит правильно определить для объекта компоненты функций безопасности. Компонент функции безопасности описывает

определенный набор требований безопасности – наименьший выбираемый набор требований безопасности для включения в профиль защиты. Между компонентами могут существовать зависимости.

Этап 5. Определение требований гарантии достигаемой защищенности

Структура требований гарантии аналогична структуре функциональных требований и включает классы, семейства, компоненты и элементы гарантии, а также уровни гарантии. Классы и семейства гарантии отражают такие вопросы, как разработка, управление конфигурацией, рабочая документация, поддержание этапов жизненного цикла, тестирование, оценка уязвимости и другие вопросы.

Требования гарантии достигаемой защиты выражаются через оценки функций СИБ объекта. Оценка функции безопасности выполняется на уровне отдельного механизма защиты, а ее результаты позволяют определить относительную способность соответствующей функции безопасности противостоять идентифицированным угрозам. Исходя из известного потенциала нападения, функция защиты определяется, например, категориями «базовая», «средняя», «высокая».

Потенциал нападения определяется путем экспертизы возможностей, ресурсов и мотивов побуждения нападающего.

Предлагается использовать табличную сводку уровней гарантированности защиты. Уровни гарантии имеют иерархическую структуру, где каждый следующий уровень предоставляет большие гарантии и включает все требования предыдущего.

Этап 6. Формирование перечня требований

Перечень требований к системе информационной безопасности, эскизный проект, план защиты (далее – техническая документация, ТД) содержат набор требований безопасности информационной среды объекта связи, которые могут ссылаться на соответствующий профиль защиты, а также содержать требования, сформулированные в явном виде.

В общем виде разработка ТД включает:

- уточнение функций защиты;

- выбор архитектурных принципов построения СИБ;

- разработку логической структуры СИБ (четкое описание интерфейсов);

- уточнение требований функций обеспечения гарантоспособности СИБ;

- разработку методики и программы испытаний на соответствие сформулированным требованиям.

Этап 7. Оценка достигаемой защищенности

На этом этапе производится оценка меры гарантии безопасности информационной среды объекта, с которой после выполнения рекомендованных мероприятий можно доверять информационной среде объекта.

Базовые положения данной методики предполагают, что степень гарантии зависит от эффективности усилий при проведении оценки безопасности.

Увеличение усилий оценки предполагает:

- значительное число элементов информационной среды объекта, участвующих в процессе оценивания;

- расширение типов проектов и описаний деталей выполнения при проектировании системы обеспечения безопасности;

- строгость, заключающуюся в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

1.4. Классификация нарушителей. Основные характеристики нарушителей

Можно выделить классы нарушителей, действия которых наиболее вероятны для данного объекта. Для каждого класса нарушителей характерны свои способы действий, цели, задачи и т.п., а соответственно методы противодействия.

Основные характеристики, которые позволяют описать основные группы нарушителей:

- мотивы;
- цели;
- финансовое обеспечение;
- наличие и уровень профессиональной подготовки нарушителей;
- техническое обеспечение;
- наличие и качество предварительной подготовки преступления;
- наличие и уровень внедрения нарушителей на объект.

1.4.1. Мотивы нарушителей

- Желание приобрести материальные ценности (в т.ч. деньги);
- конкурентная борьба;
- сведение личных счетов;
- политические мотивы;
- религиозные мотивы;
- любопытство;
- неосознанные, немотивированные действия под влиянием алкоголя или наркотических веществ.

1.4.2. Цели нарушителей

- Кража материальных ценностей;
- получение информации;
- уничтожение материальных ценностей;
- уничтожение информации;
- создание помех функционированию объекта.

1.4.3. Финансовое обеспечение

Финансовое обеспечение деятельности нарушителей может изменяться в самых широких пределах. Уровни финансового обеспечения:

- практически не ограниченное;

- ограниченное;

- отсутствует.

Неограниченное финансирование характерно для спецслужб различных государств, международных террористических организаций и т.п.

Ограниченное финансирование характерно для борьбы небольших конкурирующих организаций. Финансовое обеспечение может отсутствовать у одиночек и случайных нарушителей.

1.4.4. Наличие и уровень профессиональной подготовки нарушителей

Наличие и уровень профессиональной подготовки нарушителей зависят от финансового обеспечения, но не связаны с ним напрямую. Понятно, что организации, обладающей достаточным финансовым обеспечением, проще найти профессионалов в любой области.

Хороший уровень профессиональной подготовки может быть, например, у бывших сотрудников какой-либо спецслужбы. Иной случай – попадаются криминальные группы, сумевшие получить финансирование грубыми методами, но не имеющие достаточной профессиональной подготовки.

1.4.5. Техническое обеспечение

Техническое обеспечение гораздо больше связано с финансовым состоянием, нежели профессиональная подготовка. Во многих случаях для преодоления систем безопасности требуется дорогостоящее оборудование и материалы, в том числе:

- оборудование и оснастка для разрушения и других способов преодоления технических укреплений;

- контрольно-измерительная аппаратура для обнаружения и идентификации технических средств;

- аппаратура для блокирования технических средств;

- вооружение;

- взрывчатые вещества.

1.4.6. Наличие и качество предварительной подготовки преступления

Эффективность действий нарушителя серьезно зависит от качества предварительной подготовки преступления. Подготовка преступления включает: планирование, разведку, внедрение на объект, проведение предварительной работы по блокированию технических средств и т.п.

Классы подготовки преступления:

- долговременная подготовка преступления;
- оперативная подготовка преступления;
- отсутствие подготовки.

Долговременная подготовка – наиболее эффективна для нарушителей, она позволяет провести весь комплекс подготовительных операций, вплоть до внедрения в руководящие структуры объекта. Время долговременной подготовки – от нескольких недель до нескольких лет.

Оперативная подготовка включает в себя в первую очередь техническую подготовку группы нарушителей. Время оперативной подготовки – от нескольких часов до нескольких недель. Чаще всего за это время сложно обеспечить внедрение на объект, провести соответствующую разведку и техническую подготовку на объекте.

Отсутствие подготовки характерно для случайных преступлений, совершаемых одиночками или небольшими группами.

1.4.7. Наличие и уровень внедрения нарушителей на объект

Наличие и уровень внедрения нарушителей на объект совершенно не обязательно зависят от предварительной подготовки преступления. Во многих случаях преступления совершают сами сотрудники. Причем преступники могут занимать любые должности, вплоть до высшего руководства.

Классы внедрения на объект:

- случайное внедрение – нарушители изначально работают на объекте не с целью совершения преступлений;

- целенаправленное внешнее внедрение – нарушители внедряются на объект с заранее поставленной целью: совершение преступления.

1.5. Основные классы нарушителей

Класс А. Нарушители, действующие злонамеренно и обладающие практически неограниченным финансовым обеспечением.

Класс Б. Нарушители, действующие злонамеренно и обладающие ограниченным, но достаточно крупным финансовым обеспечением.

Класс В. Нарушители, действующие злонамеренно, обладающие малым (или вообще отсутствующим) финансовым обеспечением, но имеющие хороший профессиональный уровень подготовки.

Класс Г. Нарушители, действующие злонамеренно, обладающие малым (или вообще отсутствующим) финансовым обеспечением и имеющие низкий уровень профессиональной подготовки.

Класс Д. Нарушители, действующие не злонамеренно.

1.5.1. Группы и общие свойства нарушителей класса А

Наиболее опасный класс нарушителей.

К нарушителям класса А могут относиться следующие группы организаций:

- спецслужбы;

- международные террористические организации;

- организованные крупные криминальные структуры;

- конкурирующие организации государственного масштаба (крупные концерны, холдинги; крупные банки и т.п.).

Общие свойства нарушителей класса А:

- практически не ограниченное финансирование;

- высокий профессионализм исполнителей;

- хорошее техническое обеспечение;

- длительная подготовка операций;

- глубокое внедрение на объект (вплоть до верхних уровней управления).

В некоторых случаях нарушители класса А привлекают к своим действиям государственные ведомства – налоговую инспекцию, КРУ, ОБЭП, различные силовые структуры и т.п.

1.5.2. Группы и общие свойства нарушителей класса Б

Наиболее характерные представители класса Б – конкурентные организации. Этот класс составляют криминальные структуры средних размеров, а также относятся лица, входящие в руководство охраняемых предприятий и организовавшие в рамках этих предприятий криминальную деятельность (чаще всего – хищения в крупных размерах).

Общие свойства нарушителей класса Б:

- ограниченное финансирование;

- возможен высокий профессиональный уровень подготовки исполнителей;

- хорошее техническое обеспечение;

- длительная подготовка операций;

- подготовленное внедрение на объект (чаще всего не на верхние уровни управления).

1.5.3. Группы и общие свойства нарушителей класса В

В большинстве случаев представители класса В – профессионально подготовленные криминальные группы, состоящие из бывших сотрудников различных спецслужб.

Общие свойства нарушителей класса В:

- ограниченное финансирование;

- высокий профессионализм исполнителей;

- возможно хорошее техническое обеспечение (если нарушители имеют доступ к техническому обеспечению организации, из которой они вышли);

- длительная подготовка операций;

- возможно глубокое внедрение на объект (зависит от профессионализма нарушителей).

1.5.4. Группы и общие свойства нарушителей класса Г

Самый распространенный класс нарушителей.

В класс Г входят следующие категории нарушителей: сотрудники объекта и внешние лица.

Нарушители класса Г могут нанести существенный урон, например совершить кражу кабельного оборудования.

Общие свойства нарушителей класса Г:

- отсутствие финансирования;

- отсутствие профессионализма исполнителей;

- отсутствие технического обеспечения;

- возможна и длительная подготовка операций, и случайные действия;

- возможно случайное внедрение на объект (например если нарушители изначально работают на этом объекте).

1.5.5. Группы и общие свойства нарушителей класса Д

Нарушители, действующие не злонамеренно. Во многих случаях, такие нарушители могут нанести ощутимый урон предприятию. Группы нарушителей:

- лица, собирающие грибы, ягоды на территории объектов;

- лица в состоянии алкогольного опьянения, проникающие на территорию объектов без определенной мотивации;

- сотрудники предприятий, имеющие «собственное мнение» и действующие в нарушение регламента предприятия;

- сотрудники предприятий, совершающие ошибки в процессе производственной деятельности.

Общие свойства нарушителей класса Д:

- отсутствие финансирования;

- отсутствие предварительной подготовки;
- отсутствие специального технического обеспечения.

2. АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ

2.1. Постановка задачи анализа рисков

Правильная постановка задачи анализа рисков, равно как и обоснование требований к методике их оценки – одна из важнейших предпосылок, обеспечивающих успешность управления рисками. Существуют различные подходы к оценке рисков, зависящие от уровня требований, предъявляемых в организации к режиму ИБ, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

2.1.1. Минимальные требования к режиму информационной безопасности

Минимальным требованиям к режиму ИБ соответствует ее базовый уровень. Основная область использования этого уровня – типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких, как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для их нейтрализации обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

2.1.2. Повышенные требования к режиму информационной безопасности

В случаях, когда нарушения режима ИБ ведут к тяжелым последствиям, базовый уровень требований к режиму ИБ является недостаточным. Для того чтобы сформулировать дополнительные требования, необходимо:

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

- оценить вероятности угроз;

- определить уязвимости ресурсов.

2.2. Управление рисками

Должна быть разработана стратегия управления рисками разных классов. Возможны несколько подходов:

- уменьшение риска (предполагает использование контрмер);

- уклонение от риска;

- изменение характера риска (использование различных вариантов страхования);

- принятие риска (многие риски не могут быть уменьшены до пренебрежимо малой величины).

2.2.1. Подготовительные этапы управления рисками

Выбор анализируемых объектов и уровня детализации их рассмотрения – первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и ресурсов. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Цели оценки рисков:

- определение приемлемости существующих рисков;

- определение необходимых защитных средств.

Оценка рисков является количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками – оптимизационная задача, решаемая путем применения соответствующих программных средств.

При идентификации активов, т.е. тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации.

Информационной основой крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное оборудование, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение и из каких узлов оно используется. Информационными активами являются также данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений ИБ.

Управление рисками – процесс нелинейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может возникнуть необходимость возврата к предыдущему. Так, при идентификации активов может оказаться, что выбранные границы анализа следует расширить, а степень детализации – увеличить.

2.2.2. Основные этапы управления рисками

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они напрямую с рисками не связаны. Риск появляется там, где есть угрозы.

Первый шаг в анализе угроз – их идентификация. Целесообразно выявлять не только сами угрозы, но и источники их возникновения.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятности).

Кроме вероятности осуществления важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем.

После того как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, т.е. собственно к оценке рисков. Целесообразно применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9.

Первые два результата можно отнести к низкому риску, третий и четвертый – к среднему, два последних – к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков. Правда, граничные случаи, когда вычисленная величина совпала с приемлемой, целесообразно рассматривать более тщательно из-за приближенного характера результата.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные меры защиты.

Оценивая стоимость мер защиты, разумеется, приходится учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала.

Эту стоимость также можно оценить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и допустимым риском.

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним механизмом обеспечения безопасности сразу нескольких прикладных сервисов.

Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой.

Когда намеченные меры приняты, необходимо проверить их действенность, т.е. убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками.

3. УПРАВЛЕНИЕ ДОСТУПОМ

3.1. Требования к управлению доступом в информационных системах

Требования к управлению доступом в системах необходимо определить и задокументировать. Для обеспечения надлежащего уровня контроля доступа к информационным сервисам и данным и его поддержания следует сформулировать производственные требования к управлению доступом в системах для поставщиков услуг.

Каждый владелец производственного приложения должен сформулировать политику контроля доступа к данным, которая определяет права доступа каждого пользователя или группы пользователей. Эта политика должна учитывать:

- *требования к безопасности отдельных производственных приложений;*
- *правила распространения информации и разграничения доступа.*

Необходимо также принять во внимание соответствующее законодательство и договорные обязательства, касающиеся защиты доступа к данным и сервисам.

Следует рассмотреть возможность создания стандартных профилей полномочий доступа пользователей для общих категорий работ.

Для управления процессом предоставления прав доступа к информационным системам требуются формальные процедуры, которые должны включать все стадии жизненного цикла управления доступом пользователей – от начальной регистрации новых пользователей до удаления учетных записей пользователей, которые больше не нуждаются в доступе к информационным сервисам. Особое внимание следует уделить управлению процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.

3.1.1. Регистрация пользователей

Для управления доступом ко всем многопользовательским информационным системам должна существовать формальная процедура регистрации и удаления учетных записей пользователей.

Доступ к многопользовательским информационным системам необходимо контролировать посредством формального процесса регистрации пользователей, который должен:

- проверять, предоставлено ли пользователю разрешение на использование сервиса владельцем системы;

- проверять, достаточен ли уровень доступа к системе, предоставленый пользователю, для выполнения возложенных на него функций и не противоречит ли он политике безопасности, принятой в организации, например не компрометирует ли он принцип разделения обязанностей;

- предоставлять пользователям их права доступа в письменном виде;

- потребовать от пользователей подписания обязательства, чтобы показать, что они понимают условия доступа;

- потребовать от поставщиков услуг, чтобы они не предоставляли доступ к системам до тех пор, пока не будут закончены процедуры определения полномочий;

- вести формальный учет всех зарегистрированных лиц, использующих систему;

- немедленно изымать права доступа у тех пользователей, которые сменили работу или покинули организацию;

- периодически проверять и удалять пользовательские идентификаторы и учетные записи, которые больше не требуются;

- проверять, не выданы ли пользовательские идентификаторы, которые больше не нужны, другим пользователям.

3.1.2. Управление привилегиями

Использование специальных привилегий следует ограничить и контролировать, так как излишние системные привилегии зачастую оказываются одним из основных факторов, способствующих нарушению режима безопасности систем.

Для многопользовательских систем, требующих защиты от несанкционированного доступа, предоставление привилегий необходимо контролировать посредством формального процесса определения полномочий следующим образом:

- идентифицировать привилегии, связанные с каждым программным продуктом, поддерживаемым системой, например, с операционной системой или СУБД, а также категории сотрудников, которым их необходимо предоставить;

- предоставить привилегии отдельным лицам только в случае крайней необходимости и в зависимости от ситуации, т.е. когда они нужны для выполнения своих функций;

- реализовать процесс определения полномочий и вести учет всех предоставленных привилегий. Не следует предоставлять привилегии до окончания процесса определения полномочий;

- содействовать разработке и использованию системных программ, чтобы избежать необходимости предоставления привилегий пользователям;

- пользователи, которым предоставлены большие привилегии для специальных целей, должны использовать другой пользовательский идентификатор для обычной работы.

3.1.3. Управление пользовательскими паролями

В настоящее время пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Назначение паролей необходимо контролировать посредством формального процесса управления, заключающемся:

- в требовании от пользователей подписания обязательства по хранению персональных паролей и паролей рабочих групп в секрете;

- в выдаче пользователям надежного временного пароля, который они обязаны немедленно сменить, если пароль выбран самим пользователем. Временные пароли также выдаются, когда пользователи забывают свои пароли, и только после положительной идентификации пользователя;

- в передаче временных паролей пользователям надежным способом. Следует избегать передачи паролей через посредников или посредством незащищенных сообщений электронной почты. Пользователи должны подтвердить получение паролей.

3.1.4. Пересмотр прав доступа пользователей

Для обеспечения эффективного контроля за доступом к данным и информационным системам руководство должно реализовывать формальный процесс пересмотра прав доступа пользователей через регулярные промежутки времени. Такой процесс должен обеспечивать:

- пересмотр полномочий доступа пользователей через регулярные промежутки времени; рекомендуется период в 6 месяцев;

- пересмотр разрешения на предоставление специальных привилегированных прав доступа через более короткие промежутки времени; рекомендуется период в 3 месяца;

- проверку предоставленных привилегий через регулярные промежутки времени, чтобы не допустить получения пользователями несанкционированных привилегий.

3.1.5. Рекомендации по использованию паролей

Пароли являются основным средством подтверждения полномочий доступа пользователей к автоматизированным системам. Предлагаются следующие рекомендации по выбору и использованию паролей:

- назначать индивидуальные пароли для обеспечения подотчетности;

- хранить пароли в секрете;

- не записывать пароли на бумаге, если не представляется возможным ее хранение в защищенном месте;

- изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей;

- выбирать пароли, содержащие не менее шести символов;

- изменять пароли через регулярные промежутки времени (приблизительно через 30 суток) и избегать повторного или «циклического» использования старых паролей;

- чаще изменять пароли для привилегированных системных ресурсов, например пароли доступа к определенным системным утилитам;

- изменять временные пароли при первом входе в системы;

- не включать пароли в сценарии автоматического входа в системы, например в макросы или функциональные клавиши.

При выборе паролей не следует использовать:

- месяцы года, дни недели и т.п.;

- фамилии, инициалы и регистрационные номера автомобилей;

- названия и идентификаторы организаций;

- номера телефонов или группы символов, состоящие из одних цифр;

- пользовательские идентификаторы и имена, а также идентификаторы групп и другие системные идентификаторы;

- более двух одинаковых символов, следующих друг за другом;

- группы символов, состоящие из одних букв.

Если пользователям необходим доступ ко многим сервисам и платформам и от них требуется поддержание нескольких паролей, то им следует рекомендовать использовать один надежный пароль для входа во все системы, которые обеспечивают минимальный уровень защиты для хранения паролей.

3.1.6. Управление доступом к сети

Подключения к системам, объединенным в сеть, следует контролировать. Это необходимо для того, чтобы подключенные пользователи и компьютерные системы не нарушали защиту других сетевых сервисов. Средства контроля должны включать:

- соответствующие интерфейсы между сетевыми сервисами;
- механизмы аутентификации удаленных пользователей и оборудования;
- контроль доступа пользователей к информационным системам.

3.1.7. Предоставление ограниченных услуг

Доступ к сети и компьютерным системам, осуществляемый пользователем с конкретного терминала, должен предоставляться в соответствии с политикой управления доступом, принятой в организации. В частности, пользователям следует предоставить только прямой доступ к сервисам, использование которых им разрешено.

Данное средство контроля является особенно важным для сетевых подключений к конфиденциальным или критически важным производственным приложениям, а также для пользователей в зонах повышенного риска, например, в общедоступных местах или местах, находящихся вне пределов досягаемости администраторов безопасности организации.

3.1.8. Принудительная маршрутизация

В ряде случаев путь от пользовательского терминала к компьютерной системе необходимо контролировать. Современные сети предоставляют максимальные возможности для коллективного использования ресурсов и гибкость маршрутизации. Эти особенности также дают возможность несанкционированного доступа к производственным приложениям или незаконного использования информационных систем. Такой риск можно уменьшить, привлекая средства контроля для ограничения маршрута между

пользовательским терминалом и компьютерными системами, доступ к которым пользователю разрешен, т.е. создавая принудительный маршрут.

Цель такой принудительной маршрутизации – предотвратить нежелательное «отклонение» пользователей от маршрута между пользовательским терминалом и системами, доступ к которым пользователю разрешен. Для этого обычно требуется реализация ряда средств контроля в нескольких точках пути. Принцип состоит в том, чтобы ограничить возможности выбора маршрута в каждой точке сети посредством предопределенных вариантов.

Примерами такого ограничения пути являются:

- предоставление выделенных линий связи или телефонных номеров;
- автоматическое подключение портов к определенным прикладным системам или шлюзам безопасности;
- ограничение возможностей выбора маршрута с помощью системы меню и подменю для отдельных пользователей;
- предотвращение неограниченного «перемещения» по сети.

В основе требований к принудительной маршрутизации должна лежать политика управления доступом, принятая в организации.

3.1.9. Контроль сетевых подключений

Для удовлетворения требований политики управления доступом к определенным производственным приложениям коллективно используемые сети, особенно те из них, которые выходят за пределы границ организации, могут потребовать реализации средств контроля для ограничения возможности подключения пользователей. Такой контроль может быть осуществлен посредством межсетевых шлюзов, которые фильтруют передаваемые по сети данные с помощью предопределенных таблиц и правил. В основе ограничений на подключение пользователей должна лежать политика управления доступом к производственным приложениям.

Примерами таких ограничений являются:

- пересылка только электронной почты;
- односторонняя передача файлов;
- двухсторонняя передача файлов;
- интерактивный доступ;
- доступ к сети только в определенное время суток или в определенную дату.

3.2. Идентификация и аутентификация в системах разграничения доступа

3.2.1. Идентификаторы пользователей

Для отслеживания действий отдельных лиц всем пользователям необходимо присвоить уникальные персональные идентификаторы. Пользовательские идентификаторы не должны указывать на уровень привилегий пользователя, например администратор, наблюдатель и т.п.

