**Министерство образования Республики Беларусь**

**Учреждение образования**

**«Белорусский государственный университет**

**информатики и радиоэлектроники»**

**Кафедра защиты информации**

**Г. В. Сечко**

**Лекции по курсу:**

**«Основы защиты информации».**

**для студентов ИИТ**

**Минск 2015**

**Лекция 1. Системная методология информационной безопасности**

* 1. Основные понятия и терминология (подраздел заимствован из [9])

Ученые, анализируя тот или иной отрезок истории развития человеческого общества, присваивают ему краткое наименование, в основе которого лежит наиболее характерное свойство, присущее именно данному отрезку истории. Известны различные классификации, например, по технологическим признакам. Если следовать технологической классификации, то сегодня человечество переходит от индустриального общества к информационному. Информация из абстрактного "знания" превращается в материальную силу. Информационные технологии коренным образом изменили облик материального производства, позволили экономить материальные ресурсы, создали новые приборы и системы, в буквальном смысле изменили наши представления о времени и пространстве.

Однако широкое внедрение в жизнь информационных технологий, управляющих жизненно важными процессами, к сожалению, сделало их достаточно уязвимыми со стороны естественных воздействий среды и искусственных воздействий со стороны человека. Возникла проблема обеспечения безопасности информационных систем.

Рассмотрим основные понятия и термины науки о защите информации. Под **информацией** будем понимать сведения о лицах, предметах, фактах, событиях, явлениях и процессах. Информация может существовать в виде бумажного документа, физических полей и сигналов (электромагнитных, акустических, тепловых и т.д.), биологических полей (память человека) и в других видах. В дальнейшем будем рассматривать информацию в документированной (на бумаге, дискете и т. д.) форме и в форме физических полей (радиосигналы, акустические сигналы и т.д.). Среду, в которой информация создается, передается, обрабатывается или хранится, будем называть **информационным объектом (ИО)***.*

Под **безопасностью ИО** понимается его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования. Природа воздействия на ИО будет рассмотрена далее. Все воздействия, нарушающие нормальный процесс функционирования ИО, могут привести к последствиям (ущербу) трех видов: нарушению конфиденциальности, целостности, доступности.

**Нарушение конфиденциальности** — нарушение свойства информации быть известной только определенным субъектам.

**Нарушение целостности** — несанкционированное изменение, искажение, уничтожение информации.

**Нарушение доступности (отказ в обслуживании)** — нарушаются доступ к информации, работоспособность объекта, доступ в который получил злоумышленник.

В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ. Суть несанкционированного доступа состоит в получении нарушителем доступа к объекту в нарушение установленных правил.

Под **угрозой информационной безопасности объекта** будем понимать возможные воздействия на него, приводящие к ущербу. Другие определения угроз даны в презентации «Угрозы и уязвимости». Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть **уязвимостью**. Другие определения уязвимости даны в презентации «Угрозы и уязвимости». Действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости, будем называть**атакой***.* Целью защиты информационного объекта является противодействие угрозам безопасности.

**Защищенный информационный объект** — это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

**Комплексная защита ИО** — совокупность методов и средств (правовых, организационных, физических, технических, программных).

**Политика безопасности** — совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от заданного множества угроз безопасности.

* 1. Задачи в сфере обеспечения информационной безопасности

Основные задачи изложены в Законе об информации, информатизации и защите информации, выдержки из которого даны в [1]. Это

1.2.1 Предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы;

1.2.2 Сохранение полноты, точности, целостности документированной информации, возможности управления процессом обработки и пользования в соответствии с условиями, установленными собственником этой информации или уполномоченным им лицом;

1.2.3 Обеспечение прав физических и юридических лиц на сохранение конфиденциальности документированной информации о них, накапливаемой в информационных системах;

1.2.4 Защита прав субъектов в сфере информатизации;

1.2.5 Сохранение секретности, конфиденциальности документированной информации в соответствии с правилами, определенными настоящим Законом об информатизации и иными законодательными актами.