В исключительных ситуациях, в случае явных преимуществ для организации можно использовать общий пользовательский идентификатор для группы пользователей или конкретного задания. Такие случаи должны быть утверждены руководством и документированы. Для обеспечения подотчетности могут потребоваться дополнительные средства контроля.

3.2.2. Автоматическая идентификация терминалов

Для аутентификации подключений к конкретным узлам сети следует рассмотреть возможность автоматической идентификации терминалов. Автоматическая идентификация терминалов – это средство, используемое для тех приложений, для которых важно, чтобы сеанс связи можно было инициировать только с конкретного терминала. Идентификатор, присвоенный терминалу, можно использовать для указания того, разрешено ли конкретному терминалу инициировать сеанс связи или производить определенные действия.

Для обеспечения безопасности терминального идентификатора, возможно, потребуется физическая защита терминала.

3.2.3. Аутентификация пользователей

Несанкционированный доступ к производственным приложениям может быть осуществлен посредством внешнего подключения к компьютерам организации через общедоступные сети или сети, не принадлежащие организации. Поэтому необходима аутентификация подключений, осуществляемых удаленными пользователями через общедоступные (или не принадлежащие организации) сети.

Аутентификация может выполняться на уровне компьютера, поддерживающего приложение, или на сетевом уровне. Для определения необходимого уровня аутентификации, возможно, потребуется оценка рисков и непосредственного ущерба от реализации угроз для организации.

Как на сетевом уровне, так и на уровне компьютера аутентификацию удаленных пользователей можно осуществлять с помощью, например, систем оперативного реагирования на проблемы и шифрования линии связи. Использование выделенных частных линий связи или средства проверки сетевых адресов пользователей также дает уверенность в источнике подключений.

3.2.4. Аутентификация узлов сети

Несанкционированный доступ к производственному приложению может быть осуществлен посредством автоматического подключения удаленного компьютера, поэтому необходимо аутентифицировать подключения удаленных компьютерных систем. Это особенно важно, если подключение осуществляется через открытую сеть, находящуюся вне пределов досягаемости администраторов безопасности организации.

Аутентификацию можно выполнять на уровне компьютера, поддерживающего приложение, или на сетевом уровне. Для определения

требований к аутентификации удаленных систем, возможно, потребуется оценка рисков и непосредственного ущерба от реализации угроз для организации. На сетевом уровне аутентификация удаленной системы может быть осуществлена посредством аутентификации узлов сети с помощью, например, систем оперативного реагирования на проблемы или шифрования линии связи. Использование выделенных частных линий связи или средств проверки сетевых адресов пользователей также дает уверенность в источнике подключений.

Аутентификация узлов сети может также служить в качестве альтернативного, менее дорогостоящего средства аутентификации групп удаленных пользователей в случае, когда они подключены к защищенной, совместно используемой компьютерной системе.

4. СИСТЕМЫ ОХРАНЫ ПЕРИМЕТРА

4.1. Задачи охраны периметра

Основная задача охраны периметра – обнаружить нарушителя во время преодоления линии периметра и локализовать до того, как его действия смогут нанести вред охраняемому объекту.

Для охраны периметра необходимо:

- оборудовать контролируемый периметр инженерными заграждениями;
- оборудовать контролируемый периметр техническими средствами охраны;
- организовать реагирование сил физической охраны на несанкционированные действия нарушителя.

4.1.1. Задачи создания инженерных заграждений

Перечислим указанные задачи:

- предотвращение неумышленного несанкционированного проникновения на охраняемую территорию случайных лиц;
- предотвращение неумышленного несанкционированного выхода людей за пределы охраняемой территории;
- создание временной задержки при умышленном несанкционированном проникновении на охраняемую территорию;
- создание временной задержки при умышленном несанкционированном выходе за пределы охраняемой территории.

4.1.2. Задачи, решаемые при оборудовании периметра техническими средствами охраны

Основные:

- обнаружение факта попытки проникновения нарушителя;

- определение места проникновения нарушителя;

- оповещение группы реагирования.

Дополнительные:

- оптимизация действий группы реагирования (формирование рекомендаций по реагированию в конкретной ситуации, включение освещения участков, на которых обнаружены действия нарушителей);

- психологическое воздействие на нарушителя (формирование звуковых и световых сигналов тревоги, передача в зоне деятельности нарушителя голосовых сообщений по громкоговорящей связи и т.п.).

4.2. Концепция охраны периметра объекта связи

Разработка концепции в ходе предпроектного обследования дает возможность на начальном этапе провести всесторонний анализ разнородных данных о состоянии сооружений и оборудования периметра территории объекта.

Концепция охраны периметра может являться самостоятельным документом в том случае, когда система охраны периметра (СОП) на предприятии является доминирующей, а остальные системы (система объектовой сигнализации, система контроля и управления доступом, система охранного телевидения) входят в ее состав фрагментами. В противном случае разрабатываемые разделы «Концепции охраны периметра объекта» должны входить в состав разделов общей концепции охраны предприятия, дополняя их в части, ее касающейся.

Концепция представляет собой документ внутреннего использования, отражающий систему взглядов собственника на облик будущей системы охраны периметра и содержащий совокупность сведений, объединенных в следующие разделы:

- модель периметра;

- модель угроз;

- тактика охраны периметра.

4.2.1. Модель периметра

Раздел содержит сведения, характеризующие текущее состояние зоны периметра предприятия. Под зоной периметра понимается часть территории предприятия вдоль ее периметра (в виде кольца), ограниченная с внешней стороны внешним ограждением предприятия, а с внутренней стороны – внутренним ограждением либо указателями ее внутренней границы. В состав зоны периметра предприятия, как правило, входят контрольно-пропускные пункты, внешнее ограждение и зона отчуждения (ее ширина может достигать 3 м), а также расположенные в ней инженерно-технические средства охраны и освещения и т.п. Раздел представляется графической и текстуальной (пояснительной запиской) частью.

Графическая часть – это генеральный план распределенных на местности сооружений предприятия. Наряду с общим планом (при необходимости) могут создаваться и частные планы (схемы, чертежи), детализирующие отдельные его фрагменты. Например, чертежи развертки полотна ограждения или чертежи ворот и калиток, входящих в линию ограждения, и т.п.

Пояснительная записка содержит, как правило, ту часть информации о зоне периметра, которая не может быть отражена на плане, но необходима для составления реалистичной модели периметра.

4.2.2. Модель угроз

Модель угроз представляет собой перечень возможных действий нарушителя по преодолению зоны периметра объекта связи. Определение целей вторжения на территорию предприятия, облика возможного нарушителя и наиболее вероятных сценариев его действий дает возможность сформировать требования к инженерно-техническим средствам системы охраны периметра. Разработка модели угроз выполняется в соответствии с моделью нарушителя, которая принимается как базовая.

При формировании модели угроз в рассматриваемом случае необходимо учитывать только те угрозы охраняемому имуществу предприятия, которые включают несанкционированное преодоление зоны его периметра нарушителем, обладающим возможностями сформированной его базовой модели.

В ходе разработки модели угроз проводится оценка риска при том или ином варианте противодействия планируемой СОП вторжению нарушителя базовой модели с обозначенной целью вторжения.

Завершающим этапом разработки модели угроз является формирование требований к возможностям будущей СОП в виде списка сценариев действий нарушителя базовой модели по преодолению зоны периметра, которые она должна выявить и блокировать. При этом необходимо учитывать возможные воздействия внешних и внутренних случайных факторов, способствующих достижению нарушителем своей цели.

4.2.3. Тактика охраны периметра

Тактика охраны объекта – выбор вида охраны, методов и средств ее реализации. В зависимости от результатов анализа данных рассмотренных выше моделей выбирается вид, структура и состав системы охраны периметра предприятия, соотношение инженерных и технических средств охраны. Определение тактики охраны периметра предприятия рекомендуется проводить в два этапа.

Первоначально необходимо на основе выработанной разработчиками «Концепции рекомендаций» решить ряд стратегических задач, от варианта решения которых будет зависеть инженерно-технический облик СОП.

Результатом этой работы является оформление в разделе «Концепции» взглядов на стратегический облик будущей СОП предприятия, оптимизированный под текущие условия его функционирования, разработанную выше модель угроз. При этом облик будущей СОП должен быть

основан на финансовых и технических возможностях ее реализации как для настоящего момента, так и на ближайшую и дальнейшую перспективы развития предприятия.

На втором этапе осуществляется детализация принятых собственником стратегических решений, заключающихся:

- в планировании оптимального размещения рубежей на плане зоны периметра, оснащенных выбранными видом системы и типом технических средств охраны;

- в выборе варианта и процедур управления режимами для каждого спланированного рубежа зоны периметра предприятия, а также в выборе способа организации и типа средств передачи извещений от систем сигнализации в планируемой СОП;

- в оценке необходимости установки на КПП специального оборудования для досмотра людей и транспорта, контроля за вносом (выносом) и ввозом (вывозом) личных вещей и техники;

- в анализе проводимых строительных работ и их возможных объемов и затрат;

- в оценке списочного состава сотрудников сил охраны по функциональным задачам, в планировании ее кадрового набора, а при необходимости – в организации его обучения (повышение квалификации);

- в выборе вида системы и типа технических средств оповещения дежурных сил охраны, руководства предприятия, а при необходимости – сотрудников предприятия о факте вторжения нарушителя и угрожающем их жизни развитии событий и т.п.

Решение тактических задач при создании СОП в рамках разработки «Концепции» позволяет уйти от технических просчетов и выработать экономически приемлемый вариант защиты имущества от несанкционированного доступа (НСД) нарушителя при вторжении его через зону периметра.

4.3. Инженерные заграждения

Заграждение в составе СОП выполняет роль преграды, изменяющей условия передвижения нарушителя по направлению к охраняемому объекту.

Заграждение представляет собой физический барьер – вид ограждения, препятствующий свободному входу нарушителя на территорию объекта.

Все заграждения в зависимости от назначения можно разделить на четыре типа: сигнализационные, сигнализационно-электризуемые (электрошоковые), строительные (технические) и строительно-сигнализационные.

Сигнализационные ограждения образовывают проводящие металлические конструкции, являющиеся чувствительным элементом периметрового средства обнаружения, которое называется заградительным (перемежающиеся линии колючей проволоки, закрепленные на деревянных или бетонных столбах и включенные в два активных шлейфа, чувствительных к обрыву и короткому замыканию смежных линий).

Сигнализационно-электризуемые заграждения представляют собой систему токонесущих проводов (изолированных от опор), по которой распространяются импульсы высокого напряжения (3…10 кВ), вызывающие болевой шок у нарушителя при касании.

Строительные заграждения весьма разнообразны, их классификация дана на рис. 4.1.

Видимость сквозь заграждение определяется конструкцией, выбираемой в соответствии с пониманием безопасности и эстетики.

Высота заграждения является параметром, который определяет его проходимость, время преодоления, опасность падения, которой подвергает себя нарушитель наверху. 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.

Фундамент (прежде всего ленточный, по всему периметру) является практически обязательной частью заграждения, поскольку:

- обеспечивает меньшую подвижность заграждения при действии сильного ветра, который является существенным помеховым фактором для всех периметровых систем охраны, установленных на заграждении или вблизи него;

- при глубине свыше 50…80 см он обеспечивает достаточно надежную защиту от подкопа;

- способствует большей долговечности всего заграждения.

Рис. 4.1. Строительные заграждения

Выбор полотна и опор заграждения, как правило, определяется с учетом стоимости, строительной нагрузки и конструкции, а также, в большей степени, выполняемой охранной функции.

Важным звеном в КТСО является полоса грунта шириной до 3 м, примыкающая к заграждению с внутренней стороны периметра объекта (полоса

отчуждения). Она предназначена для возможной установки периметровых систем охраны (в том числе и в грунт) и формирования зоны обнаружения, что накладывает ограничения на посадку деревьев, кустов, а также на перемещение людей в этой зоне.

4.4. Технические средства охраны периметра

Любая периметральная система охраны должна отвечать определенному набору критериев, некоторые из которых перечислены ниже:

- возможность раннего обнаружения нарушителя – еще до его проникновения на объект;
- точное следование контурам периметра, отсутствие «мертвых» зон;
- скрытая установка датчиков системы;
- независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т.д.);
- невосприимчивость к внешним факторам «нетревожного» характера – индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы;
- устойчивость к электромагнитным помехам – грозовые разряды, источники мощных электромагнитных излучений и т.п.

Общие признаки средств охранной сигнализации:

- наличие чувствительного элемента (сенсора), обнаруживающего изменение того или иного физического параметра и преобразующего это изменение в электрический сигнал (или изменение сигнала);
- наличие анализатора сигнала, который выделяет представительный параметр, несущий информацию об изменении параметра, (детектирует его) и сравнивает выделенный параметр с пороговым значением или эталоном и в случае превышения порога формирует сигнал тревоги.

Ключевым элементом в системе сигнализации является сенсор. Обнаруживающие свойства сенсоров основаны на самых разных физических

принципах действия. В зависимости от принципа действия, используемого эффекта, параметра, формы, наименования сенсора и других признаков различают и системы обнаружения. Известны сейсмические, емкостные, электродинамические, контактные, резистивные, волоконно-оптические и другие системы. Часть из применяемых систем предполагает создание и установку специальных конструкций, дублирующих ограду по всему периметру. Чувствительные элементы других систем монтируются непосредственно на существующих оградах и не требуют значительных дополнительных строительных работ. Рассмотрим особенности применения некоторых из них.

4.4.1. Геофонные системы

Геофоны – сейсмические датчики (сенсоры) для регистрации колебания почвы в звуковом диапазоне частот, возбужденных на поверхности и в глубине земли. Геофоны обладают высокой чувствительностью. Их чувствительность зависит от направления источника колебаний. Максимальная чувствительность наблюдается в вертикальном направлении (вдоль оси датчика), минимальная чувствительность – в перпендикулярном к оси направлении. Эту особенность учитывают при проектировании и монтаже систем охранной сигнализации.

4.4.2. Кабельные вибрационные системы

В таких системах используют сенсоры в форме кабелей. В некоторых системах используют приспособленные элементы (реальные кабели, выпускаемые промышленностью для иных целей). В других системах используют сенсорные кабели, специально разработанные для целей охранной сигнализации.

В приспособленных элементах для обнаружения вибраций используются, как правило, паразитные эффекты и явления, которые производители стремятся снизить при производстве продукции для ее основного назначения.

На рис. 4.2 показано сечение многожильного телефонного кабеля. Под воздействием вибрации происходит микродеформация кабеля, и изолированные проводники трутся друг о друга. В результате на изоляции наводится объемный заряд и на проводниках образуется разность потенциалов (трибоэффект). Это типичный пример применения в качестве сенсора приспособленного кабеля.

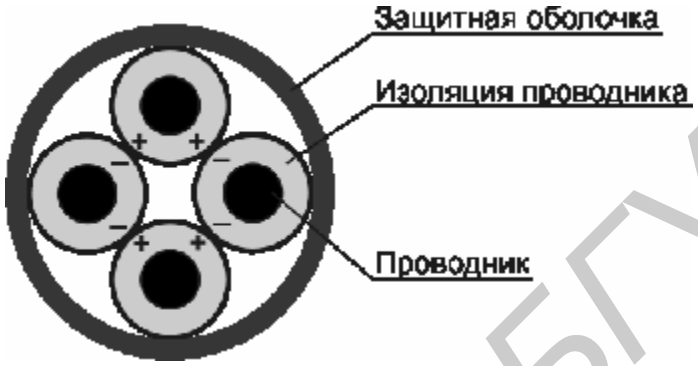

Рис. 4.2. Трибоэффект в многожильном кабеле

Распространены также системы с использованием специально разработанных коаксиальных сенсорных кабелей. Два чувствительных проводника свободно размещаются в специальных углублениях в диэлектрике внутри коаксиального кабеля, в котором создается поле между центральным проводником и экраном (рис. 4.3). При смещении тела кабеля под воздействием вибрации чувствительные проводники, обладающие массой, остаются на месте. На них воздействует изменяющееся электрическое поле, связанное со смещением тела кабеля, и образуется разность потенциалов, которая воспринимается анализатором. Подобные сенсоры относятся к активным сенсорам, так как сами не генерируют сигнал, а требуют внешнего источника сигнала или поля. Отношение сигнала к шуму и стабильность параметров у подобных систем выше, чем у систем, основанных на трибоэффекте.

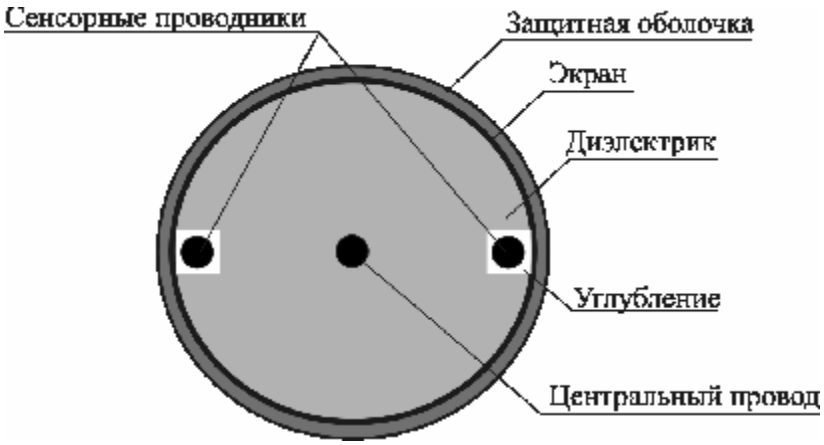

Рис. 4.3. Электростатический сенсор вибраций

Одно из достоинств кабельных вибрационных систем состоит в том, что сенсорным кабелем могут быть защищены ворота и калитки, попадающие в зону охраны. Для этой цели используют комплект для подключения сенсора к воротам, а на створках ворот или калитки крепят петлю сенсора. Один конец петли сенсора на створке ворот с помощью этого комплекта электрически соединяется с сенсорным кабелем, прикрепленным к ограде. Другой конец петли подключается к фидерному кабелю, который пропускается под воротами по обводной трубе и с помощью второго комплекта подключается к петле сенсора на второй створке ворот. Петля сенсора на второй створке ворот, в свою очередь, подключается к сенсору, прикрепленному к ограде уже по другую сторону ворот. Так образуется непрерывная цепь охранной сигнализации в зоне (рис. 4.4).

Рассмотренные кабельные вибрационные системы просты, не требуют зоны отчуждения и удобны в монтаже. Они широко используются для защиты периметра самых разнообразных объектов. Большинство из них успешно действует в самых разных климатических условиях.

Надежная работа вибрационных систем с использованием сенсорных кабелей возможна лишь при выполнении нескольких обязательных условий:

- механические свойства инженерного заграждения должны обеспечивать распространение механических колебаний;

- механические свойства инженерного заграждения должны быть однородны в пределах зоны охраны;

- применяемая система должна быть сопрягаема с данным инженерным заграждением;

- инженерное заграждение не должно служить источником случайных вибраций.

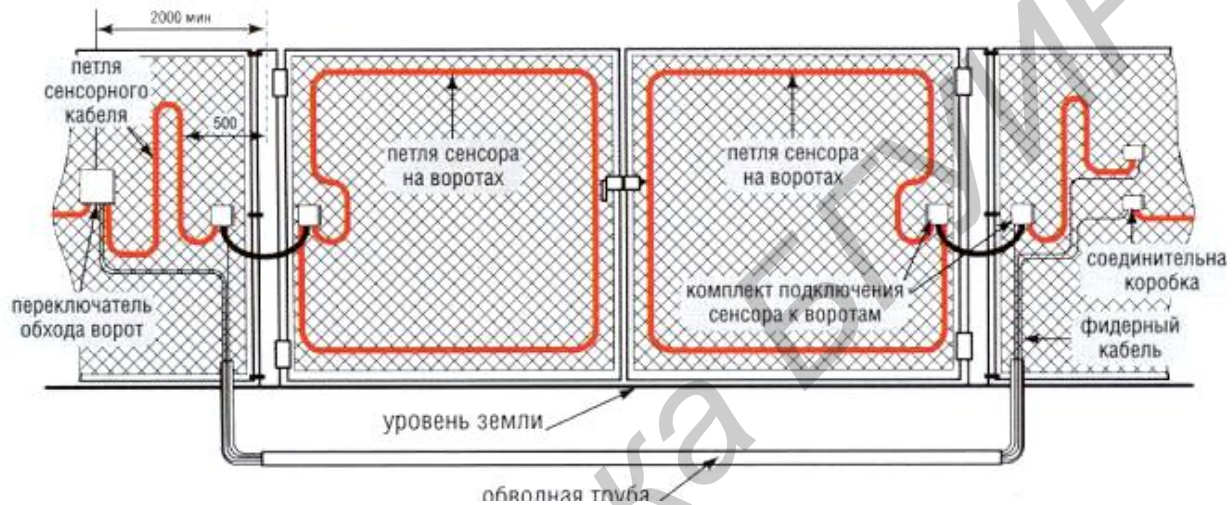

Рис. 4.4. Организация охраны периметра при наличии ворот

Высота ограды должна быть такой, чтобы ее невозможно было преодолеть без касания.

4.4.3. Радиоволновые системы

На некотором расстоянии параллельно друг другу прокладываются два кабеля (две антенны) специальной конструкции (рис. 4.5). Зазоры между разреженными проводами «экрана» своеобразного коаксиального кабеля образуют щелевую антенну. Один из кабелей служит передающей антенной, другой – приемной антенной. При возбуждении первой антенны высокочастотными колебаниями она начинает излучать электромагнитное поле, воспринимаемое второй антенной. При этом приемник, подключенный к приемной антенне, принимает сигнал. Если в окрестности двух антенн

появляется тело определенного объема с диэлектрической и/или магнитной проницаемостью, отличной от проницаемости свободного пространства, электромагнитное поле, воспринимаемое приемной антенной, искажается (изменяются его амплитуда и фаза). Это изменение детектируется и анализируется приемником-анализатором. Если анализируемый сигнал превышает пороговое значение, формируется сигнал тревоги.

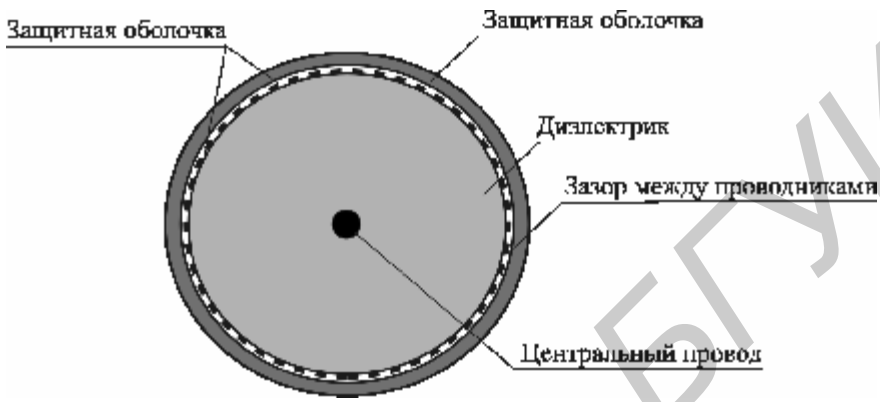

Рис. 4.5. Конструкция кабеля радиоволновой системы

Максимальная чувствительность системы лежит в плоскости, перпендикулярной плоскости расположения кабелей, совпадающей с центральной осью. Минимальная чувствительность системы находится в плоскости расположения кабелей.

Радиоволновые системы требуют зоны отчуждения, поскольку зона их чувствительности выходит за пределы линии ограды. Сигнал тревоги может вызвать и прохожий, идущий вдоль ограды, защищенной радиоволновой системой, и поливальная машина или грузовик с металлоломом, проезжающий по дороге в десяти–пятнадцати метрах от ограды. При расположении кабелей в горизонтальной плоскости (в земле) влияние проезжающего транспорта снижается, поскольку он попадает в зону минимальной чувствительности системы. Конфигурация линии периметра и перепады высот не оказывают влияния на свойства радиоволновых систем. Во избежание образования мертвых зон кабели смежных зон охраны размещают с некоторым перекрытием (2…5 м) в продольном направлении.

4.4.4. Радиолучевые системы

Радиолучевые системы содержат передатчики и приемники с узконаправленными антеннами. Используемый диапазон частот обычно лежит в пределах от 10 до 40 ГГц. Сечение радиолуча в горизонтальной (а) и вертикальной (б) плоскостях показано на рис. 4.6. Рабочей зоной радиолучевых систем считают зону на участке BC. На участке AB луч слишком узкий, и его можно обойти. На участке CD площадь поперечного сечения луча слишком велика по сравнению с площадью потенциального нарушителя, и обнаруживающая способность системы оказывается пониженной. В то же время наличие луча на достаточно протяженном участке CD за пределами рабочей зоны накладывает серьезные ограничения на минимальные размеры зоны отчуждения. При использовании одиночных совмещенных приемопередатчиков типа радиолокаторов зона отчуждения должна превышать размеры участка CD. При разнесении приемника 2 и передатчика 1 по разные концы охраняемой зоны (рис. 4.7, а) требования к зоне отчуждения снижаются, но все же остаются из-за наличия мертвых зон вблизи передатчика и приемника (рис. 4.7, б). Фактически рабочая зона заключена между точками B и B_1, а участки AB и B_1A_1 выходят за пределы охраняемой зоны. Они могут быть отнесены к зонам отчуждения. Мертвые зоны образуются и от затенения радиолуча складками местности и посторонними предметами, расположенными на линии охраны (рис. 4.7, в).

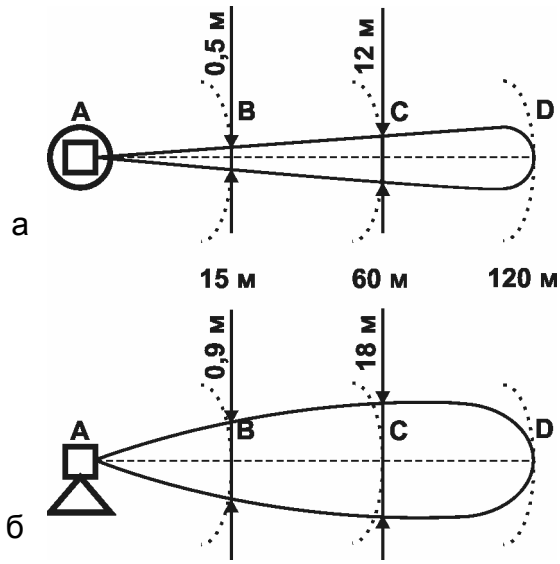

Рис. 4.6. Радиолучевая система

Радиолучевые системы чаще всего используют для контроля протяженных прямолинейных участков, когда имеется достаточно свободного пространства для вынесения приемников и передатчиков за пределы охраняемых зон. Радиолучевые средства обнаружения, как правило, применяются одновременно с другими средствами, которые позволяют закрыть присущие радиолучевым системам мертвые зоны.

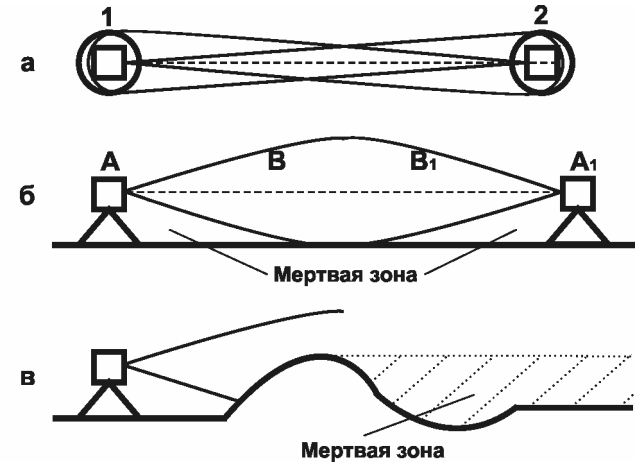

Рис. 4.7. Радиолучевая система с разнесенными приемником и передатчиком:

а – форма диаграмм направленности приемной и передающей антенн в горизонтальной плоскости; б – мертвые зоны, связанные с диаграммой направленности антенн в вертикальной плоскости; в – мертвые зоны, связанные с неровностями почвы и наличием посторонних предметов

4.4.5. Инфракрасные барьеры

Инфракрасные активные средства защиты отличаются от радиолучевых средств диапазоном частот и шириной диаграммы направленности лучей. Площадь сечения луча инфракрасных (ИК) систем значительно меньше, чем у радиолучевых систем. Для обеспечения надежной защиты периметра по высоте используют так называемые инфракрасные барьеры.

Инфракрасные барьеры строят с применением активных ИК-извещателей с разнесенными передатчиками и приемниками. Принцип их действия заключается в следующем. Передатчик излучает электромагнитный поток ИК-диапазона – невидимый луч, который направляется в сторону приемника. В отсутствие препятствий на пути луча приемник воспринимает его и преобразует в электрический сигнал. Изменение интенсивности принимаемого луча при попытке его пересечения детектируется и анализируется процессором приемника. Для создания барьера группу передатчиков и приемников встраивают в стойку, размещая их на различной высоте (рис. 4.8).

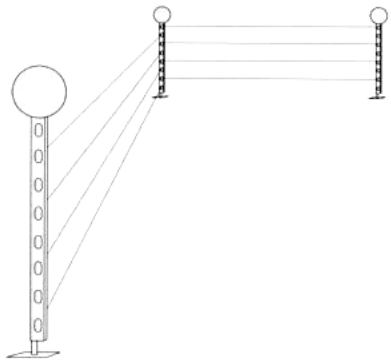

Рис. 4.8. Инфракрасный барьер

Для разделения каналов осуществляют синхронизацию каждого приемника с соответствующим передатчиком. Встроенный процессор позволяет анализировать каждый из сигналов раздельно, группами или в произвольной их комбинации. Это позволяет гибко использовать систему, как в плане логического анализа, так и в плане приспособления к местным условиям. Если пересекается только нижний луч, например, мелким животным, возникает состояние предтревоги, но сигнал тревоги не формируется. Последующее пересечение второго луча уже вызывает сигнал тревоги, так же как и одновременное пересечение двух лучей. Перекрестная синхронизация приемников и передатчиков, расположенных на разной высоте, позволяет обойти мертвые зоны, которые образуются из-за специфики рельефа (рис. 4.9).

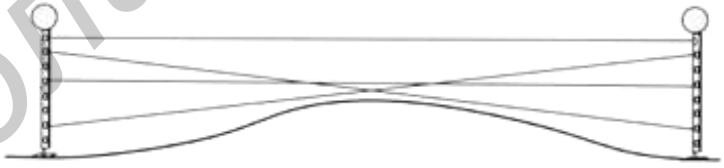

Рис. 4.9. Пример обхода неровности почвы

5. ОХРАННОЕ ТЕЛЕВИДЕНИЕ

5.1. Свет

Свет – электромагнитное излучение, которое вызывает зрительные ощущения. Человек видит окружающие его предметы потому, что они по-разному отражают свет. Интенсивность света, отражаемого или излучаемого поверхностью, определяется яркостью.

Яркость предметов зависит от интенсивности и угла падения света, угла наблюдения предмета, спектрального состава излучения и окраски поверхностей. При одинаковых условиях освещения детали поверхности предметов видны потому, что они отличаются друг от друга по яркости.

Человек обладает цветным зрением. Глаз человека воспринимает электромагнитное излучение с длиной волны 380…760 нм – это видимый диапазон спектра. Различие в длине волны света воспринимается как различие по цветам. Источники света отражают не только свет, воспринимаемый глазом. Свет с длиной волны 100…380 нм называется ультрафиолетовым, а с длиной волны 760…14000 нм – инфракрасным . В свою очередь ИК-диапазон делится на ряд поддиапазонов, которые соответствуют полосам прозрачности атмосферы: 760…1200 нм – ближний ИК-диапазон, 3…5 мкм – средний ИК-диапазон, 8…14 – дальний ИК-диапазон.

Наибольшей чувствительностью глаз обладает к желтовато-зеленым лучам с длиной волны 560 нм. Максимум чувствительности глаза совпадает с максимумом в спектре излучения Солнца. Спектр лучей, которые пропускает морская вода, также практически совпадает с кривой видимости глаза человека.

При наблюдении предметов, не излучающих свет, количество света, воспринимаемое глазом, определяется углом падения света на поверхность предметов и углом наблюдения. Интерпретация отражения света поверхностью является одним из ключевых понятий зрительного восприятия текстуры

поверхности реальных объектов. Не принимая во внимание особенности восприятия зрительного образа в целом, текстура поверхности отражает осязаемые свойства материала объекта: мягкий – твердый, рыхлый – плотный, сплошной – пористый, привлекательный – неприятный.

Угол наблюдения в большей степени определяет общее восприятие предмета. Изображение любого предмета ограничено линиями: прямыми или кривыми. Линию человек видит как множество точек, отличающихся от окружающего их фона.

Таким образом, наличие четкого контура объекта определяется контрастом. Различия в яркости называются яркостным контрастом, а в цвете – цветовым.

Свойство глаза различать контрастность увеличивает объем воспринимаемой информации. Обычно увеличение количества света, отражаемого поверхностью, влечет за собой увеличение контрастности.

5.2. Восприятие света глазом человека

Глаз – один из сложнейших органов человека (рис. 5.1), который вместе с мозгом образуют зрительную систему. Через нее поступает 70…90 % всей информации к человеку.

Зрачок глаза может менять свой диаметр, что позволяет приспосабливаться в широких пределах световых потоков.

Роговица образует переднюю камеру, которая заполнена влагой. Передняя камера и хрусталик образуют оптическую систему с аккомодацией, образующей действительное перевернутое изображение на сетчатке. Плотность хрусталика немного больше плотности воды. Хрусталик состоит из нескольких слоев и может менять свою форму (кривизну передней поверхности), так что меняется действующее фокусное расстояние глаза как оптической системы, т.е. глаз обладает способностью менять свою оптическую силу от 60 диоптрий (при рассматривании удаленных объектов) до 70 диоптрий (близкие предметы).

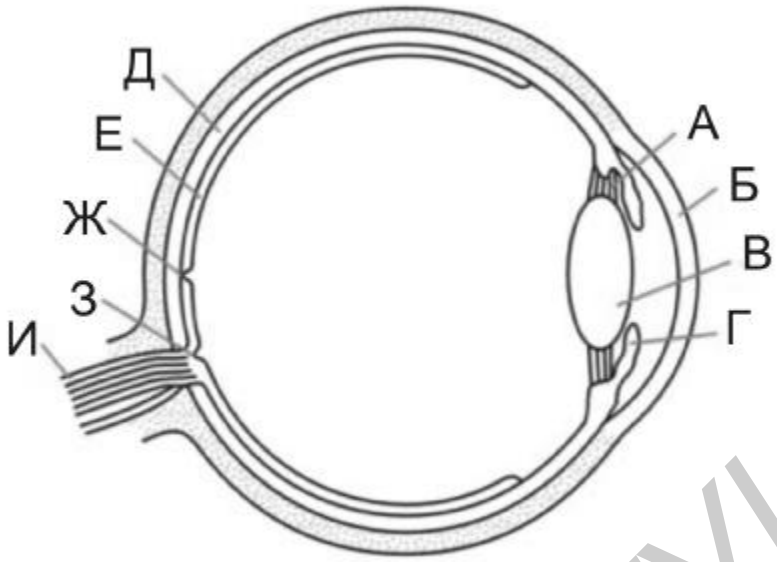

Рис. 5.1. Схема строения глаза человека:

А – мышцы хрусталика; Б – роговая оболочка; В – хрусталик; Г – радужная оболочка; Д – сосудистая оболочка; Е – сетчатая оболочка; Ж – центральная ямка сетчатки; З – слепое пятно; И – зрительный нерв

Сетчатая оболочка (ретина) – переплетение волокон зрительного нерва, которые заканчиваются палочками и колбочками. Объединясь в группы и узлы, они присоединяются к нервным волокнам, на выходе которых создаются импульсы.

Абсолютный порог чувствительности глаза определяется палочковыми рецепторами (сумеречное, скотопическое зрение). Палочки расположены с уменьшением концентрации от зоны максимальной чувствительности к периферии и к центру. Зона максимальной чувствительности находится на расстоянии $10…12^0$ от оси глаза.

Колбочки являются рецептором дневного (фотопического) зрения. Наиболее плотно они располагаются в центральном участке ретины – в желтом пятне, имеющем овальную форму. В центре желтого пятна есть углубление – центральная ямка, где присутствуют только колбочки, и плотность их максимальна. Поэтому это место сетчатки образует наиболее чувствительную по остроте зону.

Колбочки имеют цветовую чувствительность, а палочковый аппарат такой чувствительности не имеет.

Зрительная система человека возбуждается колебаниями в диапазоне длин волн 350…780 нм, вызывающими ощущение света.

Если есть световой поток, имеющий равномерный спектр (одинаковую спектральную плотность) по мощности в диапазоне 380…770 нм, то глаз ощущает белый (серый) цвет. Во всех остальных случаях возникают различные ощущения цвета.

Как всякое поле излучения, электромагнитное излучение можно характеризовать количественными параметрами. Вопросами метрологии электромагнитного излучения в целом занимается радиометрия, изучающая область видимого света. Ее единую методологию можно было бы использовать и для световых измерений. Однако исторически сложилось (именно в силу восприятия человеком области света), что вначале появилась метрология только в области света, которая получила название «фотометрия». Фотометрия – совокупность методов измерения энергетических характеристик электромагнитного излучения и световых величин. Основой фотометрии являются свойства статистически среднего глаза человека.

5.3. Светотехнические единицы

Обычно в качестве основной величины для светотехнических расчетов выбирают световой поток P (F), т.е. мощность потока лучистой энергии, которая измеряется в ваттах [Вт], фотонах в секунду [фотон/с], световаттах [свВт] или люменах [лм].

При λ = 555 нм (зеленый свет) световой поток мощностью 1 Вт создает световое ощущение в 683 лм. Это световое ощущение и называется 1 свВт. Для других длин волн мощность в световаттах всегда меньше мощности, выраженной в ваттах, потому что

$$P[\text{свВт}] = P[\text{Вт}] \cdot n, \qquad (5.1)$$

где n – коэффициент видности, меньший 1 для всех длин волн, кроме зеленого света, когда он равен 1.

Сила света I определяется как величина светового потока ΔF в единичном телесном угле Δω, т.е. является плотностью светового потока в пространстве:

$$I = \frac{\Delta F}{\Delta \omega}, \qquad (5.2)$$

где Δω=1 стерадиан.

Сила света измеряется в канделах [кд] $1\,\text{кд} = \frac{1\,\text{лм}}{1\,\text{стер}}$.

Кандела – сила света, испускаемого с площади 1/600 000 м^2 сечения полного излучателя в перпендикулярном к этому сечению направлении при темепературе затвердевания платины (2042 К) и давления 101 325 Н/м^2.

Яркость – характеристика светящихся тел, равная отношению силы света в каком-либо направлении к площади проекции светящейся поверхности на плоскость, неперпендикулярную к этому направлению. Измеряется в канделах на метр квадратный [кд/м^2]:

$$L = \frac{I}{S}, \qquad (5.3)$$

где S – площадь светящейся поверхности.

Освещенность – величина светового потока, падающего на единицу поверхности, измеряется в люксах [лк]:

$$E = \frac{F}{S}. \qquad (5.4)$$

5.4. Черно-белое и цветное телевидение

Телевидение – область науки, техники, культуры, связанная с передачей на расстояние изображений объектов и звукового сопровождения (речи,

музыки) при помощи радиосигналов (эфирное телевидение) или электрических сигналов, передаваемых по проводам (кабельное телевидение). Принцип телевидения состоит в последовательном преобразовании во времени элементов изображения в электрические сигналы (анализ изображения), передаче этих сигналов по каналам связи в пункт приема и обратном их преобразовании в видимое изображение (синтез изображения).

Исторически телевидение развивалось, начиная с передачи только яркостной характеристики каждого элемента изображения (черно-белое телевидение). К началу 50-х гг. XX-го века в США, России и затем в других странах были разработаны системы цветного телевидения электронного типа. В современных стандартных системах цветного телевидения (например, SECAM, PAL), совместимых с черно-белыми, передаются одновременно два вида сигналов: сигнал яркости, несущий информацию о яркости передаваемой сцены; сигнал цветности (образован двумя так называемыми цветоразностными сигналами), несущий информацию о ее цвете.

Цвет – очень важная и сложная проблема в охранном телевидении. Хотя многие все еще предпочитают монохромные камеры, которые имеют более высокую чувствительность и реагируют на невидимый инфракрасный спектр, цветные камеры получают все более широкое распространение. Цвет дает ценную дополнительную информацию о наблюдаемых объектах. Но важнее то, что человеческий глаз фиксирует цветовую информацию быстрее, чем мелкие детали объекта. Недостатком цветной камеры являются плохие эксплуатационные показатели в условиях слабой освещенности. Однако постоянное усовершенствование технологии приборов с зарядовой связью (ПЗС) значительно улучшает работу цветной камеры при минимальном освещении.

Идея создания цветов в телевизоре заключается в смешении путем сложения (аддитивном) соседних люминесцентных точек трех основных

цветов. Эти точки очень малы и представляют собой элементы маски экрана монитора.

Фактическое смешивание цветов происходит тогда, когда смотрят на монитор с оптимального расстояния (в пару метров), и глаз воспринимает итоговый цвет каждой из этих трех точек. При аддитивном смешении цвет получается путем покрытия электронно-лучевой трубки (ЭЛТ) люминофором, и сложение цветов делает итоговый цвет ярче. Например, чтобы получился белый цвет, должны присутствовать все три цвета в соответствующей пропорции. Таким образом, итоговые цвета возникают в результате сложения основных цветов.

5.5. Цветовая температура и источники света

Цветовая температура – это температура, до которой нагрето воображаемое абсолютно черное тело, излучающее свет вследствие нагрева.

Согласно физической теории спектр света, произведенного нагреванием, зависит главным образом от температуры тела, а не от материала. Это важнейшее утверждение было доказано Максом Планком, который вывел формулу, объясняющую взаимосвязь между максимальными длинами излучаемых волн и температурой, до которой нагрето тело:

$$\lambda_m = \frac{2896}{T}, \qquad (5.5)$$

где λ_m – длина волны,

T – температура в градусах Кельвина.

Максимальные значения различных температур находятся вне видимого спектра, т.е. в инфракрасной области (рис. 5.2). Для нити накаливания из вольфрама рабочая цветовая температура приблизительно равна 2800 К, и больше чем 3/4 энергии излучается в инфракрасной области в виде теплового излучения. Тепло – это не что иное как инфракрасный свет.

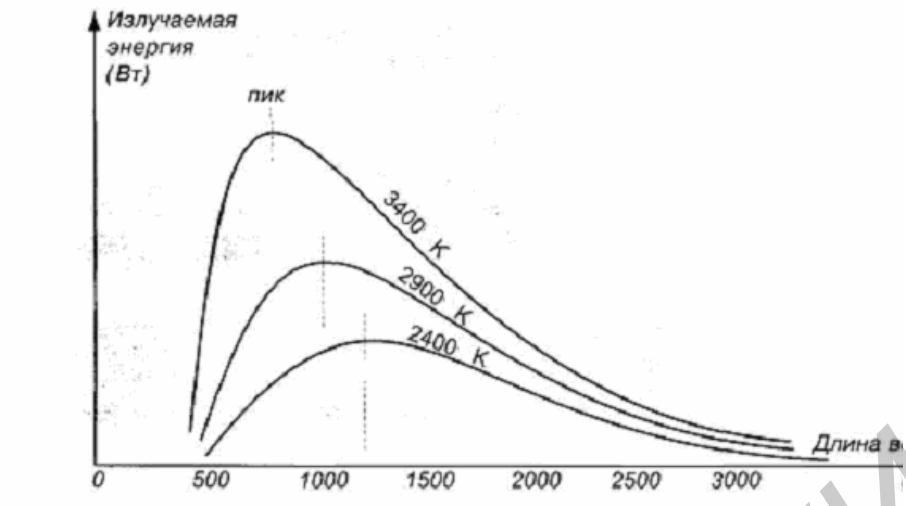

Рис. 5.2. Спектральная характеристика черного тела при различных температурах

Вольфрамовые лампы годятся для ч/б камер, так как они более чувствительны к инфракрасной части спектра. Цветным камерам нужно обеспечивать компенсацию желтого/красноватого цвета, производимого источником света в 2800 К. В фотоаппаратах это компенсируется синими (дополнительный цвет) оптическими фильтрами, помещенными непосредственно на объектив, тогда как в электронных камерах это делается с помощью электроники: информация об основных цветах меняется до определенного процентного соотношения.

Солнце как естественный источник света имеет очень высокую физическую температуру, но эквивалентная цветовая температура света, получаемая на поверхности Земли, колеблется в зависимости от времени суток и погодных условий. Это происходит в результате отражения и преломления света в атмосфере. Чем ниже цветовая температура, тем более красными будут снимки, и чем выше цветовая температура, тем больше будет синего цвета.

В целях получения контрольной точки и правильного воспроизведения цветов были определены стандартные источники белого света. На практике используется несколько стандартов. Эти стандартные источники белого света обозначаются как A, B, C, D6500 и W.

5.6. ПЗС-видеокамеры

Основной принцип работы ПЗС заключается в сохранении информации электрических зарядов в фотоэлементах, а затем, когда потребуется, передаче этих зарядов на выходной каскад.