Для достижения поставленных задач необходимы

1.2.6 Разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка, реализация и уточнение концепции правового обеспечения информационной безопасности РБ;

1.2.7 Принятие и реализация общегосударственных программ, предусматривающих формирование общедоступных архивов информационных ресурсов органов государственной власти и местных органов управления, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства Беларуси, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти и местных органов управления, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

1.2.8 Развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РБ;

1.2.9 Гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

1.3 Охраняемые сведения и демаскирующие признаки

В Законе об информатизации указано, что собственник информационной системы или уполномоченные им лица обязаны обеспечить уровень защиты документированной информации в соответствии с требованиями Закона и иных актов законодательства. Информационные ресурсы, имеющие государственное значение, должны обрабатываться только в системах, обеспеченных защитой, необходимый уровень которой подтвержден сертификатом соответствия. Защита другой документированной информации устанавливается в порядке, предусмотренном ее собственником или собственником информационной системы. Собственник или владелец информационной системы обязан сообщать собственнику информационных ресурсов обо всех фактах нарушения защиты информации

государственные секреты;

В вышеназванном аспекте к охраняемым (защищаемым) сведениям относятся:

1.3.1 **Государственные секреты** (сведения, составляющие государственные секреты) — сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с Законом «О государственных секретах» (см. лекцию 2) и другими актами законодательства Республики Беларусь, а также с**лужебная информация ограниченного распространения**. Государственные секреты являются собственностью Республики Беларусь (см. Закон РБ "О государственных секретах"). Государственные секреты Республики Беларусь подразделяются на две категории: государственная тайна и служебная тайна.

**Государственная тайна** (сведения, составляющие государственную тайну) — сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь (статья 16 Закона РБ "О государственных секретах").

**Служебная тайна** — сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь. Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

**Служебная информация ограниченного распространения** - сведения, распространение которых в соответствии с действующим законодательством РБ организации считают нежелательными в интересах своей деятельности (см. Постановление Совета Министров "О служебной информации ограниченного распространения»). На документах, содержащих такую информацию, проставляется гриф "Для служебного пользования". В постановлении приводится перечень сведений ограниченного распространения:

— мобилизационные вопросы;

— наука и техника;

— оборона и государственная безопасность;

— правоохранительная деятельность.

* + 1. Коммерческая информация
    2. Персональная информация.

Все перечисленные сведения уязвимы и могут быть подвергнуты атаке злоумышленников. Демаскирующие признаки таких атак рассмотрим более подробно на примере защищаемой коммерческой и персональной информации. В условиях глобальной информатизации общества на основе создания и совершенствования новых информационных технологий, единых локальных вычислительных сетей (ЛВС) предприятия и телекоммуникационных мегасетей (типа Internet), к которым подключены рядовые «юзеры», злоумышленники пытаются маскировать свою атаку на чужую коммерческую и персональную информацию.

Демаскирующими признаками атак злоумышленников являются: а) повтор определенных событий; б) неправильные или несоответствующие текущей ситуации команды; в) признаки работы средств анализа уязвимостей; г) несоответствующие параметры сетевого трафика; д) непредвиденные атрибуты; е) необъяснимые проблемы.

*Повтор определенных событий.* Злоумышленник, пытаясь осуществить несанкционированное проникновение, вынужден совершать определенные действия несколько раз, т.к. с одного раза он не достигает своей цели. Например, подбор пароля при аутентификации; сканирование портов с целью обнаружения открытых из них и т.д.

*Неправильные или несоответствующие текущей ситуации команды.* Обычно это обнаружение неправильных запросов или ответов, ожидаемых от автоматизированных процессов и программ. Например, в процессе аутентификации почтовых клиентов системы вместо традиционных процедур вдруг обнаружены иные команды. При анализе оказалось, что Злоумышленник пытался получить доступ к файлу паролей почтового шлюза.

*Признаки работы средств анализа уязвимостей.* Имеется ряд средств автоматизированного анализа уязвимостей сети: nmap, Internet Scanner и др., которые в определенном порядке обращаются к различным портам с очень небольшим интервалом времени. Такие обращения являются признаками атак.

*Несоответствующие параметры сетевого трафика.* Примеры несоответствующихпараметров входного и выходного трафика: 1) в ЛВС приходят из внешней сети пакеты, имеющие адреса источника, соответствующие диапазону адресов внутренней сети. 2. Из ЛВС выходят пакеты с адресом источника, находящегося во внешней сети. 3. Адрес источника запрещен, адрес источника и получателя совпадают. 4. Некорректные значения параметров различных полей сетевых пакетов (взаимоисключающие флаги). 5. Аномалии сетевого трафика (параметры сетевого трафика отличатся от традиционных: коэффициент загрузки, размер пакета, среднее число фрагментированных пакетов, использование нетипичного протокола).