ПЗС-видеокамеры (рис. 5.3) обладают многими преимуществами (конструктивными) перед видеокамерами с передающими трубками:

Рис. 5.3. Внешний вид видеокамеры SF-1092

- пригодность для всех профессиональных задач по наблюдению, обеспечению безопасности и контроля;
- длительная работа без износа и последующих затрат;
- высокая стабильность оптических и электрических параметров;
- надежная продолжительная работа в течение длительного времени благодаря применению долгоживущих компонентов;
- отсутствие заправок и повреждений от переэкспозиции;
- отсутствие «смазывания» изображения при подвижных снимаемых объектах;
- отсутствие влияния магнитных и электрических полей;
- съемка с точностью оригинала без геометрических искажений;
- высокая устойчивость к ударам и вибрациям;
- стандартизированные крепление объектива, видео- и системные разъемы.

5.6.1. Критерии выбора камеры

Почти все современные ПЗС-камеры удовлетворяют важнейшим требованиям, которые ставятся перед видеокамерами:

- пригодность для продолжительной работы;
- сопрягаемость со всеми современными передающими системами и системами дистанционного управления;
- удобство использования;
- отличное соотношение цена/производительность.

Кроме этого, имеются технические характеристики и свойства, в отношении которых всегда должны приниматься индивидуальные решения:

- черно-белая или цветная камера;
- разрешение;
- чувствительность;
- чувствительность в инфракрасной области;
- компенсация пиковой засветки;
- возможность внешней синхронизации;
- внешнее влияние внутреннего контура регулирования.

При использовании этих критериев решения должны приниматься не в пользу камер с самыми лучшими техническими характеристиками, а исходя из экономических соображений в пользу достаточных для решения проблем характеристик. Таким образом экономятся значительные средства и в то же время достигаются желаемые результаты.

5.6.2. Цветная и черно-белая камеры

Доминирующими сегодня однозначно являются черно-белые камеры. Основания для этого – повышенная светочувствительность черно-белых камер и возможность применения при инфракрасном освещении.

Превосходство поколения цветных камер становится особенно ясным при съемке самых светлых и темных участков и при ограничении пиковой засветки,

т.к. разрешение (резкость деталей) у черно-белых камер выше, чем у цветных камер.

При правильно установленной гамма-коррекции хорошая черно-белая камера может воспроизводить на соответствующем мониторе приблизительно 25 различных полутонов.

5.6.3. Разрешение, чувствительность

Разрешение – размер воспроизводимых деталей – резкость изображения, снимаемого камерой.

Горизонтальное разрешение определяется как число вертикальных линий (рассчитывается из общей ширины изображения), которое камера явно может воспроизвести.

Разрешение в решающей степени определяется числом элементов изображения (пикселей) и последующей процессорной техникой, а также форматом матричного светочувствительного элемента (сенсора) (2/3, 1/2, 1/3 дюйма).

Проектировщик должен в принципе определить не формат сенсора, а необходимое для решения конкретной задачи горизонтальное разрешение. Далее приведены некоторые численные значения горизонтального разрешения и их оценки.

Горизонтальное разрешение 200…400 линий – оценка «удовлетворительно». Достаточно для всех стандартных применений, при которых должны хорошо распознаваться объекты, отдельные люди или события в зонах съемки на близкой средней дальности (от 2 до 25 м).

Горизонтальное разрешение 400…500 линий – оценка «хорошо». Подходит для применений, при которых требуется очень хорошая распознаваемость во всех зонах съемки.

Горизонтальное разрешение более 500 линий – оценка «отлично». Для профессиональных применений, при которых требуется высокая способность распознавания деталей во всех зонах съемки.

Цветным камерам можно поставить более высокую оценку за счет дополнительно цветовой информации при том же числе линий разрешения. Чувствительность определяется минимальной освещенностью в люксах, при которой ПЗС-камера еще выдает нужное изображение. При 2865 К на объективе измеряется отраженная от объекта освещенность, при которой амплитуда видеосигнала с камеры составляет 50 % от нормальной. Хотя при такой освещенности помехи уже оказывают влияние на изображение, оно еще может быть признано удовлетворительным.

5.6.4. Чувствительность в ИК-диапазоне длин волн

Для выполнения определенных задач от камеры требуется чувствительность в инфракрасной области. Это может быть необходимо, например, там, где нужно избежать дополнительного освещения наблюдаемого объекта (здания, территории и т.п.), ослепления участников движения или где по другим причинам необходимо скрытое наблюдение. Если подсветить такую зону наблюдения невидимым для глаза инфракрасным светом, то съемка с использованием подходящих для этого камер может проводиться в темноте так же, как и при дневном свете.

5.6.5. Ограничение пиковой засветки

ПЗС-камеры имеют недостаток, который называется Smear-эффектом. Он проявляется при очень слабом освещении снимаемой сцены в форме светлых вертикальных линий от верхней до нижней границы изображения, которые проходят через каждый источник света, попавший в поле зрения камеры. Это могут быть, например, прожектор поезда, уличные фонари, свет карманного фонаря и т.п. или сильно отражающие плоскости в солнечном свете при дневной работе.

Smear-эффект возникает благодаря физически обусловленному процессу переноса заряда в ПЗС-сенсоре и может быть подавлен путем применения совершенной коммутационной техники в периферийной электронике.

При выборе ПЗС-камер необходимо учитывать критерий ограничения пикового света – подавления Smear-эффекта – в зависимости от их применения. Самостоятельное ночное применение камер младшего класса с достаточной чувствительностью при наличии пиковых источников света было бы неверным.

5.6.6. Возможность синхронизации

Если в видеоустановке сигналы с камер должны переключаться с помощью средних или матричных коммутаторов, рекомендуется применение камер с возможностью синхронизации. Таким образом, связывая камеры с современным коммутационным оборудованием, избегают мешающего срыва кадровой синхронизации в момент переключения. Подходящими для этого являются камеры, тактовый генератор которых может фазироваться от имеющегося напряжения сети переменного тока, причем исходной точкой является переход фазового напряжения через нуль.

Для этого вида синхронизации не надо никаких дополнительных затрат на кабели, а необходима только однократная фундаментальная юстировка при первом пуске. Для определенных типов камер также возможны общая кадровая и строчная синхронизации. Такой режим может быть достигнут следующим образом:

- для всех камер строчные и кадровые синхроимпульсы или композитная синхропоследовательность поступают от центрального тактового генератора;

- полный (цветной) телевизионный сигнал от одной камеры передается для синхронизации на все другие камеры.

Общая строчная и кадровая синхронизации требуются только тогда, когда сигналы камер должны поступать на электронный делитель изображения или в дальнейшем должны быть обработаны на микшерном оборудовании. Для

работы на коммутационном оборудовании с цифровой обработкой изображений, таких, как, например, квадраторы и мультиплексоры, синхронизация камер не требуется.

5.6.7. Внешние воздействия на внутренние регулировки

Для особенно критичных системных применений может возникнуть необходимость прямого или дистанционного воздействия на внутренние регулировки. В зависимости от типа камеры могут быть включены следующие функции:

- гамма-коррекция;
- контурная коррекция;
- компенсация пиковой засветки;
- автоматическая регулировка усиления (АРУ);
- автоматическая регулировка уровня «черного».

При этом нужно также исходить из экономических соображений при необходимости, определенной применением.

5.6.8. Фокусное расстояние объектива

Объективы с большим фокусным расстоянием, например, 50, 75 или 100 мм (телеобъективы), имеют относительно малую область глубины резкости, так что при их использовании необходима по возможности точная установка дальности до объекта.

С уменьшением фокусного расстояния, например 6 мм (широкоугольный объектив), увеличивается область глубины резкости. Это увеличение заходит даже так далеко, что для короткофокусных объективов (4,8; 3,5 мм) глубина резкости достигает от 10 см до бесконечности, так что такие объективы совсем не требуют установки дальности.

5.6.9. Установка диафрагмы

Область глубины резкости определяется через установленный раскрыв диафрагмы. Малый раскрыв диафрагмы (соответствует большим ее значениям, например 8–16–22) определяет большую глубину резкости. Большой раскрыв диафрагмы (соответствует малым ее значениям, например 1,4–1,2–0,95) определяет очень малую глубину резкости.

5.7. Видеомониторы

Видеомонитор воспроизводит поступающий с видеокамеры сигнал после того, как он пройдет через средства передачи видеосигналов и устройства коммутации (рис. 5.4). Видеокамера может быть высочайшего качества, с высокой разрешающей способностью, но если видеомонитор не способен воспроизвести сигнал равным или лучшим образом, то вся система потеряет в качестве.

Рис. 5.4. Внешний вид видеомонитора SP 717A

В охранном телевидении так же, как и в телевещании, большинство видеомониторов выполнено на кинескопах, т.е. устройствах, действующих на основе технологии электронно-лучевых трубок, которые преобразуют электрическую информацию видеосигнала в визуальную. Сегодня существует множество альтернатив кинескопам: жидкокристаллические мониторы (ЖК),

плазменные панели, проекционные и т.п., но наиболее популярны все же видеомониторы на кинескопах.

Видеомониторы в охранном телевидении подразделяются на две основные группы: черно-белые и цветные. По рекомендациям ТВ-стандартов между черно-белыми и цветными видеомониторами должна сохраняться совместимость. Другими словами, черно-белый видеосигнал может быть воспроизведен на цветном видеомониторе, а цветной сигнал – на черно-белом видеомониторе. Черно-белые видеомониторы характеризуются более высокой разрешающей способностью (поскольку имеют одно непрерывное люминесцентное покрытие), а цветные видеомониторы дают ценную информацию о цветах объектов. Какой фактор более важен – зависит от применения. Например, для видеосистемы распознавания номерных знаков важнее высокое разрешение, и поэтому лучшим выбором будет черно-белая видеосистема камера/монитор, а в других случаях, когда, скажем, требуется идентификация личности, лучше выбрать цветную видеосистему.

Видеомониторы характеризуются размерами диагонали экрана, обычно выраженными в дюймах, иногда в сантиметрах. Черно-белые видеомониторы бывают самых разных размеров, чаще всего используются 9 дюймов (23 см) и 12 дюймов (31 см). Видеомониторы меньших размеров – 5 дюймов (13 см) и 7 дюймов (18 см) – не очень удобны, за исключением разве что систем заднего обзора, видеопереговорных систем, а также для регулировки заднего фокуса объективов. Большие мониторы чаще всего используются с видеомультиплексорами, доступны следующие размеры: 15 дюймов (38 см), 17 дюймов (43 см) и 19 дюймов (48 см).

5.7.1. Настройка видеомонитора

На передней панели видеомониторов обычно имеется четыре регулятора: **строчная синхронизация** (horizontal hold), **кадровая синхронизация** (vertical hold), **яркость** (brightness) и **контрастность** (contrast).

Эффект от настройки **строчной синхронизации** похож на сдвиг картинки влево или вправо. Если фаза строчной развертки установлена слишком далеко, то в крайнем положении регулятора изображение становится неустойчивым и строчная синхронизация срывается. Аналогичный эффект может проявиться в случае, если мал размах строчных синхроимпульсов или они искажены при передаче по слишком длинному коаксиальному кабелю (падение напряжения, вызванное значительным сопротивлением, и завал высоких частот из-за значительной емкости). Последний эффект не может быть компенсирован регулировкой строчной синхронизации. Этой регулировкой можно только центрировать изображение.

Регулятор **кадровой синхронизации** настраивает фазу кадрового синхроимпульса. Это может потребоваться для компенсации различного положения кадровых синхроимпульсов от разных видеокамер. Обычно видеомонитор настраивается на один видеосигнал, так что изображение остается стабильным. Однако если несколько несинхронизированных видеосигналов последовательно переключаются на данный видеомонитор, может проявиться нежелательный эффект, который называется **picture roll** (медленное перемещение изображения по вертикали). Это самый нежелательный эффект в охранном телевидении. Это также означает, что различные видеомониторы имеют разное время синхронизации (вхождения в синхронизм).

В охранном телевидении наиболее распространенным типом систем являются системы с переключением нескольких видеокамер на один видеомонитор.

Системы типа одна видеокамера – один видеомонитор используются очень редко. Не только потому, что это дорого, но и потому, что это не практично. Прежде всего, требуется дополнительное физическое пространство для размещения мониторов, но самое главное, оператор не может долго концентрировать внимание сразу на нескольких видеомониторах.

Однако для небольших видеосистем подобная конфигурация имеет право на жизнь, т.к. у нее ряд неоспоримых преимуществ: отсутствует неконтролируемое время на переключение, нет оцифровки с присущими ей недостатками, а «живучесть» системы намного выше, поскольку легко диагностировать и заменить неисправный элемент.

Контрастность позволяет настраивать динамический диапазон электронного луча, что повышает и понижает контрастность изображения (диапазон от черного до белого). Обычно это делается тогда, когда меняются условия освещенности в помещении, где установлены мониторы.

Яркость отличается от регулировки контрастности: она поднимает или снижает уровень постоянной составляющей тока электронного луча, сохраняя тот же динамический диапазон. Этой настройкой пользуются в том случае, когда воспроизведение тонов видеосигнала выглядит неестественно.

Яркость и контрастность настраиваются так, чтобы зритель увидел максимально возможное количество деталей. Чем слабее свет в помещении с видеомониторами, тем ниже установка контрастности. Снижение контрастности улучшает четкость изображения (меньше сечение электронного луча) и продлевает время жизни кинескопа. Иногда не удается хорошо настроить яркость и контрастность, особенно при переключении различных видеокамер с разными видеосигналами. Для объективной регулировки яркости и контрастности следует использовать тестовый генератор телевизионных сигналов, дающий сигнал градаций яркости – таблицу с равномерно распределенными уровнями серого. После чего контрастность и яркость настраиваются таким образом, чтобы все ступени были одинаково хорошо различимы. После такой настройки можно объективно судить о яркости и контрастности видеокамеры.

Еще два регулятора – **линейность** (linearity) и **размер по вертикали** (picture height) – обычно находятся на задней стенке видеомонитора.

Линейность настраивает линейность кадровой развертки, что отражается на вертикальной симметрии изображения. Если линейность не настроена соответствующим образом, круги принимают яйцеобразную форму. Для настройки линейности видеомонитора потребуется тестовый генератор телевизионных сигналов.

Размер по вертикали позволяет настроить изображение по высоте. Если высота не настроена, круги окажутся эллиптическими. Затрагивается также и размер растра (он уменьшается или увеличивается), что косвенным образом изменяет разрешающую способность по вертикали.

Большинство видеомониторов имеет регулировку фокусировки электронного луча **(focus)**, обычно он находится внутри видеомонитора, поблизости от высоковольтного блока. Этот регулятор настраивает сечение электронного луча в месте контакта со слоем люминофора, влияя на четкость изображения. На некоторых видеомониторах этот регулятор расположен на передней панели и называется **aperture**.

На цветных видеомониторах есть регулятор **цвет (color)**, позволяющий увеличивать или уменьшать насыщенность цвета в цветовом сигнале. Он отличается от регулировки яркости. Цветные видеомониторы особо чувствительны к статическим и другим внешним электромагнитным полям, т.к. воспроизведение цвета в сильной степени зависит от точности динамического сведения трех электронных лучей (красного, зеленого, синего).

5.8. Устройства обработки видеосигналов

Самое простое и наиболее широко распространенное устройство, используемое в небольших и средних видеосистемах, – это последовательный видеокоммутатор.

Поскольку в большинстве систем охранного телевидения видеокамер больше, чем видеомониторов, то требуется устройство, последовательно

переключающееся с сигнала одной видеокамеры на сигнал другой. Такое устройство называется **последовательным видеокоммутатором**.

При помощи органов настройки данного устройства может быть изменено время наблюдения. Наиболее распространенная и целесообразная установка времени наблюдения составляет 2…3 с. Более короткое время слишком непрактично и будет утомлять глаза оператора, а более длительное время сканирования может привести к потере информации с тех видеокамер, которые не отображались в это время на экране.

Кроме классификации по количеству видеовходов последовательные коммутаторы можно классифицировать по наличию или отсутствию входов тревоги. В качестве источников сигнала тревоги могут служить различные устройства тревожной сигнализации.

Матричный видеокоммутатор (Video Matrix Switcher – VMS) является мозгом системы и входит в состав больших систем охранного телевидения.

Если расположить на схеме видеовходы против видеовыходов, то получим матрицу – отсюда и название «матричный» – это электронные переключатели, которые в любой момент могут подключить любой вход к любому выходу, сохраняя при этом режим согласования нагрузки. Так, один видеосигнал может быть выбран одновременно более чем на одном выходе. А несколько входов могут быть выбраны для переключения по одному выходу, только в этом случае получим последовательное переключение между несколькими входами, т.к. иметь более одного видеосигнала на одном выходе в один момент времени невозможно.

Таким образом, матричный видеокоммутатор по существу представляет собой большой последовательный коммутатор с рядом усовершенствований:

- VMS может контролироваться несколькими операторами;

- VMS обрабатывают сигналы со многих видеовходов и подают их на большое число выходов, но, что наиболее важно, их число может быть легко расширено просто добавлением модулей;

- в состав VMS входят цифровые контроллеры для управления поворотными устройствами и объективами. Клавиатура обычно имеет встроенный джойстик или кнопки, служащие управляющими элементами;

- VMS генерирует код идентификации видеокамеры, время, дату, имя оператора системы, сообщения тревоги в блоке выводимой на экран информации, накладываемой на видеосигнал;

- VMS имеет множество входов и выходов тревоги и может быть расширен до практически любого их количества.

Видеоквадратор помещает изображение от четырех (или менее) видеокамер на один экран, разделенный на четыре прямоугольные области, по аналогии с прямоугольной системой координат иногда называемые квадрантами. Для решения этой задачи видеосигнал вначале должен быть оцифрован, а затем сжат до размера соответствующего квадранта. Электроника прибора приводит все синхроимпульсы к единой временной базе, в результате формируется единый видеосигнал, в котором представлены сигналы всех четырех квадрантов, поэтому нет необходимости во внешней синхронизации.

Естественная эволюция устройств цифровой обработки изображений сделала видеомультиплексоры лучшей альтернативой видеоквадраторам, особенно для записи. **Видеомультиплексоры** – это устройства, выполняющие временное мультиплексирование входных видеосигналов и дающие два типа выходных видеосигналов: один для просмотра и один для записи.

Выход для видеонаблюдения позволяет показывать изображения со всех видеокамер на одном экране одновременно. Например, при использовании 9-канального видеомультиплексора с 9 видеокамерами все они будут представлены на экране в виде мозаики 3 x 3 (мультиэкранное отображение). В большинстве видеомультиплексоров любая видеокамера может быть выбрана для полноэкранного отображения.

Видеодетекторы движения (Video Motion Detector – VMD) – это устройства, анализирующие поступающие на вход видеосигналы и

определяющие наличие изменений в видеосигнале; в случае их появления активируется выход тревоги.

Быстро развивающаяся технология обработки изображений позволяет запоминать и обрабатывать изображения в течение очень короткого времени. Если время обработки равно или меньше 1/50 с (PAL) или 1/60 с (NTSC), что, как известно, равно скорости обновления «живого» видео, то можно обрабатывать изображение без потери полей и сохранить видимость «движения в реальном времени».

Устройства видеопамяти. Концептуально устройство видеопамяти – это очень простое электронное устройство, предназначенное для временного хранения изображений. Две его основные части – это аналого-цифровой преобразователь и оперативное запоминающее устройство (RAM). Первая часть осуществляет преобразование аналогового видеосигнала в цифровой код, который затем сохраняется в ОЗУ до тех пор, пока подключено питание.

Главным преимуществом устройства видеопамяти в сравнении с видеомагнитофонами является время отклика. Так как устройство не содержит механических частей, то запись изображений при активации тревоги выполняется мгновенно. Затем информация передается на видеопринтер или видеомонитор для просмотра или проверки.

Видеопринтеры обычно используются в больших системах, когда необходимо получать твердые копии «живого» или записанного изображения для их последующей оценки или использования в качестве свидетельства. Есть два типа видеопринтеров: черно-белые и цветные. В черно-белых видеопринтерах выходным носителем обычно служит термографическая бумага, но более дорогие модели могут выводить печать на обычную бумагу. Видеопринтеры с термографической бумагой, используемые для вывода черно-белого сигнала, работают так же, как и факсимильные аппараты: размер и разрешение выводимых изображений зависят от разрешения принтера. Отпечатки, сделанные на термографических принтерах, не долговечны и не

стабильны (из-за старения термографической бумаги), и для длительного хранения приходится фотокопировать отпечатанные изображения.

5.9. Устройства видеозаписи

Концепция видеозаписи на магнитную ленту в **бытовых видеомагнитофонах VHS** (Video Home System) основана на спиральном сканировании. В этом случае видеоголовки располагаются на наклонном барабане, вращающемся со скоростью, равной частоте кадров, то есть 25 оборотов в секунду для системы PAL и 30 – для системы NTSC. Необходимая скорость движения ленты относительно головки достигается главным образом вращением головки барабана.

Первоначально в конструкции бытовых видеомагнитофонов VHS фактически использовались две видеоголовки, расположенные под углом 180° друг к другу. Они монтировались на вращающемся цилиндре, называемом барабаном видеоголовок. Таким образом, когда производится запись или воспроизведение, каждая головка записывает или воспроизводит одно телевизионное поле. Видеолента охватывает барабан на 180°, таким образом, одна из двух видеоголовок всегда находится в контакте с лентой.

Однако применение бытовых видеомагнитофонов VHS в охранном телевидении вызывает многочисленные неудобства:

- отсутствие встроенных времени и даты в записываемый видеосигнал;
- отсутствие входов для внешних датчиков тревоги;
- максимальное время записи может быть достигнуто в режиме длительного воспроизведения, который не превышает 10 ч (PAL) или 8 ч (NTSC).

Видеомагнитофоны с прерывистой записью. Time Lapse (TL) видеомагнитофоны – особая категория видеомагнитофонов, которые были разработаны специально для индустрии безопасности.

Основное отличие TL-видеомагнитофонов VHS от бытовых видеомагнитофонов состоит в следующем.

TL-видеомагнитофоны могут производить запись продолжительностью до 960 ч на 180- (PAL) или 120-минутную ленту (NTSC). Это достигается с помощью шагового двигателя, который позволяет перемещать ленту с дискретным шагом, в то время как барабан видеоголовок непрерывно вращается. Обычно вплоть до режима 12-часовой записи лента перемещается с постоянной скоростью, после которого, начиная с режима «24 часа», она движется дискретными шагами. Время, прошедшее между последовательными кадрами, увеличивается при выборе более длительного режима.

Когда TL-видеомагнитофон делает запись в TL-режиме, события не записываются в режиме реального времени, поскольку каждую секунду не записываются 50 полей (60 для NTSC). Соответствующее воспроизведение напоминает видеовоспроизведение в режиме паузы, происходящее короткими, но регулярными интервалами. TL-видеомагнитофоны могут записывать и воспроизводить запись в любом режиме независимо от того, в каком режиме она была сделана.

5.10. Средства передачи видеосигнала и дополнительное оборудование

5.10.1. Средства передачи видеосигнала

Изображение, зафиксированное объективом и видеокамерой и затем преобразованное в электрический сигнал, поступает на коммутатор, видеомонитор или записывающее устройство. Для того чтобы видеосигнал попал из видеокамеры в монитор, он должен пройти через передающую среду.

Самыми распространенными средствами передачи видеоинформации в охранном телевидении являются:

- коаксиальный кабель;

- кабель витой пары;

- микроволновая связь;

- радиочастотная передача (эфирная);

- связь с помощью инфракрасного излучения;

- телефонная линия;

- оптико-волоконный кабель.

Для видеопередачи чаще всего используется коаксиальный кабель, но все большую популярность приобретает волоконная оптика, благодаря ее превосходным характеристикам. Также можно использовать смешанные средства передачи, например микроволновую передачу видеосигнала и передачу управляющих поворотным устройством и трансфокатором данных через витую пару.

5.2.10. Поворотные устройства

Фиксированные видеокамеры устанавливаются на кронштейне, при этом используются объективы с фиксированным фокусным расстоянием, а зона обзора видеокамеры находится в строго определенном направлении.

Альтернативой фиксированным видеокамерам являются видеокамеры (рис. 5.5), положение которых в пространстве можно изменять (с помощью поворотного устройства). Такая видеокамера помещается на способную поворачиваться платформу, при этом обычно используются вариообъективы, так что весь комплекс может поворачиваться в горизонтальной и вертикальной плоскостях, увеличивать изображение объектов и осуществлять фокусировку.

Рис. 5.5. Внешний вид видеокамеры с очистителем, установленной на поворотном устройстве

С точки зрения применения выделяются 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. Они несут более тяжелый кожух, а часто еще и дополнительные устройства (омыватель, очиститель, инфракрасный осветитель).

Внутренние поворотные устройства используются только в условиях, защищенных от внешних факторов, особенно от дождя, ветра и снега. 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 устройства.

5.10.3. Купольные поворотные устройства

Имеется и другое направление в области поворотных устройств, которые по их внешнему сходству с куполами называют купольными поворотными устройствами (скоростные поворотные видеокамеры) (рис. 5.6). Главная черта этих устройств – высокая скорость поворота, что обеспечивается за счет малой массы собственно видеокамеры.

Рис. 5.6. Купольное поворотное устройство с установленной видеокамерой ACV-301QPT

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.

5.10.4. Поворотные устройства с предустановкой

Такие устройства имеют встроенные переменные резисторы, которые механически соединены с каждым электродвигателем. Также резисторы подключены к электронике приемника сигналов телеуправления. К каждому резистору подводится низкое напряжение (около 5 В постоянного тока), а с его движка снимается напряжение, зависящее от угла наклона или поворота платформы поворотного устройства, благодаря чему конкретная позиция

поворотного устройства может быть запомнена. Затем производится отработка к этому значению, либо по введенной вручную команде, либо автоматически по сигналу тревоги.

Например, если дверь защищена датчиком открывания дверей, при его срабатывании можно заставить видеокамеру автоматически поворачиваться в этом направлении, увеличивать изображение и фокусироваться на ранее зафиксированной позиции.

Число сохраняемых предустановок в блоке управления поворотным устройством (приемнике сигналов телеуправления) зависит от самой конструкции, но обычно оно равно 8, 10, 16 или 32.

6. ОРГАНИЗАЦИЯ ЗАЩИТЫ ОБЪЕКТА СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1. Категории объектов

Категория охраняемого объекта – комплексная оценка состояния объекта, учитывающая его экономическую или иную, например культурную, значимость в зависимости от концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны. Результат оценки может быть выражен качественно или количественно. Примером качественных оценок служат так называемые перечневые классификаторы (список категорий объектов с краткими пояснениями). Приведем классификацию, основанную на оценке ущерба от реализации угроз (табл. 6.1).

К категории А следует отнести особо важные объекты, на которых возможный ущерб в случае реализации основных угроз безопасности максимален по характеру и по масштабам. Его последствия выходят за пределы территории объектов и не могут быть локализованы в пространстве и во времени за счет принятия немедленных ликвидационных мер. Характер ущерба заключается в создании угрозы для жизни и здоровья персонала и населения, а также в негативном воздействии на природную среду.

К категории Б предлагается отнести важные объекты, на которых характер возможного ущерба заключается в угрозе для жизни и здоровья персонала объекта, а его последствия не выходят за пределы территории объекта и могут быть локализованы путем принятия ликвидационных мер. К этой же категории предлагается отнести объекты, возможный ущерб на которых носит материальный характер, но его масштабы имеют региональное значение.

Таблица 6.1

Классификация объектов

Категория	Наименование категории	Ущерб или последствия от осуществления угроз	Назначение или принадлежность объектов
А	Особо важные	Особо крупный или невосполнимый материальный ущерб, экологическая катастрофа на объекте или в регионе, гибель большого числа людей на объекте или в регионе, политические последствия, утечка государственных секретов, другие особо тяжкие последствия	Хранилища и депозитарии банков, предприятия по производству или хранилища химически опасных, наркотических и взрывчатых веществ, боеприпасов, ядерных материалов; предприятия оборонного профиля; правительственные учреждения; энергетические комплексы
Б	Важные	Значительный материальный или финансовый ущерб, угроза здоровью или жизни людей, утечка государственных или коммерческих секретов	Кассовые залы банков, подъезды инкассаторских машин; помещения для хранения и работы с конфиденциальной информацией; крупные торговые центры; производственные помещения
В	Прочие	Материальный или финансовый ущерб; информационный ущерб; нарушение комфортности личной жизни или служебной деятельности	Магазины, служебные помещения, офисы, производственные помещения, жилые помещения

Прочие объекты (категория В) характеризуются тем, что возможный ущерб носит локальный и в основном материальный характер и по масштабу может иметь как региональное, так и международное значение.

В свою очередь, каждую категорию объектов можно классифицировать по масштабу или размеру нанесенного ущерба в результате несанкционированного доступа (НСД) нарушителей.

Например, особо важные объекты предлагается дополнительно разделить на три группы безопасности (№1, 2, 3). Номер группы определяет масштаб возможного ущерба, который может иметь последствия, соответственно трансграничного, государственного, регионального значений.

Для других категорий объектов можно использовать предложенную в табл. 6.2 классификацию по группам значимости и уровням защищенности. При этом следует заметить, что при установлении уровня защищенности необходимо дополнительно учитывать возможные угрозы безопасности для конкретного объекта, которые определяются в основном сложившейся криминогенной обстановкой в данном регионе.

Принадлежность объекта к соответствующей категории и группе необходимо определять на начальной стадии проектирования системы информационной безопасности (СИБ), т.к. от этого зависит не только уровень его защищенности, но и планируемая тактика действий сил охраны. От этой тактики зависят общие затраты на создание СИБ.

Разница в тактике действий сил охраны должна учитываться в процессе создания СИБ: при определении структуры, количественного состава и оснащенности сил охраны, а также при выборе типов и взаимного расположения инженерных средств задержки нарушителя. Оптимизация структуры СИБ по критерию «эффективность–стоимость» позволяет обеспечить достаточно эффективную защиту объекта от НСД нарушителей при минимальных затратах ресурсов.

6.2. Классификация помещений и территории объекта связи

К вопросу классификации служебных помещений с точки зрения их безопасности существует несколько подходов. Учитывая, что степень безо-

Таблица 6.2

Классификация территории и помещений объекта связи

Категория зоны	**I**	**II**	**III**	**IV**	**V**	**VI**
Наименование зоны	Свободная зона	Наблюдаемая зона	Регистрационная зона	Режимная зона	Зона усиленной защиты	Зона высшей защиты
Пример функциональ ного назначения	Места свободного посещения	Комнаты приема посетителей	Кабинеты сотрудников	Секретариат, подразделения множительной оргтехники, компьютерные залы, архивы	Материальны е склады	Кабинеты высших руководителей, комнаты для ведения конфиденциальн ых переговоров, специальные хранилища
Условия доступа сотрудников	Свободный	Свободный	Свободный	По служебным удостоверения м или идентификацио нным картам	По спецдокумен там	По спецдокументам
Условия доступа посетителей	Свободный	Свободный	Свободный с регистрацией по удостоверениям личности	По разовым пропускам	По спецпропуска м	По спецпропускам
Наличие охраны	Есть	Есть	Есть	Усиленная охрана	Усиленная охрана	Усиленная охрана
Наличие технических средств охраны	Нет	Средства наблюдения	Охранная сигнализация	Охранная сигнализация, система контроля доступа	Охранная сигнализация (два рубежа), система контроля доступа, механическое усиление	Охранная сигнализация (два рубежа), система контроля доступа, защита утечки информации, механическое усиление

пасности от перечисленных выше угроз тесно связана, прежде всего, с режимом пребывания в помещениях сотрудников и посетителей, целесообразно проводить классификацию по степени режимных ограничений и возможности

доступа в них. Предлагается все помещения и территорию разбить на шесть категорий или зон, представленных в табл. 6.2.

I. Свободная зона – это помещения и прилегающая территория, доступ в которые свободен для любой категории лиц. За этими территориями не ведется наблюдение и там не размещено никаких технических средств охраны и безопасности. Примером такой зоны может быть бюро пропусков, справочное бюро и др.

II. Наблюдаемая зона – это помещения и территория, доступ в которые также не ограничен, но за ними ведется систематическое наблюдение силами службы безопасности или охраны. Наблюдение может вести лицо, находящееся в данном помещении или в других помещениях, с помощью оптических или телевизионных приборов. Типичным примером может служить вестибюль объекта, территория служебной автостоянки и др.

III. Регистрационная зона – зона, вход в которую свободен для любого желающего при условии, что он предъявит для регистрации документ, удостоверяющий его личность. Такая система часто используется в учреждениях, работающих с большим числом клиентов.

IV. Режимная зона – зона, на входе в которую находится пост охраны. Проход допускается либо по пропускам установленной формы, либо по именным заявкам лиц, имеющих соответствующее право.

V. Зона усиленной защиты – это, как правило, помещения, куда допускаются только сотрудники предприятия, а для посторонних лиц доступ туда возможен только по специальным пропускам или в сопровождении уполномоченных лиц. Такого рода помещения, как правило, оборудуются средствами контроля доступа и охранной сигнализацией. Вход в эту зону может также контролироваться постом охраны.

VI. Зона высшей защиты – зона, вход в которую ограничен не только для клиентов и посетителей, но и для собственных сотрудников, не имеющих прямого отношения к данным помещениям. Хорошим примером могут служить

помещения высшего руководства или помещения, связанные с хранением и обработкой особо ценной и конфиденциальной информации. Зона высшей защиты оборудуется инженерно-техническими средствами, приборами контроля и наблюдения и дополнительными постами охраны.

Представленные шесть категорий режимности помещений практически способны охватить все варианты функционального назначения служебных помещений. Отметим факторы, регламентирующие помещение по одной из вышеуказанных категорий:

- условия доступа сотрудников предприятия;
- условия доступа клиентов и посторонних лиц;
- наличие и вид физической охраны;
- виды использования технических средств наблюдения и охраны.

Кроме этого, нанесение на план здания банка, например, категорий режимности всех помещений позволит наглядно увидеть все недостатки в распределении помещений по функциональному назначению. Наиболее оптимальным способом распределения помещений является компактное размещение в одном месте помещений одной и той же категории. При этом желательно, чтобы между собой соседствовали зоны одинаковых или не слишком различающихся категорий. Например, попасть в помещение IV зоны можно только из помещения III или V зоны. Это позволит наиболее экономным способом разместить средства инженерного усиления строительных конструкций и технические средства безопасности.

6.3. Охрана объекта связи

Для того чтобы организация охраны объекта связи была оптимальной, прежде всего необходимо определить задачи, которые эта система должна решать, и четко сформулировать все функции, подлежащие выполнению персоналом в процессе охраны. В самом общем виде задачи, возлагаемые на систему охраны, могут быть следующие:

- осуществление контроля за территорией, зданиями и помещениями объекта связи;

- поддержание установленного режима работы объекта связи и посещения его клиентами и посторонними людьми;

- осуществление противопожарной инспекции зданий и помещений;

- охрана имущества и ценностей, находящихся в помещениях объекта связи;

- выполнение предписанных ей функций в чрезвычайных ситуациях;

- выполнение специальных поручений руководства, предусмотренных должностными обязанностями.

Охрана любого объекта обеспечивается оптимальным сочетанием технических средств и охранников. Посты охраны, в свою очередь, могут быть классифицированы как по функциональному назначению, так и по степени своей уязвимости. По своему назначению посты охраны делятся на следующие виды:

- стационарный пост (выполняет охранные функции, предусматривающие несение службы на конкретном месте (пост проверки документов, досмотр транспортных средств на КПП и т.д.);

- обходной (патрульный) пост выполняет функции по охране территории, группы помещений, периметров зданий, участков местности и т.д. Осуществляет патрулирование по заданному маршруту и, как правило, по жесткому временному графику. Часто наряду с охранными функциями обходному посту поручают инспекционные функции, например, контроль противопожарной безопасности, проверку стационарных постов;

- сопровождающий пост (выполняет функции по охране людей или грузов на маршрутах следования);

- пост наблюдения (разновидность стационарного поста, но с задачей держать в поле зрения большое количество объектов с помощью технических средств);

- пост «тревожная группа» (организуется на предприятиях с большим числом охраняемых объектов, с задачей локализовать случаи нарушения режима охраны по сигналу тревоги от других постов).

Основное назначение поста охраны – не допустить нежелательных действий на территории объекта любых лиц (кражи, нападения с целью ограбления, проникновения со взломом, несанкционированного посещения помещений с ограниченным доступом и т.д.). Однако реально такое противодействие поста ограничено, например, в силу своих возможностей, в использовании оружия, как правило, недостаточно подготовлен к вооруженному сопротивлению и, наконец, пост охраны не всегда готов к добросовестному выполнению своих обязанностей по разным причинам. Вот почему весьма важно точно квалифицировать возможности постов физической охраны для успешного планирования мероприятий по поддержанию должного уровня безопасности на объекте. Посты физической охраны можно классифицировать по степени их уязвимости от внешних угроз и соответственно наличия средств защиты, как это показано в табл. 6.3.

Таблица 6.3

Классификация постов охраны

Тип поста	**П0**	**П1**	**П2**	**П3**	**П4**	**П5**
1	2	3	4	5	6	7
Огнестрельное оружие	—	—	—	+	+	+
Холодное оружие	—	+	+	—	—	+
Спецсредства	—	+	+	+	+	+

Окончание табл. 6.3

1	2	3	4	5	6	7
Средства индивидуальной защиты	—	—	+	+	+	+

Средства связи	—	—	+	+	+	+
Тревожная сигнализация	—	—	+	+	+	+
Средства контроля	—	—	—	—	+	+
Пулезащитное ограждение	—	—	—	—	—	+

1. Огнестрельное оружие – это служебное или гражданское огнестрельное оружие, разрешенное Законом «Об оружии» для использования ведомственными или частными охранниками.

2. Холодное оружие – аналогично предыдущему.

3. Специальные средства – это средства, разрешенные к применению в соответствии с законодательством.

4. Средства индивидуальной защиты – бронежилеты, защитные шлемы, маски и перчатки, щиты.

5. Средства связи – портативные радиостанции для подвижных постов, телефоны прямой связи для стационарных постов.

6. Средства тревожной сигнализации – индивидуальные малогабаритные носимые средства подачи сигнала тревоги охранником при нападении на него или в другой чрезвычайной ситуации. Также это может быть разновидность устройств, подающих сигнал тревоги при невыполнении охранником предписанных ему действий в заданном промежутке времени (например нажатие специальных кнопок).

7. Средства контроля – технические средства в распоряжении охранников, позволяющие им производить гласный или негласный контроль за посетителями или подозрительными лицами (например, детекторы на обнаружение оружия, взрывчатых веществ, радиоактивных материалов и т.д.).

8. Пулезащитные ограждения – инженерные сооружения, позволяющие охраннику выполнять свои функции, но при этом защищающие его от поражения огнестрельным стрелковым оружием (например, защитные кабины, пуленепробиваемые окна, двери и др.).

6.4. Инфраструктура информационной безопасности

Чтобы инициировать и контролировать процесс обеспечения информационной безопасности, необходимо создать в организации соответствующую структуру управления.

В организации должны проводиться регулярные совещания руководства для разработки и утверждения политики безопасности, распределения обязанностей по обеспечению защиты и координации действий по поддержанию режима безопасности.

6.4.1. Совещание руководства по проблемам защиты информации

Ответственность за обеспечение информационной безопасности несут все члены руководящей группы. Поэтому руководству организации необходимо регулярно проводить совещания, посвященные проблемам защиты информации, чтобы вырабатывать четкие указания по этому вопросу, а также оказывать административную поддержку инициативам по обеспечению безопасности. Если вопросов по защите информации недостаточно для повестки дня специальных совещаний, необходимо периодически рассматривать эти проблемы на одном из регулярно проводимых в организации совещаний.

Обычно на подобных совещаниях рассматриваются следующие вопросы:

- анализ и утверждение политики информационной безопасности и распределение общих обязанностей;

- отслеживание основных угроз, которым подвергаются информационные ресурсы;

- анализ и слежение за инцидентами в системе безопасности;

- утверждение основных инициатив, направленных на усиление защиты информации.

6.4.2. Распределение обязанностей по обеспечению информационной безопасности

Необходимо четко определить обязанности по защите отдельных ресурсов и выполнению конкретных процессов обеспечения безопасности.

Политика информационной безопасности должна давать общие рекомендации по распределению функций и обязанностей по защите информации. Там где необходимо, следует дополнить эти рекомендации более подробными разъяснениями, касающимися конкретных систем или сервисов; в этих дополнениях нужно четко определить ответственных за конкретные ресурсы (как физические, так и информационные) и за процессы обеспечения защиты, например за планирование бесперебойной работы организации.

Защита информационной системы должна быть обязанностью ее владельца. Владельцы информационных систем могут делегировать свои полномочия по защите отдельным пользователям-администраторам или поставщикам услуг. Тем не менее, владельцы все равно несут ответственность за обеспечение безопасности системы.

Чтобы избежать каких-либо недоразумений, касающихся отдельных обязанностей, крайне важно четко определить зоны ответственности каждого администратора и, в частности, следующее:

- различные ресурсы и процессы обеспечения безопасности, связанные с каждой системой, необходимо идентифицировать и четко определить;

- кандидатура администратора, отвечающего за каждый ресурс или процесс обеспечения защиты, должна быть согласована, а его обязанности документированы.

Уровни полномочий необходимо четко определить и документировать.

6.4.3. Процесс утверждения информационных систем

Следует определить процедуру утверждения новых информационных систем руководством, чтобы гарантировать, что установка оборудования имеет определенную цель для организации, обеспечивает достаточный уровень защиты и не оказывает вредного влияния на безопасность существующей инфраструктуры.

Необходимо рассмотреть два уровня полномочий по утверждению систем:

- утверждение руководством. Каждый случай установки систем должен быть утвержден соответствующим руководством, которое дает разрешение на ее проведение. Необходимо также получить разрешение от администратора, отвечающего за поддержание режима локальной информационной безопасности; это гарантирует, что установка систем будет соответствовать политике безопасности и требованиям к ней;

- техническое утверждение. В случае необходимости следует проверить, все ли устройства, подключенные к коммуникационным сетям или сопровождаемые конкретным поставщиком услуг, имеют тип, который был утвержден.

6.4.4. Рекомендации специалистов по информационной безопасности

Каждая организация, крупная или мелкая, может извлечь пользу из рекомендаций, даваемых специалистами по безопасности. В идеале в штатном расписании организации должна быть предусмотрена соответствующая должность, и ее должен занимать опытный специалист.

Следует так подобрать специалистов по защите информации и сотрудников службы поддержки, чтобы обеспечить решение любой проблемы, касающейся информационной безопасности. Качество их оценок угроз системе безопасности и рекомендуемые ими меры противодействия будут определять эффективность программы обеспечения информационной безопасности в организации. Для обеспечения максимальной эффективности такой программы

этим специалистам должен быть предоставлен прямой доступ к администраторам информационных систем и руководству организации.

В подозрительных случаях нарушения защиты следует как можно раньше обратиться к консультанту по вопросам обеспечения информационной безопасности или в службу поддержки, чтобы получить необходимые указания или ресурсы для расследования таких инцидентов.

6.5. Классификация ресурсов и их контроль

Ответственность за ресурсы позволяет обеспечить их надлежащую защиту. Следует определить владельцев основных ресурсов и назначить ответственных за реализацию соответствующих защитных мер. Ответственность за реализацию защитных мер может быть передана другому лицу, однако назначенный владелец ресурса все равно несет ответственность за него.

Инвентаризация ресурсов помогает убедиться в том, что обеспечивается их эффективная защита, кроме того, перечень ресурсов может потребоваться для других производственных целей, например, при принятии мер по охране здоровья и по технике безопасности, для страхования или финансовых целей. Инвентаризацию необходимо провести для всех основных ресурсов, связанных с каждой информационной системой. Каждый ресурс должен быть четко идентифицирован, а его владелец и категория секретности согласованы и документированы. Примерами ресурсов, связанных с информационными системами, являются:

- информационные ресурсы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, операционные процедуры и процедуры поддержки, планы обеспечения бесперебойной работы организации, процедуры перехода на аварийный режим;

- программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

- физические ресурсы: компьютеры и коммуникационное оборудование, магнитные носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения;

- сервисы: вычислительные и коммуникационные сервисы, другие технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха).

Категории секретности следует использовать, чтобы показать необходимость в защите и задать приоритеты для ее обеспечения.

Различная информация имеет разную степень конфиденциальности и важности. Некоторые виды информации могут потребовать дополнительной защиты или специального обращения. Систему классификации информации по категориям секретности необходимо использовать для определения соответствующего набора уровней защиты и для уведомления пользователей о необходимости специального обращения с этой информацией.

Категории секретности и связанные с ними защитные меры для производственной информации должны учитывать производственную необходимость в коллективном использовании информации или ограничении доступа к ней, а также ущерб для организации, связанный с НСД или повреждением информации. В частности, следует рассмотреть необходимость обеспечения следующих мер:

- конфиденциальности;

- целостности;

- доступности.

Ответственность за присвоение категории секретности конкретному виду информации, например, документу, файлу данных или дискете, а также за периодическую проверку этой категории, следует возложить на лицо, создавшее эти данные, или на их назначенного владельца.

Секретная информация и выходные данные систем, поддерживающих секретную информацию, должны иметь соответствующие грифы секретности.

Однако часто информация перестает быть конфиденциальной через некоторый промежуток времени, например, когда она становиться общедоступной. Это следует принять во внимание, т.к. чрезмерное засекречивание информации может привести к неоправданным, дополнительным затратам организации.

Выходные данные информационных систем, содержащие секретную информацию, должны иметь соответствующий гриф секретности. Этот гриф должен отражать категорию секретности наиболее уязвимой информации в выводимых данных. Примерами таких выходных данных являются печатные отчеты, информация, выводимая на экраны дисплеев, данные, хранимые на магнитных носителях (лентах, дисках, кассетах), электронные сообщения и передаваемые файлы.

7. СЛУЖБА БЕЗОПАСНОСТИ ОБЪЕКТА СВЯЗИ

7.1. Основные функции службы безопасности

7.1.1. Установление обстоятельств недобросовестной конкуренции со стороны других предприятий

Под ***недобросовестной конкуренцией*** понимается применение в конкурентной борьбе средств и методов, связанных с нарушением действующего законодательства, регламентирующего производственную и коммерческую деятельность предприятий, или норм и правил взаимоотношений между конкурентами, принятых на рынке товаров и услуг.

Недобросовестная конкуренция возможна путем использования коррумпированных чиновников, лиц из уголовной среды и шпионажа.

7.1.2. Расследование фактов разглашения коммерческой тайны предприятия

Под **коммерческой тайной** понимается не являющаяся государственным секретом, специально охраняемая собственником (владельцем) управленческая, производственная, научно-техническая, финансовая, торговая и иная деловая информация.

Информация может быть отнесена к коммерческой тайне в случае попадания ее в «Перечень сведений, составляющих коммерческую тайну предприятия», утвержденном его руководством и объявленном под расписку всем причастным к ней сотрудникам.

По факту разглашения коммерческой тайны предприятия служба безопасности должна проводить расследование по следующим направлениям:

- человек;
- документ;

- изделие-процесс.

Именно в рамках этой триады (разумеется при ее конкретизации) расположены каналы утечки информации, поэтому наиболее целесообразно организовать работу службы безопасности по перечисленным направлениям.

7.1.3. Сбор информации о лицах, заключивших с предприятием контракты

Предприятие обычно заключает два типа контрактов: **коммерческий** (документ, представляющий собой договор поставки товаров или предоставления услуг) и **трудовой** (вид трудового договора, заключающегося в письменной форме со своими постоянными или временными работниками). Одним из договорных условий может быть письменное согласие лица, с которым подписывается контракт, на сбор информации о его биографических и других характеризующих личность данных. При этом в контракте должно быть оговорено, что такого рода сбор информации проводится как до вступления контракта в силу (например во время прохождения испытательного срока), так и во время его реализации, т.е. до расторжения контракта.

Совокупность вышеуказанных сведений в достаточной мере может характеризовать человека и помочь руководству предприятия принять решение о целесообразности дальнейшего с ним сотрудничества.

7.1.4. Поиск утраченного имущества предприятия

Под ***имуществом*** предприятия понимаются находящиеся в его ведении или собственности материальные ценности, денежные средства в кассе, на расчетном счете и других счетах в банках, нематериальные активы (патенты, лицензии, программы, ноу-хау и т.п.). В узком смысле слова под имуществом предприятия понимаются вещи (материальные ценности).

Утраченное имущество предприятия условно делится на две категории:

- ставшее бесхозяйным (т.е. собственник которого неизвестен);

- утерянное по халатности его сотрудников.

Содержание работы сотрудников службы безопасности в зависимости от категории утраченного имущества носит различный характер.

7.1.5. Расследование фактов неправомерного использования товарных (фирменных) знаков предприятия

Товарный знак – обозначение, способное отличать соответственно товары и услуги одних юридических и физических лиц от однородных товаров и услуг других юридических или физических лиц.

Нарушением прав владельца товарного знака признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью товарного знака или товара, обозначенного этим знаком, или обозначения, сходного с ним до степени смешения в отношении однородных товаров. Важнейшей особенностью такого нарушения является его большой территориальный разброс, наличие большого количества потенциальных правонарушителей и сложности с его документированием, что чрезвычайно затрудняет деятельность сотрудников службы безопасности.

7.1.6. Выявление ненадежных деловых партнеров

Ненадежность делового партнера определяется:

- большим количеством сорванных по его вине сделок с другими фирмами;
- несвоевременным и некачественным выполнением условий заключенных договоров;
- значительным количеством в фирме ранее судимых лиц;
- фактами ведения против предприятия-учредителя экономического шпионажа;
- использование помощи сотрудников правоохранительных органов, налоговых инспекций и т.д. с целью парализации экономической деятельности своего партнера;
- умышленным затягиванием деловых переговоров;

- неуважительным отношением к авторскому или патентному праву;

- предъявлением к нему значительного количества судебных исков;

- наличием большого долга;

- непрочной позицией на рынке;

- нерегулярной и ненадежной поставкой сырья и товаров;

- отсутствием доверия потребителей;

- испорченной репутацией среди деловых кругов.

Способность службы безопасности своевременно выявить хотя бы отдельные параметры ненадежности будущих или настоящих партнеров в значительной степени может повлиять на степень экономической безопасности предприятия.

7.1.7. Сбор информации для проведения деловых переговоров

Основными стадиями переговоров являются:

- подготовка к переговорам;

- процесс их ведения;

- анализ результатов переговоров и выполнение достигнутых договоренностей.

Сотрудники службы безопасности участвуют в сборе информации на первой и второй стадиях. При всей условности такого деления служба безопасности должна представлять на различных стадиях руководству предприятия свою информацию. Например, в процессе подготовки к переговорам сведения об участниках будущих переговоров, их сильных и слабых сторонах, их позициях и планах ведения переговоров, подготовленных материалах, конкурентоспособности и платежеспособности делового партнера и т.д.

Во время проведения переговоров служба безопасности должна поставлять информацию об изменениях позиции партнеров по переговорам, о возможных попытках с их стороны шантажировать, подкупать членов

делегации предприятия, о проведении в отношении их разведывательных мероприятий и т.д.

7.1.8. Защита жизни и здоровья персонала от противоправных посягательств

Защиту организует служба безопасности либо всего персонала предприятия (во время нахождения его на работе), либо некоторых его категорий (руководителей) в рабочее и, как исключение, в нерабочее время, либо применяются оба варианта. При этом четко определяется время (круглосуточно, только в дневное время и т.д.) проведения охранных мероприятий. Охранники должны быть нацелены, прежде всего, на пресечение насильственных преступлений (покушение на убийство, рэкет) и административных проступков (мелкое хулиганство) в отношении охраняемых лиц. Должны широко применяться технические средства защиты.

7.1.9. Охрана имущества предприятия

Под ***охраной имущества*** понимается комплекс оперативно-режимных, организационно-управленческих и инженерно-технических действий, проводимых с целью обеспечения сохранности материально-технических и финансовых средств собственника. Охране подлежат все материальные ценности независимо от их местоположения (внутри или за пределами предприятия).

В то же время существуют объекты первостепенной важности, охране которых необходимо уделять особое внимание, так как именно они чаще всего подвергаются противоправному посягательству. К таким объектам относятся:

- дефицитное оборудование (компьютеры, автозапчасти и т.д.);
- деньги, инвалюта и т.д.;
- наиболее важная и конфиденциальная документация.

7.1.10. Обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий

Обеспечение порядка необходимо:

- во время проведения представительских (выставки, ярмарки и т.д.),

- массовых (спортивные соревнования, концерты и т.д.),

- конфиденциальных (заседание правления, совещания руководителей и специалистов по служебным вопросам и т.д.) мероприятий.

В зависимости от их типа меняется и содержание деятельности службы безопасности. Например, при проведении закрытых совещаний основное внимание уделяется, прежде всего, защите сведений, составляющих коммерческую тайну; на выставках необходимо принимать меры к недопущению кражи или порчи имущества предприятия; при проведении концертов основное внимание уделяется физической безопасности людей и т.д.

7.1.11. Консультирование и представление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности

В обязанности службы безопасности входит не только консультирование и дача рекомендаций сотрудникам предприятия по вопросам обеспечения безопасности, но и ее реализация. В связи с этим необходимо внести в проект Устава службы безопасности положение об обязанности сотрудников подразделений предприятия выполнять эти рекомендации и определить ответственность (материальную и дисциплинарную) за их невыполнение. Проведение консультаций и рекомендаций по вопросам безопасности обычно не выходит за пределы таких ее основных видов, как экономическая, информационная, пожарная, физическая безопасность.

7.1.12. Проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации

Средства охранно-пожарной сигнализации предназначены для обнаружения попыток проникновения на объект и возникновения пожара, оповещения сотрудников службы безопасности о появлении и нарастании этих угроз и обеспечения контроля доступа на охраняемый объект. Деятельность подразделения службы безопасности, выполняющего функцию внедрения и эксплуатации охранно-пожарной сигнализации, осуществляется в несколько этапов.

Первый этап (проектирование) предусматривает планирование работ по внедрению и капитальному ремонту средств сигнализации, обследование объекта с целью получения исходных данных для разработки исполнительной проектно-сметной документации; материально-техническое обеспечение монтажных работ.

На этапе выполнения монтажных работ, для проведения которых обычно приглашаются специализированные организации, осуществляется технический надзор за качеством их производства, особенно при проведении пусконаладочной работы.

Наконец, последний этап (эксплуатационное обслуживание) включает:

- сдачу этих средств в эксплуатацию;
- планирование эксплуатационных мероприятий и контроль за их исполнением;
- техническое обслуживание, технический контроль эксплуатации средств сигнализации;
- ремонт приборов и аппаратуры охранно-пожарной сигнализации;
- материальное обеспечение эксплуатационных нужд;
- ведение установленной технической документации;

- сбор и обобщение статистических данных по эксплуатационно-техническому обслуживанию;

- анализ причин отказов в работе аппаратуры и причин, способствующих совершению краж и приводящих к пожарам в заблокированных участках объекта.

7.2. Система управления службой безопасности

Такая система состоит из субъекта, объекта управления, прямой и обратной связи. ***Субъектами управления*** службой безопасности выступают руководитель предприятия, совет безопасности предприятия и начальник службы безопасности. Успешно выполнять свои задачи эти субъекты могут только в том случае, если компетенция каждого из них будет строго определена в правовых актах таким образом, чтобы не возникала почва для конфликтов. Если это сделано достаточно успешно, то можно говорить о сформированной управляющей подсистеме.

Объектами управления (управляемой подсистемой) в службе безопасности выступают ее отдельные сотрудники и подразделения. Объект управления соединен с субъектом управления каналами прямой и обратной связи (информационными каналами). По каналу прямой связи информация в виде управленческих решений поступает от субъекта управления к объекту, а по каналам обратной связи – в обратном направлении, сигнализируя о состоянии объекта управления, его реакции на управленческие воздействия.

Само управленческое воздействие, в свою очередь, реализуется в форме таких функций управления, как прогнозирование, планирование, организация, регулирование, мотивация и контроль. В системе управления все эти функции объединены в целостный процесс, хотя из методических соображений целесообразно рассматривать их отдельно. Рассмотрим вышеуказанные функции с учетом специфики деятельности службы безопасности.

7.2.1. Прогнозирование

Предполагает составление заключения (прогноза) о будущем событии, тенденции развития службы безопасности. Прогнозные оценки бывают оперативными (с упреждением не более одного месяца), краткосрочными (от 1 месяца до 1 года), среднесрочными (от 1 года до 5 лет). Составляются они как привлеченными со стороны специалистами, так и сотрудниками службы безопасности (в первую очередь сотрудниками штаба).

Качество прогнозных оценок повышается, если они составляются сотрудниками службы безопасности с помощью приглашенных экспертов-специалистов в той или иной области.

Представляется, что наиболее целесообразным было бы составление следующих видов прогнозных оценок:

- криминологические;
- риски (коммерческий, финансовый и т.д.) в предпринимательской деятельности;
- экономическая, физическая, информационная и т.д. безопасность предприятия.

7.2.2. Планирование

Предполагает определение целей, задач службы безопасности на предстоящий период деятельности, средств и времени на их достижение. Наиболее распространенными в деятельности служб безопасности являются комплексные и специальные планы.

Комплексные планы охватывают все сферы деятельности службы безопасности и включают, как правило, организационные разделы, обеспечение всех видов безопасности предприятия (в рамках компетенции службы безопасности), работу с кадрами, ресурсное обеспечение, контроль и т.д.

Специальные планы разрабатываются на случай возникновения чрезвычайных происшествий и чрезвычайных ситуаций (нападения на объект, угроза взрыва бомбы, захват заложников, наводнение, пожар и т.д.).

7.2.3. Организация

Функция организации состоит в установлении постоянных и временных взаимоотношений между всеми подразделениями службы безопасности, определении порядка и условий ее функционирования. Это процесс объединения сил и средств для достижения поставленных целей.

7.2.4. Регулирование

Представляет собой «наладку» системы, приведение ее в нормальное рабочее состояние. Необходимость в ней возникает в силу изменения внешних условий либо из-за возникновения каких-то нарушений, «сбоев» в функционировании самой системы. Посредством этой функции достигается поддержание управляемых процессов в рамках, заданных программой, регламентом, планом. Орган управления службы безопасности через эту функцию должен обеспечить сохранение заданных параметров следующими приемами:

- выравнивание отклонений (профилактические беседы, рейды, операции и т.д.);

- компенсация возмущений (бесплатные питание и проезд в общественном транспорте, увеличение количества отгулов и т.д.);

- устранение воздействия помех (стихийные бедствия, нападения на охраняемый объект, дискредитация руководства предприятия в средствах массовой информации, поджоги помещений и т.д.).

7.2.5. Мотивация

Процесс побуждения сотрудников службы безопасности к деятельности для достижения целей самой службы и ее подразделений. Мотивация

представляет собой совокупность сил, побуждающих сотрудника осуществлять деятельность с затратой определенных усилий, на определенном уровне старания и добросовестности, с определенной степенью настойчивости в направлении достижения определенных целей.

В основе любой теории мотивации лежат потребности человека, которые можно удовлетворить вознаграждениями. Причем выделяют внешние вознаграждения (заработная плата, премии и т.д.) и внутренние – чувство успеха при достижении цели, получаемое от самой работы.

Для практических целей достаточна типология с использованием трех типов мотивации:

I тип – сотрудники, ориентированные преимущественно на содержательность и общественную значимость труда;

II тип – сотрудники, преимущественно ориентированные на оплату труда и другие нетрудовые ценности;

III тип – сотрудники, у которых значимость разных ценностей сбалансирована.

7.2.6. Контроль

Состоит в процессе соизмерения (сопоставления) фактически достигнутых результатов с запланированными. Эффективная система контроля должна соответствовать следующим требованиям:

- контроль должен быть всеобъемлющим;
- контроль следует сосредоточить на результате;
- система контроля должна быть простой;
- контроль не может быть ни целенаправленным, ни нейтральным;
- контроль должен быть постоянным.

Субъектами контрольной деятельности в службе безопасности являются: руководитель предприятия-учредителя, члены совета (комитета) безопасности предприятия, руководители службы безопасности и его

подразделений (в рамках своей компетенции). Кроме этого, внешними субъектами контроля могут быть сотрудники лицензионно-разрешительных подразделений органов внутренних дел и прокуратуры.

Подконтрольными объектами могут быть: деятельность подразделений, состояние технической укрепленности охраняемого объекта, защищенность коммерческой тайны, система профессиональной подготовки и переподготовки сотрудников службы безопасности и т.д. Выбор объекта контроля определяется его способностью влиять (положительно или отрицательно) на деятельность службы безопасности в целом. В рамках подконтрольного объекта очень важны его составные элементы, после определения которых можно непосредственно приступить к контролю.

Различают три вида контроля:

- предварительный (осуществляется до фактического начала работ);
- текущий (осуществляется в ходе осуществления работ);
- заключительный (осуществляется после выполнения работ).

С учетом специфики деятельности службы безопасности преимущественное внимание следует уделить предварительному и текущему контролю.

7.3. Методы, принципы и процесс управления службой безопасности

Методы управления подразделяются на три группы:

- экономические;
- организационно-распорядительные;
- социально-психологические.

На уровне сотрудника службы безопасности преимущественным влиянием пользуется такой ***экономический стимул***, как заработная плата. Умелое использование этого стимула с учетом уровня профессионализма, стажа работы, результатов деятельности сотрудника и т.д. позволяет в значительной степени повысить его трудовую активность.

Организационно-распорядительные методы управления (приказы, распоряжения, указания, инструкции и т.д.) подразделяются на три группы:

- распорядительные;
- организационно-стабилизирующие;
- дисциплинирующие.

Социально-психологические методы основаны на использовании моральных стимулов к труду и воздействуют на личность сотрудника службы безопасности с помощью психологических приемов в целях превращения задания в осознанный долг, внутреннюю потребность человека. Это достигается посредством приемов, которые носят личностный характер (личный пример, авторитет и т.д.).

Принципы управления службой безопасности определяют требования к системе, структуре и организации процесса управления. В рамках службы безопасности это следующие принципы:

- научность – все управленческие действия осуществлялись на базе применения научных методов и подходов);

- единоначалие и коллегиальность – на основе мнений руководителей низшего звена и рядовых исполнителей конкретных решений вышестоящий начальник пользуется правом единоличного решения вопросов, входящих в его компетенцию;

- системность и комплексность – необходимость использования системного анализа в каждом управленческом решении и всестороннего охвата управляемой системы;

- оптимальное сочетание централизации и децентрализации – оптимальное распределение полномочий при принятии управленческих решений;

- плановость – установление основных направлений и пропорций службы безопасности в перспективе;

- сочетание прав, обязанностей и ответственности – каждый сотрудник службы безопасности должен выполнять возложенные на него обязанности, при этом он наделяется адекватными ему правами и несет ответственность за качество их выполнения.

Структура процесса управления в самом общем виде состоит из трех стадий, каждая из которых включает в себя последовательно осуществляемые этапы или операции:

I стадия. Сбор, обработка, обобщение и анализ информации.

II стадия. Выработка и принятие управленческого решения.

III стадия. Организация исполнения управленческого решения.

8. КОНТРОЛЬНО-ПРОПУСКНОЙ РЕЖИМ ОБЪЕКТА СВЯЗИ

8.1. Организация и осуществление контрольно-пропускного режима

Контрольно-пропускной режим является неотъемлемой частью общей системы обеспечения безопасности объекта связи. Режим должен соответствовать действующему законодательству, уставу организации (объекта), а также иным нормативно-правовым актам.

Основные цели контрольно-пропускного режима сводятся к следующему:

- защита законных интересов прав организации, поддержание устойчивости порядка внутреннего управления;
- сохранение собственности, ее рационального и эффективного использования;
- способствование росту прибыли;
- достижение внутренней и внешней стабильности предприятия;
- сохранение коммерческих секретов и прав интеллектуальной собственности.

Для достижения целей контрольно-пропускного режима организации должны отвечать следующим требованиям:

- обеспечение прохода сотрудников и посетителей, ввоз (вывоз) продукции и материальных ценностей;
- пресечение незаконного прохода лиц на охраняемые территории и в отдельные здания (помещения), бесконтрольного въезда (выезда) транспортных средств;
- выявление угроз жизненно важным интересам организации, причин и условий, способствующих нанесению материального и морального ущерба, ее нормальному функционированию и развитию;

- формирование надежных гарантий поддержания организационной стабильности внешних и внутренних связей организации, отработка механизма оперативного реагирования на угрозы и негативные тенденции в развитии;

- пресечение посягательств на законные интересы организации, использование юридических, экономических, организационных, социально-психологи-

ческих, технических и иных средств для выявления и ослабления источников угрозы ее безопасности.

Основные мероприятия контрольно-пропускного режима разрабатываются службой безопасности, утверждаются руководителем фирмы и оформляются инструкцией о контрольно-пропускном режиме. Ответственность за организацию контрольно-пропускного режима возлагается на начальника службы безопасности.

Практическое осуществление контрольно-пропускного режима возлагается на охрану (дежурных по КПП, контролеров, охранников), работники которой должны знать установленные на объекте правила контрольно-пропускного режима, действующие документы по порядку пропуска на объект (с объекта) сотрудников и посетителей, ввоза (вывоза) товарно-материальных ценностей. Контрольно-пропускной режим может быть установлен как в целом по объекту, так и в отдельных корпусах, зданиях, отделах, хранилищах и других специальных помещениях.

Требования по контрольно-пропускному режиму должны быть доведены в обязательном порядке до каждого сотрудника объекта. Все рабочие и служащие объекта обязаны соблюдать их. По каждому случаю нарушения контрольно-пропускного режима должно проводится административное расследование.

Обязанности охраны по контрольно-пропускному режиму определяются в инструкции и в должностных обязанностях контролеров контрольно-пропускных пунктов.

Разработка мероприятий и нормативных документов контрольно-пропускного режима начинается с определения исходных данных. Оценивая исходные данные, разработчик определяет основные положения инструкции о контрольно-пропускном режиме. Целесообразно предложить следующую последовательность определения и оценки исходных данных.

1. Организационная структура фирмы, места расположения ее отдельных элементов и характер производства (деятельности) на них. Выяснение этих вопросов позволяет решить следующие практические задачи:

- выделить объекты, площадки, здания, помещения, на которых необходимо организовать контрольно-пропускной режим;
- определить характер контрольно-пропускных пунктов (КПП) для пропуска сотрудников, транспортных средств.

2. Провести оценку «суточного объема» потоков транспортных средств, грузов, материальных ценностей и людей (персонала фирмы и посетителей), проходящих через КПП и в отдельные здания (помещения). Только на основе оценки реального состояния мест пропуска можно оценить пропускную способность действующих КПП и привести ее в соответствие с задачами основного производства на объекте. Такая оценка позволит выбрать оптимальный вариант автоматизации и контроля прохода, проезда на охраняемые территории.

3. Выделить на территории (по степени важности) категории объектов, транспортных средств и грузов, а также категории лиц, пересекающих установленные границы. Для достижения четкости в определениях предлагается помещения и территорию объекта классифицировать в зависимости от условий доступа и степени защищенности.

8.2. Разработка инструкции о пропускном режиме

Пропускной режим является неотъемлемой частью общей системы охраны предприятий. Практическое решение этих вопросов оформляется в виде

«Инструкции о пропускном режиме». Указанная инструкция должна определять систему организационно-правовых охранных мер, устанавливающих разрешительный порядок (режим) прохода (проезда) на объект (с объекта), и может включать:

1. Общие положения. В этом разделе указываются:

- нормативные документы, на основании которых составлялась инструкция;

- определение контрольно-пропускного режима и цель его установления;

- лицо, на которое возлагается руководство пропускным режимом, практическое его осуществление;

- санкции к нарушителям контрольно-пропускного режима;

- требования к оборудованию различных помещений.

2. Порядок пропуска сотрудников предприятия, командированных лиц и посетителей через контрольно-пропускные пункты. В этом разделе рекомендуется:

- перечислить все КПП и их назначение, описание, расположение и установить их единую нумерацию;

- изложить требования к оборудованию КПП;

- установить порядок прохода сотрудников и посетителей на территорию объекта и в категорированные подразделения;

- определить права и основные обязанности контролеров КПП;

- установить помещения, где запрещается принимать посетителей и представителей сторонних организаций.

3. Порядок допуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей. В этом разделе указываются:

- порядок допуска на территорию объекта (с объекта) автотранспорта, принадлежащего объекту;

- въезд и стоянка на территории объекта транспорта, принадлежащего сотрудникам на правах личной собственности;

- порядок пропуска автомашин сторонних организаций, прибывших с грузом в адрес объекта в рабочее и нерабочее время;

- порядок вывоза (ввоза) товарно-материальных ценностей;

- правила оформления документов на вывоз (вынос) материальных ценностей с территории объекта.

4. Виды пропусков, порядок их оформления. В этом разделе определяются:

- виды пропусков, их количество и статус;

- описание пропусков;

- порядок оформления и выдачи пропусков;

- общая замена и перерегистрация пропусков;

- мероприятия при утере пропуска сотрудником.

5. Обязанности должностных лиц по поддержанию контрольно-пропускного режима.

6. Учет и отчетность, порядок хранения пропусков, печатей.

В зависимости от структуры предприятия и характера его деятельности инструкция может содержать и другие разделы.

8.3. Виды пропусков

Для допуска на предприятие, в отдельные помещения, как правило, устанавливаются несколько видов пропусков: постоянные, временные, разовые и материальные. Образцы бланков пропусков разрабатываются администрацией объекта (службой безопасности). По своему внешнему виду и содержанию пропуска должны отличаться друг от друга и обладать защитными свойствами. Все виды пропусков, за исключением материальных, оформляются и выдаются бюро пропусков (или иным подразделением) по письменным заявкам. Виды пропусков определяются в зависимости от специфики предприятия.

Постоянные пропуска выдаются сотрудникам объекта, принятым на постоянную работу, а также работникам других организаций, закрепленных для

постоянного обслуживания объекта. Постоянные пропуска могут делиться на группы, их количество и назначение определяется инструкцией о контрольно-пропускном режиме. Постоянные пропуска могут храниться как на руках у сотрудников объекта, так и в кабинах на КПП. Постоянные пропуска лиц, убывающих с объекта на длительное время (отпуск, болезнь, командировка и т.п.), сдаются на хранение в бюро пропусков (отдел кадров), а при оставлении таких пропусков в кабине, на ячейке (где хранится пропуск) делается соответствующая отметка. Пропуска уволенных с работы уничтожаются установленным порядком.

Временные пропуска выдаются лицам, работающим по контракту, находящимся на временной работе, прикомандированным к предприятию, и хранятся, как правило, на КПП. Срок действия и порядок оформления временных пропусков определяется инструкцией о контрольно-пропускном режиме.

Временные пропуска могут быть с фотографией и без фотографии. Временные пропуска без фотографии действительны только при предъявлении документа, удостоверяющего личность.

Разовые пропуска (для посетителей и клиентов) выдаются на одно лицо и только для разового посещения предприятия и его подразделений. Пропуск оформляется и действителен при наличии документа, удостоверяющего личность. Разовые пропуска должны периодически меняться по цвету бланков и другим отличительным признакам.

Разовый пропуск, выданный водителю транспортного средства, может служить одновременно и разовым пропуском для транспорта. Разовый пропуск действителен для входа на территорию объекта или его подразделения в течении определенного времени.

Контроль за посетителями предприятия по разовому пропуску осуществляется с помощью отметки на оборотной стороне пропуска, где

указывается время посещения, заверенное подписью лица, принявшего посетителя.

Разовый пропуск изымается на посту контролером при выходе посетителя с объекта и сдается в бюро пропусков. О лицах, не вышедших с объекта по истечению установленного срока действия пропуска, контролер докладывает начальнику караула (дежурному по КПП) для принятия мер по выяснению причин задержки. Фамилии лиц, посетивших объект по разовому пропуску, могут записываться в специальную книгу учета.

Материальные пропуска для вывоза (выноса) товарно-материальных ценностей выдаются администрацией предприятия. Срок действия пропуска определяется инструкцией о контрольно-пропускном режиме. Материальные пропуска должны изыматься на КПП и сдаваться в бюро пропусков.

Образцы действующих пропусков должны находиться на КПП. Для обучения работников охраны выделяется необходимое количество образцов пропусков.

8.4. Оборудование КПП

Для организации пропускного режима на предприятии оборудуются контрольно-пропускные пункты. Оборудование КПП должно обеспечивать необходимую пропускную способность и возможность тщательной проверки пропусков, документов у проходящих лиц, досмотра всех видов транспорта, провозимых грузов и удовлетворять следующим требованиям:

- исключать возможность несанкционированного проникновения через КПП на объект (с объекта) людей и транспортных средств;

- способствовать сокращению времени на проверку документов, досмотр транспорта и материальных ценностей;

- способствовать исключению (сведению к минимуму) ошибок охранника при пропуске людей и транспорта;

- обеспечивать меры безопасности охранника при досмотре транспортных средств.

Все виды КПП должны быть оборудованы необходимыми видами связи и тревожной сигнализации для вызова резерва охраны. На КПП рекомендуется располагать внутренний телефон и список телефонов администрации предприятия.

8.4.1. КПП для прохода людей

Для контроля лиц, проходящих на объект и в отдельные здания (помещения), строятся КПП. Каждый КПП рекомендуется оборудовать комнатой для охраны, комнатой для досмотра граждан, камерой хранения, гардеробом, турникетом с фиксирующими устройствами-запорами.

Размещение помещений определяется проектами и зависит от средств механизации, автоматизации КПП и особенностей предприятия.

В контрольно-пропускном зале устраиваются проходы, которые оборудуются техническими средствами охраны и физическими барьерами. В комплект оборудования, как правило, входят:

- средства механизации, автоматизации, системы контроля доступа;
- физические барьеры (ограждения, турникеты, калитки);
- основное и резервное освещение;
- средства связи и тревожной сигнализации;
- системы видеоконтроля.

В качестве средств контроля доступа могут использоваться различные турникеты. Турникеты предназначены для управления потоками людей и регулирования входа (выхода). В последнее время наиболее широкое распространение получили электромеханические турникеты. Электромеханические турникеты в отличие от громоздких и неудобных в управлении механических легко управляются с пульта охранника и могут работать в составе автоматизированной системы контроля доступа.

Турникеты-триподы с тремя преграждающими планками являются одним из наиболее оптимальных средств для осуществления контроля санкционированного прохода. Триподы имеют современный элегантный вид и легко монтируются. Триподы позволяют осуществлять эффективный контроль доступа, т.к. разделяют поток людей по одному, обеспечивая при этом высокую пропускную способность. Триподы могут применяться в системах электронных проходных, в том числе в условиях большого потока людей. Для предотвращения возможности подлезть под планки турникета или перепрыгнуть через них на турникеты рекомендуется устанавливать специальные датчики, которые срабатывают при попытке несанкционированного прохода.

Роторные турникеты-вертушки применяются в тех случаях, когда необходимо полное перекрытие зоны прохода. Они могут быть различными по высоте – от поясных до турникетов в полный рост, которые конструктивно подобны вращающимся дверям.

8.4.2. Автотранспортные КПП

В состав автотранспортного КПП входит досмотровая площадка и служебные помещения. Досмотровая площадка предназначается для размещения автомобилей при их досмотре. Досмотровые площадки могут располагаться как на территории предприятия, так и за ее пределами, на местности, непосредственно примыкающей к основным воротам КПП. Досмотровая площадка должна отвечать следующим требованиям:

- иметь достаточную площадь для размещения досматриваемого транспорта, технические средства для обеспечения нормальных условий работы охранника;

- исключать возможность несанкционированного проникновения на объект (с объекта) людей и транспортных средств;

- обеспечивать при установленной интенсивности движения в любое время суток и года досмотр автомобильного транспорта и перевозимых грузов;

- быть изолированной от других сооружений, не имеющих отношения к охране объекта и оборудованию КПП;

- обеспечивать меры безопасности охранника при выполнении своих обязанностей.

Размеры досмотровой площадки устанавливаются в зависимости от габаритов транспорта и перевозимых грузов и могут составлять: 10…12 м в длину и 5…6 м в ширину.

На территории, отведенной для строительства досмотровой площадки, производится планировка местности с таким расчетом, чтобы на ней не задерживались дождевые и талые воды. Поперечный уклон досмотровой площадки составляет не менее 2 % от места выставления охранника в направлении ее боковых сторон (перпендикулярно проезжей части). Поверхность досмотровой площадки покрывается бетоном или асфальтом.

На проезжей части площадки выделяется место остановки транспорта для досмотра, ограниченное двумя линиями СТОП, выполненными белой краской.

Перед въездом на досмотровую площадку с внешней стороны основных и вспомогательных ворот (шлагбаума), не ближе 3 м от них, также наносится поперечная линия и надпись СТОП. В целях обеспечения безопасности движения транспорта не менее чем в 100 м от ворот с правой стороны или над дорогой устанавливается указательный знак «Движение в один ряд», а в 50 м от знака – знак ограничения скорости до 5 км/ч.

Автотранспортные КПП могут оборудоваться светофорами, весами для взвешивания автомобилей, досмотровой ямой или эстакадой для осмотра грузов, механизированными устройствами для автоматического открытия и закрытия ворот с фиксаторами.

Досмотровые площадки по периметру оборудуются физическими барьерами и рубежом сигнализации. Площадки, как правило, выгораживаются

просматриваемым забором из металлической сетки или декоративных решеток высотой до 2,5 м. На площадке оборудуются основные и вспомогательные механизированные ворота. Основные ворота устанавливаются на линии основного ограждения объекта, а вспомогательные – на противоположной стороне досмотровой площадки. Вместо ворот могут применяться механизированные шлагбаумы. На автомобильных КПП используются ворота с ограничением и без ограничения габаритов по высоте. По конструкции они могут быть распашными или раздвижными (выдвижными). Распашные ворота должны оборудоваться фиксаторами.

Для регулирования движения транспорта, проходящего через проезды досмотровых площадок КПП, могут применяться двухсекционные светофоры с линзами красного и зеленого цветов.

В состав электромеханического оборудования КПП для автомобильного транспорта обычно включаются:

- электродвигатели, привод ворот;
- концевые выключатели автоматического отключения электродвигателей при полностью закрытых и открытых створках ворот;
- магнитные пускатели электродвигателей;
- электрооборудование светофоров;
- кабельные, силовые линии.

Групповой распределительный щит (щит управления) может устанавливаться в помещении КПП, а при отсутствии здания КПП – в специальном металлическом шкафу непосредственно на досмотровой площадке.

8.5. Пропуск сотрудников, посетителей на объект и в отдельные категорированные помещения

Проход сотрудников и посетителей на территорию объекта, в категорированные подразделения и обратно осуществляется по установленным

на объекте пропускам через контрольно-пропускные пункты. Пропуск должен являться основным документом, дающим право на проход.

Допуск командированных (посетителей) производится по разовым пропускам в установленные и указанные в пропуске часы, в исключительных случаях по утвержденным начальником службы безопасности спискам с предъявлением документов, удостоверяющих личность.

Представители средств массовой информации допускаются на объект на общих основаниях в сопровождении представителей администрации.

В нерабочее время, выходные и праздничные дни допуск сотрудников на объект должен быть ограничен и производится по предварительным заявкам (спискам) руководителей подразделений, завизированным начальником службы безопасности, с предъявлением постоянного пропуска. На предприятиях со сменным режимом работы к пропуску могут выдаваться специальные вкладыши сменности.

Дежурные специальных служб объекта (электрики, сантехники, работники связи и т.д.), работающие посменно, допускаются на территорию объекта в нерабочее время, в выходные и праздничные дни по спискам, подписанным начальниками соответствующих служб и утвержденным начальником службы безопасности.

На основании действующего законодательства и решения администрации отдельные категории лиц пользуются правом прохода на объект без пропуска, при предъявлении служебного удостоверения. К ним относятся:

- работники прокуратуры;

- работники милиции по территориальности;

- инспекторы труда, энергонадзора по территориальности;

- должностные лица и отдельные категории работников санитарно-эпидемиологической службы органов здравоохранения, осуществляющие санитарный надзор.

Категории лиц, имеющих право прохода на объект без пропуска (по служебным удостоверениям), должны быть четко отражены в инструкции о контрольно-пропускном режиме.

В целях осуществления пропускного режима на территории объекта и в его структурных подразделениях приказом начальника предприятия утверждается перечень категорированных подразделений (помещений). В этих помещениях устанавливается специальный режим и повышенная ответственность за его соблюдение работниками этих подразделений.

Допуск в эти помещения осуществляется строго по списку, согласованному со службой безопасности. Прием посетителей сторонних организаций и предприятий, как правило, максимально ограничивается.

Во всех помещениях категорированных подразделений должны быть вывешены в застекленных рамках списки работников, имеющих допуск в эти помещения. Все помещения по окончании работ осматриваются дежурными по подразделениям и лицами, ответственными за их противопожарное состояние. Электроосветительная и электронагревательная аппаратура обесточивается, окна и форточки закрываются, двери запираются на замок и опечатываются. По окончании рабочего дня оборудованные охранной сигнализацией данные помещения закрываются и опечатываются ответственными лицами этих подразделений и сдаются под охрану. Представитель охраны проверяет сигнализацию в присутствии работников, сдающих помещение. Ключи от этих помещений в опечатанных пеналах сдаются под расписку начальнику караула.

Получение ключей, вскрытие помещений, оборудованных охранной сигнализацией, производят лица, имеющие допуск на право вскрытия этих помещений с предъявлением постоянного пропуска. Списки лиц, имеющих право вскрывать (закрывать) указанные помещения, с указанием номеров печатей, которыми опечатываются помещения и номеров служебных телефонов, подписываются начальником подразделения и утверждаются начальником службы безопасности.

Все лица, пытающиеся пройти через КПП без предъявления пропуска, по чужому или неправильно оформленному пропуску, пронести на объект (с объекта) запрещенные предметы, задерживаются и передаются в службу безопасности предприятия. По каждому факту задержания начальник караула или дежурный по объекту составляет служебную записку о нарушении пропускного режима.

8.5.1. Допуск на территорию объекта связи транспортных средств, вывоз материальных ценностей

Допуск на территорию (с территории) объекта связи транспортных средств, принадлежащих данному предприятию, производится при предъявлении водителем личного пропуска со специальным шифром или транспортного пропуска и путевого листа. Грузчики и сопровождающие лица, следующие с транспортом, пропускаются через КПП на общих основаниях.

Все транспортные средства при проезде через КПП подвергаются досмотру. Въезд и стоянка на территории предприятия транспорта, принадлежащего сотрудникам на правах личной собственности, разрешаются по специальным спискам.

Автомашины сторонних организаций, прибывшие с грузом в адрес предприятия в рабочее время, допускаются на территорию по служебным запискам с досмотром на автотранспортном КПП. Заезд машин на территорию предприятия производится штатным водителем в сопровождении представителя администрации (грузополучателя).

Вывоз и вынос готовой продукции и других материальных ценностей с территории объекта осуществляется по материальным пропускам установленного образца.

Убедившись в правильности оформления документов и их полном соответствии с вывозимыми ценностями, охранник оставляет на КПП пропуск,

ставит на пропуске дату и время вывоза груза, расписывается и дает разрешение на вывоз материальных ценностей.

Все документы вывозимых (выносимых) с предприятия материальных ценностей регистрируются в бюро пропусков в книге учета и в течение следующего дня передаются в бухгалтерию. Бланки всех видов материальных пропусков изготавливаются типографским способом и хранятся в бухгалтерии, выдаются в подразделения предприятия по служебным запискам. Документы на вывоз (вынос) материальных ценностей должны быть выписаны только на то количество груза (мест, веса и т.п.), которое может быть вывезено (вынесено) одновременно, и действительны только на дату, указанную в разрешительном документе.

Контроль за транспортными средствами, въезжающими (въезжающими) на предприятие, рекомендуется проводить в следующей последовательности.

Работник охраны, убедившись в правильности оформления сопроводительных документов, должен удостовериться в соответствии наименования и количества ввозимого (вывозимого) груза данным в сопроводительных документах, а также проверить скрытые места транспортного средства (которые могут использоваться для хищения). С этой целью он осматривает транспортное средство и груз, используя специальную смотровую площадку, эстакаду. Материальные ценности на транспортном средстве должны быть уложены в определенном порядке, удобном для контроля. При пропуске опломбированных (опечатанных) грузов охранник сверяет пломбы (печати) с указанными в накладных, после чего, когда никаких сомнений в соответствии количества и наименования груза сопроводительным документам нет, разрешается въезд или выезд автотранспорта. Материальные пропуска, товаротранспортные накладные регистрируются охранником в книге учета (отдельно на ввозимые и вывозимые грузы) в строгом соответствии с порядком их поступления.

9. ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЗАЩИТЫ ОБЪЕКТА СВЯЗИ

9.1. Технический контроль защиты объектов от утечки информации за счет побочных электромагнитных излучений

Технический контроль (инструментальная проверка) объектов заключается в проведении измерений с помощью контрольно-измерительной аппаратуры с целью проверки эффективности специальной защиты технических средств, систем и объектов от возможной утечки информации по техническим каналам.

При проведении технического контроля защиты объектов от утечки информации за счет побочных (нежелательных) электромагнитных излучений технических средств осуществляется измерение параметров излучений с помощью специальной аппаратуры. К числу измеряемых параметров сигналов относятся частота, ширина спектра, уровень сигнала и т.д.

Измерения проводятся в соответствии с определенными методиками в заданном диапазоне частот. Для измерения частоты сигнала могут быть использованы электронно-счетные частотомеры, измерительные приемники, селективные вольтметры и анализаторы спектра.

Для измерения уровня напряженности электромагнитного поля применяются измерительные устройства, состоящие из измерительной (калиброванной) антенны и приемника с калиброванным усилителем и вольтметром (рис. 9.1).

Рис. 9.1. Структурная схема измерения напряженности электрического поля

На результаты измерения напряженности поля или плотности потока мощности существенное влияние оказывает форма сигнала. Поэтому важно,

чтобы измерительная аппаратура реагировала на сигналы той формы, которые подлежат измерению. Это достигается выбором характеристик детектора, ширины полосы пропускания, динамического диапазона, времени накопления и других параметров измерительной аппаратуры.

Измерение уровня побочных электромагнитных излучений (ПЭМИ) может осуществляться либо на границе контролируемой территории (рис. 9.2), либо в непосредственной близости от контролируемого объекта на расстоянии, определяемом методикой измерения (рис. 9.3).

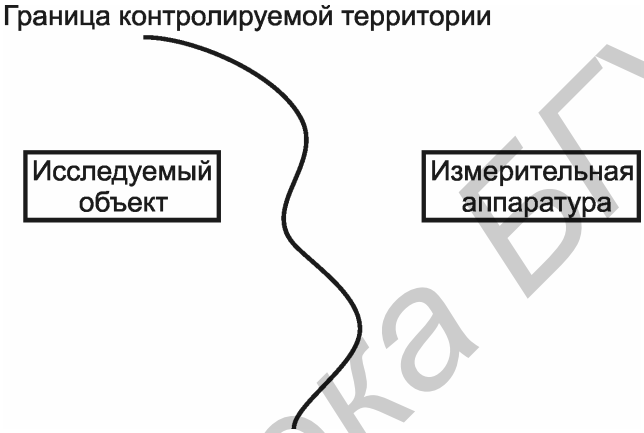

Рис. 9.2. Измерение уровня ПЭМИ на границе контролируемой территории

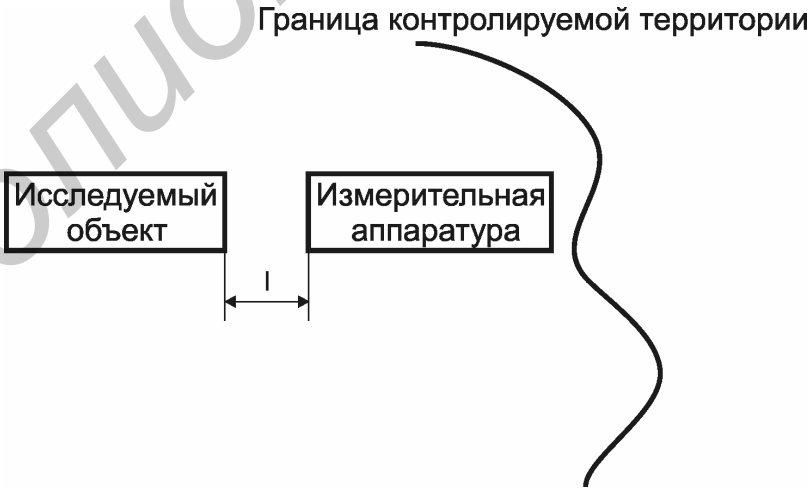

Рис. 9.3. Измерение уровня ПЭМИ в непосредственной близости от объекта

В последнем случае осуществляется пересчет результатов измерений на расстояние, соответствующее границе контролируемой территории.

Измерение параметров ПЭМИ проводится для каждого технического средства, входящего в состав проверяемого объекта. По результатам измерений рассчитывают необходимый радиус контролируемой территории для каждого технического средства и объекта в целом.

Ряд технических средств и систем подлежит проверке на отсутствие самовозбуждения. Такая проверка проводится с использованием специальных тестовых сигналов по определенным методикам в заданных диапазонах частот (рис. 9.4). По результатам контроля защиты объектов от утечки за счет побочных электромагнитных излучений оформляется протокол измерений и расчетов.

Рис. 9.4. Структурная схема проверки технических средств на отсутствие самовозбуждения

9.2. Технический контроль защиты объектов от утечки информации за счет наводок

Этот вид технического контроля осуществляется путем измерения напряжений и (или) токов опасных сигналов в проводниках и других токопроводящих коммуникациях (цепях электропитания, заземления и т.д.). Такие измерения проводятся с помощью специальной измерительной аппаратуры (селективных вольтметров, измерителей радиопомех и т.п.), подключаемой к контролируемым коммуникациям через специальные входные согласующие устройства. В качестве входных устройств используются в зависимости от ситуации эквиваленты сети, пробники, токосъемники, измерительные сопротивления, трансформаторы тока и т.д.

Наиболее распространенными видами измерений являются измерения напряжений и токов наводок опасных сигналов в цепях электропитания и заземления технических средств обработки информации (рис. 9.5).

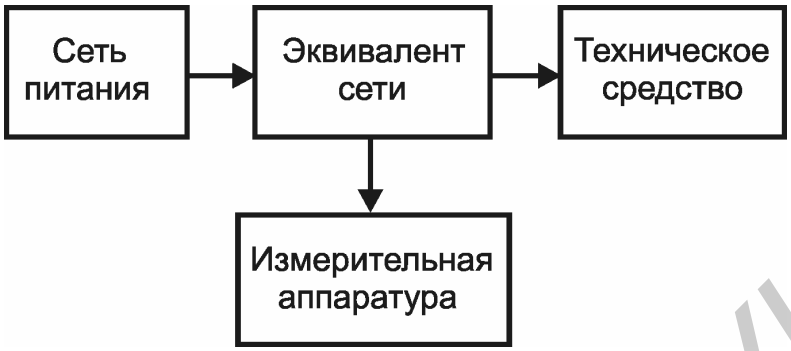

Рис. 9.5. Структурная схема измерения напряжения опасных сигналов в цепи электропитания технического средства

Эквивалент сети – устройство, включаемое в сеть питания и предназначенное для создания регламентированного сопротивления нагрузки на частоте измерения. Кроме того, эквивалент сети исключает возможность проникновения помех из сети питания на вход измерительной аппаратуры и является согласующим устройством между высоковольтной сетью питания и высокочувствительными входными цепями измерительной аппаратуры.

Техническое средство должно функционировать в тестовом режиме, имитирующем обработку информации. Например, в системах звукоусиления в качестве тестового сигнала используется тональный сигнал частотой f = 1000 Гц.

Поиск, обнаружение и измерение параметров опасных сигналов осуществляется в широком диапазоне частот (от 50 Гц до 1 ГГц). Измерения проводятся в каждом сетевом проводе.

Полоса пропускания приемника, входящего в состав измерительной аппаратуры, выбирается в зависимости от решаемой задачи (обнаружение сигнала или измерение параметров сигнала), вида и параметров тестового сигнала, циркулирующего в контролируемом техническом средстве.

Измерение опасных напряжений в цепи заземления в диапазоне частот от 50 Гц до 1 МГц может осуществляться с помощью измерительной установки, структурная схема которой представлена на рис. 9.6.

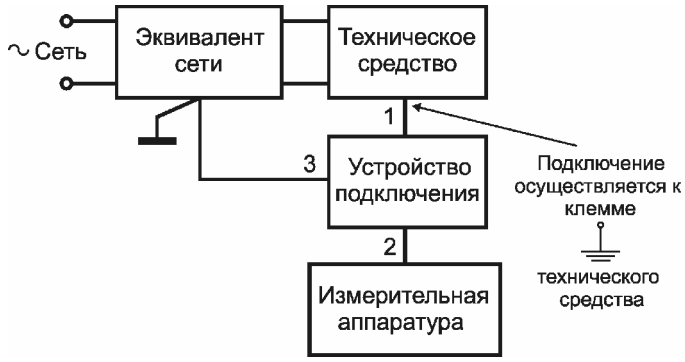

Рис. 9.6. Структурная схема измерения опасных напряжений в цепи заземления в диапазоне частот от 50 Гц до 1 МГц

В диапазоне частот от 1 МГц до 1 ГГц измерения могут проводиться на установке, структурная схема которой изображена на рис. 9.7.

Рис. 9.7. Структурная схема измерения опасных напряжений в цепи заземления в диапазоне частот от 1 МГц до 1 ГГц

В качестве устройства подключения здесь используется переменное измерительное сопротивление, выполненное по схеме, представленной на рис. 9.8.

Переменное измерительное сопротивление монтируется в экранированном корпусе. Номиналы сопротивлений R_1-R_5 выбираются в зависимости от величины входного сопротивления измерительной аппаратуры. Величина измерительного сопротивления $R_и$ равна

$$R_{и} = \sum_{i=1}^{k} R_i, k \in [1, 5]. \qquad (9.1)$$

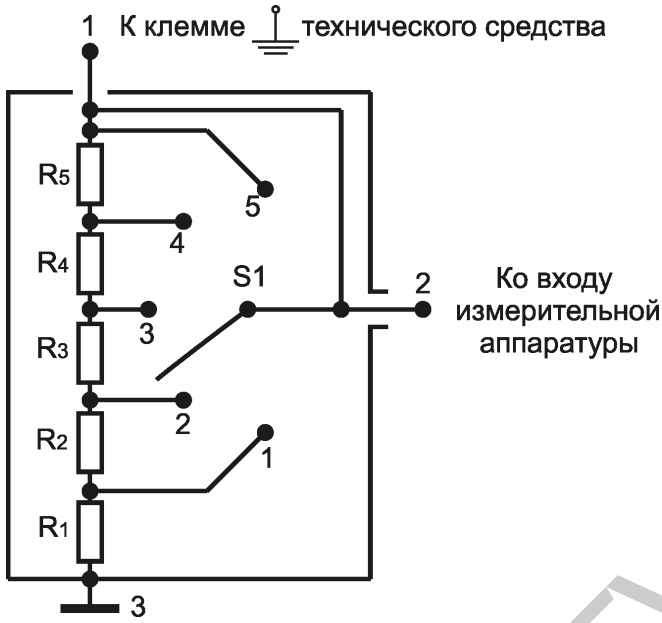

Рис. 9.8. Схема устройства подключения

Поиск опасных сигналов в диапазоне частот от 1 МГц до 1 ГГц осуществляется при максимальной величине измерительного сопротивления $R_и$ (на рис. 9.8 переключатель S1 в положение 5):

$$R_{и\,max} = \sum_{i=1}^{5} R_i \,. \qquad (9.2)$$

Если опасный сигнал обнаружен в диапазоне частот от 50 Гц до 1 МГц, то проводится расчет величины тока опасного сигнала $I_{ос}$, протекающего по заземляющему проводнику. С этой целью на каждой частоте, где обнаружен опасный сигнал, осуществляется измерение уровней его напряжения при всех возможных положениях переключателя S1 измерительного сопротивления. Результаты измерений фиксируются, и для каждого значения $R_и$ проводится расчет величины тока опасного сигнала $I_{ос}$:

$$I_{ос} = \frac{U_{ос}}{R_и}, R_и \in [R_{и\,min}\,, R_{и\,max}]. \qquad (9.3)$$

По результатам измерений и расчетов для каждой рабочей частоты осуществляется построение графика $I_{ос}= f(R_{изм})$ и определение с его помощью величины тока опасного сигнала при $R_{и} \to 0$.

Результаты измерений уровней напряжений (токов) опасных сигналов используются для расчета отношения «опасный сигнал/шум» в проверяемой цепи для каждой контролируемой частоты. Если это отношение не превышает требуемого для данного технического средства значения (нормы), определяемого нормативно-техническими документами, то считают, что возможность утечки информации за счет наводок опасных сигналов на контролируемые токоведущие цепи исключена. В противном случае необходимо предпринимать дополнительные меры защиты.

9.3. Технический контроль защиты объектов от утечки информации за счет высокочастотного навязывания

Проведение технического контроля защиты объектов от утечки информации за счет высокочастотного навязывания осуществляется путем воздействия на технические средства, функционирующие в тестовом режиме, высокочастотных (навязываемых) электромагнитных колебаний. Обнаружение в цепях технического средства или в окружающем его пространстве навязываемого высокочастотного сигнала, промодулированного тестовым сигналом, свидетельствует об утечке информации.

Генератор навязываемых высокочастотных сигналов подключается к телефонной линии через согласующее устройство, исключающее взаимовлияние аппаратуры навязывания и технического средства. В непосредственной близости от телефонного аппарата (ТА) размещают генератор тестового акустического сигнала, формирующий звуковой сигнал частотой f = 1000 Гц и заданным уровнем звукового давления.

При контроле явления навязывания в линии измерительная аппаратура подключается к этой линии через соответствующее входное устройство (рис. 9.9), обеспечивающее развязку линии и подключаемых к ней устройств.

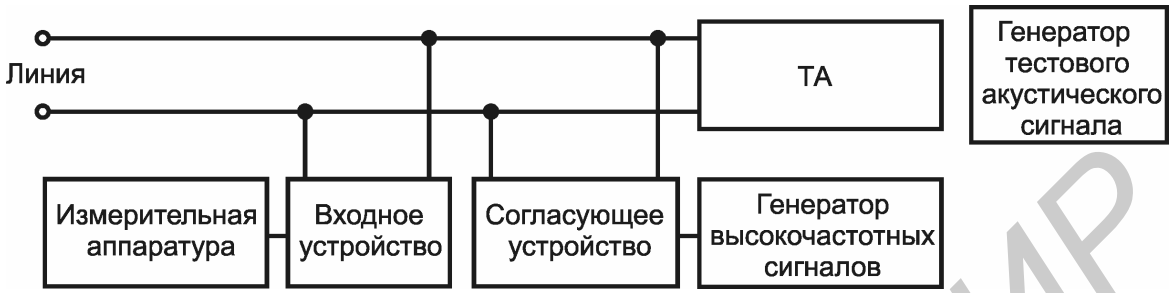

Рис. 9.9. Структурная схема контроля навязывания в линии

При контроле навязывания по полю прием излучаемых линией высокочастотных колебаний осуществляется с помощью измерительной антенны, подключаемой ко входу измерительного приемника.

Наличие на выходе измерительного приемника низкочастотного тестового сигнала частотой f = 1000 Гц свидетельствует о том, что канал утечки информации за счет высокочастотного навязывания существует.

При наличии посторонних проводов, имеющих параллельный пробег с проводами и соединительными линиями технического средства обработки информации, контроль защиты от утечки за счет навязывания проводится и в этих проводах, играющих в рассматриваемом случае роль случайных приемных антенн.

В таких ситуациях подключение измерительной аппаратуры к посторонним проводам, проходящим параллельно проводам или соединительным линиям контролируемого технического средства, также осуществляется через входные устройства (рис. 9.10).

Возможен вариант реализации высокочастотного навязывания путем подключения аппаратуры навязывания к посторонним проводам, имеющим параллельный пробег с проводами или соединительными линиями технических средств обработки информации. В этих случаях посторонние провода играют

роль случайных передающих и приемных антенн. Технический контроль защиты от утечки информации за счет навязывания в таких ситуациях может быть осуществлен путем подключения аппаратуры навязывания и аппаратуры контроля к этим посторонним проводам (рис. 9.11).

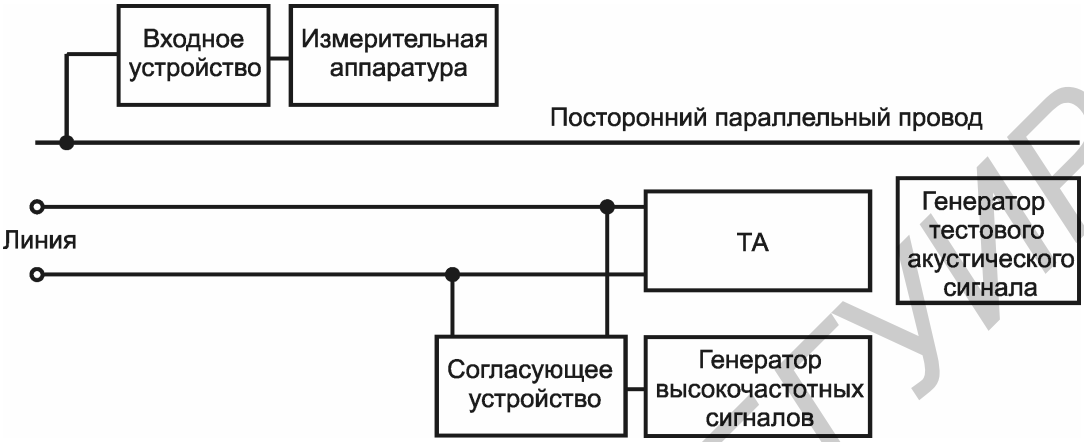

Рис. 9.10. Структурная схема контроля навязывания в посторонних параллельных проводах

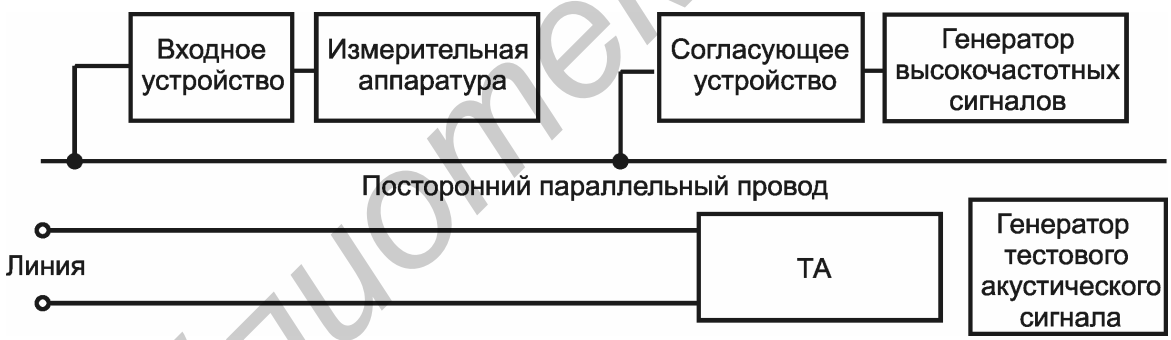

Рис. 9.11. Структурная схема контроля навязывания при подключении аппаратуры навязывания к посторонним параллельным проводам

Проведение технического контроля защиты систем и средств информатизации и связи от утечки информации за счет высокочастотного навязывания по соединительным проводам и линиям осуществляется в широком диапазоне частот навязываемых сигналов (до 400 МГц).

9.4. Технический контроль защиты объектов от утечки информации за счет электроакустических преобразований

Рассматриваемый вид технического контроля предназначен для обнаружения и измерения уровней опасных сигналов, возникающих в технических средствах обработки информации и соединительных линиях за счет микрофонного эффекта (т.е. за счет преобразования акустических колебаний в электрические сигналы).

К элементам технических средств, обладающим свойствами электроакустических преобразователей, относятся динамические головки громкоговорителей, микрофонные и телефонные капсюли, электрозвонки, электромагниты, трансформаторы и т.д.

С помощью генератора акустического сигнала формируется тональное звуковое колебание частотой f = 1000 Гц и определенным звуковым давлением в районе размещения технического средства на штатном месте эксплуатации (рис. 9.12).

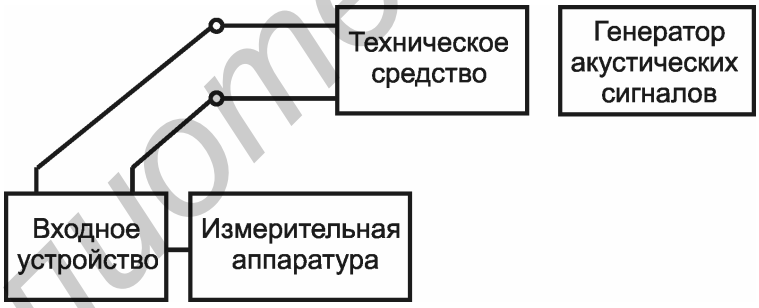

Рис. 9.12. Структурная схема контроля утечки информации за счет электроакустических преобразований

Измерительная аппаратура подключается к контролируемой линии через входное устройство экранированным проводом и настраивается на частоту 1000 Гц при минимальной полосе пропускания приемника. При наличии на выходе измерительного прибора сигнала необходимо убедиться в том, что этот сигнал обусловлен воздействием на техническое средство акустических

колебаний генератора (путем выключения генератора акустических колебаний), и зафиксировать измеренное значение напряжения.

Поиск, обнаружение и измерение уровня электрического сигнала на частоте f = 1000 Гц осуществляется во всех линиях, связанных с контролируемым техническим средством и выходящих за пределы контролируемой территории, включая провода и шины систем электропитания и заземления.

9.5. Технический контроль эффективности систем активного электромагнитного зашумления

Технический контроль эффективности систем активного зашумления заключается в измерении уровней побочных электромагнитных излучений контролируемого технического средства и излучений системы активного зашумления и определении отношения сигнал/шум на границе контролируемой территории.

При проведении контроля обеспечивается функционирование технического средства в тестовом режиме. Осуществляется поиск, обнаружение и измерение уровней электрической $E_{изм}$ и магнитной $H_{изм}$ составляющих побочных электромагнитных излучений этого средства. При выключенном техническом средстве проводится включение системы активного зашумления и измерение уровней электрической $E_{ш}$ и магнитной $H_{ш}$ составляющих маскирующих шумов на тех частотах, где были обнаружены побочные излучения технического средства. Для каждой из частот по результатам измерений проводится расчет отношения сигнал/шум $\frac{E_{изм}}{E_{ш}}\left(\frac{H_{изм}}{H_{ш}}\right)$ на границе контролируемой территории. Рассчитанные значения сравниваются с требуемыми значениями δ, определяемыми нормами защиты. Считают, что при выполнении условия $\frac{E_{изм}}{E_{ш}}\left(\frac{H_{изм}}{H_{ш}}\right) \le \delta$ требуемый уровень защиты обеспечен.

При использовании активных шумовых помех необходимо иметь в виду, что значения напряженности поля радиопомех, создаваемых системой активного зашумления, не должны превышать значений $E_{ш\ доп}$, определяемых нормами на уровни индустриальных радиопомех.

9.6. Технический контроль звукоизоляции помещений

Технический контроль звукоизоляции объектов осуществляется в целях определения ее соответствия требованиям, предъявляемым к помещениям, в которых проводятся закрытые мероприятия.

Источник звука размещается около стены помещения на расстоянии l_1 (рис. 9.13). Измерительная аппаратура размещается у противоположной стены на расстоянии l_2, сначала с внутренней, а затем с внешней стороны помещения.

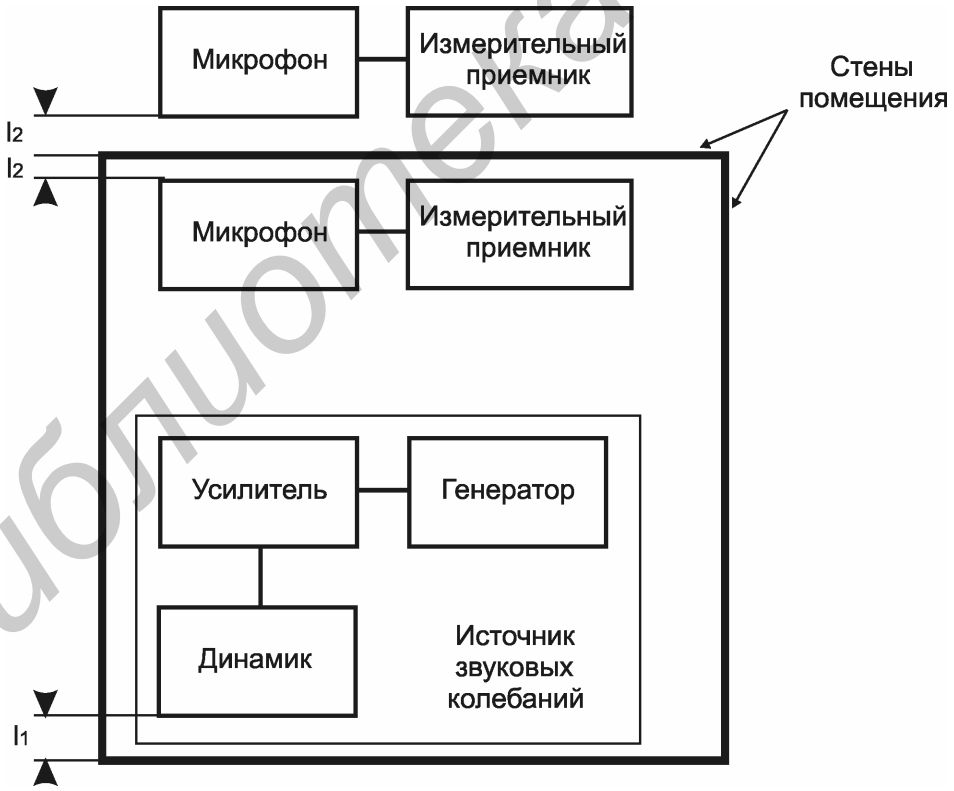

Рис. 9.13. Структурная схема контроля звукоизоляции помещений

Осуществляется установка требуемого уровня звукового давления, создаваемого источником звуковых колебаний. Проводится измерение уровня звукового давления $P_{пад}$ около стены внутри помещения на каждой частоте из заданного диапазона звуковых частот. Далее проводится измерение уровня звукового давления $P_{пр}$ около стены с внешней стороны помещения на каждой частоте.

Эффективность звукоизоляции помещения на каждой контролируемой частоте определяется в соответствии с выражением

$$Q = 20 \lg \frac{P_{пад}}{P_{пр}}, \left(Q_{[дБ]} = P_{пад[дБ]} - P_{пр[дБ]}\right). \qquad (9.4)$$

Измерения проводятся при закрытых дверях, окнах, форточках на каждой частоте в нескольких контрольных точках.

За эффективность звукоизоляции помещения принимается минимальное из всех полученных значений Q, определенных для каждой контролируемой частоты.

ЛИТЕРАТУРА

1. Поздняков, Е. Н. Защита объектов / Е. Н. Позняков. – М. : Концерн «Банковский деловой центр», 1997. – 224 с.

2. Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки / Ю. К. Меньшаков. – М. : Российский гуманитарный университет, 2002. – 399 с.

3. Торокин, А. А. Основы инженерно-технической защиты информации / А. А. Торокин. – М. : Изд-во «Ось-89», 1998. – 336 с.

4. Дамьяновски, В. CCTV. Библия охранного телевидения / В. Дамьяновски. – М. : Ай-эс-эс Пресс. 2003. – 344 с.

5. Гедзберг, Ю. Охранное телевидение / Ю. Гедзберг. – М. : «Горячая Линия – Телеком», 2006. – 312 с.

6. Конеев, И. Р. Информационная безопасность предприятия / И. Р. Конеев. – СПб. : БХВ-Петербург, 2003. – 752 с.

7. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. – 2-е изд. – Минск : Академический проект, 2005. – 544 с.

8. Бузов, Г. А. Защита от утечки информации по техническим каналам : учеб. пособие для подготовки экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : «Горячая линия – Телеком», 2005. – 416 с.

Учебное издание

Лыньков Леонид Михайлович
Борботько Тимофей Валентинович
Мухуров Николай Иванович

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Н. В. Гриневич*
Корректор *М. В. Тезина*
Компьютерная верстка *Е. Н. Мирошниченко*

Подписано в печать 21.11.2007. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Печать ризографическая. Усл. печ. л. 8,25. Уч.-изд. л. 5,8. Тираж 100 экз. Заказ 384.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6