*Непредвиденные атрибуты*. Их признаками являются: 1) отклонения от типового профиля запросов пользователей, отклонения от их типовых действий, 2) нетипичные время и дата – например, работа в нерабочее время, в выходные, в отпуске – это тоже признак непредвиденных атрибутов, 3) нетипичное местоположение пользователя, нетипичные запросы сервисов и услуг.

*Необъяснимые проблемы.* Проблемы с программным и аппаратным обеспечением, с системными ресурсами, с производительностью.

1.4 Угрозы информационной безопасности и их классификация по виду, происхождению, источникам и характеру возникновения

Определение – п. 1.1. К настоящему времени известно большое количество угроз. Приведем их классификацию по различным классификационным признакам [1]:

По виду:

— физической и логической целостности (уничтожение или искажение информации);

— конфиденциальности (несанкционированное получение);

— доступности (работоспособности);

— права собственности;

По происхождению:

— случайные (отказы, сбои, ошибки, стихийные явления);

— преднамеренные (злоумышленные действия людей);

По источникам:

— люди (персонал, посторонние);

— технические устройства;

— модели, алгоритмы, программы;

— внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Рассмотрим более подробно перечисленные угрозы.

**Случайные угрозы** обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).

**Преднамеренные угрозы** связаны с действиями людей (работники спецслужб, самого объекта, хакеры). Огромное количество разнообразных информационных объектов делает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов. Например, для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться:

— штатными каналами доступа, если нет никаких мер защиты;

— через терминалы пользователей;

— через терминал администратора системы;

— через удаленные терминалы,

или нештатными каналами доступа:

— побочное электромагнитное излучение информации с аппаратуры системы;

— побочные наводки информации по сети электропитания и заземления;

— побочные наводки информации на вспомогательных коммуникациях;

— подключение к внешним каналам связи.

Несколько отличается от классификации [1] популярная в литературе общая классификация угроз в зависимости от их источника и происхождения, показанная на рис. 1.1 и более подробная, приведенная в в табл. 1.1

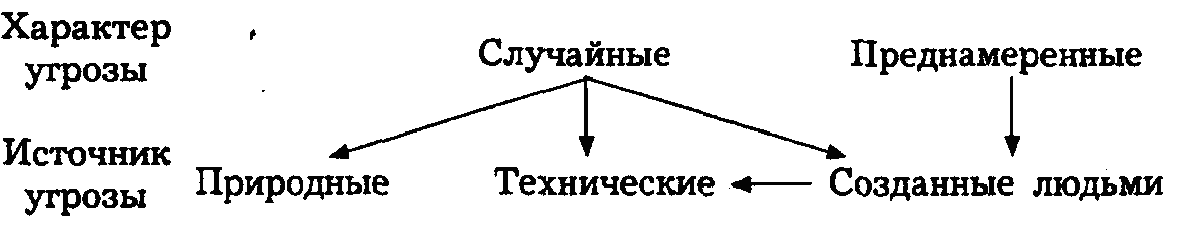
**

Рис. 1.1 – Возможная общая классификация угроз безопасности

Таблица 1.1 – Возможная подробная классификация угроз информационной безопасности в зависимости от их источника и происхождения

|  |  |  |
| --- | --- | --- |
| Природные угрозы (1) | Угрозы техногенного характера (2) | Угрозы, созданные людьми (3) |
| 1.1. Стихий-ные бедствия  1.2. Магнит-ные бури  1.3. Радио-активные излучения и осадки  1.4. Другие угрозы | 2.1. Сбои в работе КС, вызванные отключением или колебанием электропитания или другими средствами функционирования КС  2.2. Отказы и сбои КС вследствие её ненадёжности  2.3. Электромагнитные излучения и наводки  2.4. Утечки через каналы связи – электрические, акустические, оптические и др.  2.5. Другие угрозы | 3.1. Непреднамеренные действия:  3.1.1. Обслуживающего персонала  3.1.2. Пользователей  3.1.3. Архивной службы  3.1.4. Службы безопасности  3.1.5. Управленческого персонала  3.1.6. Других людей  3.2. Преднамеренные действия:  3.2.1–3.2.5. Лиц по пунктам 3.1.1–3.1.5.  3.2.6. Хакерские атаки  3.2.7. Другие угрозы |

Другие виды классификации будут рассмотрены на практическом занятии. Ни одна из классификаций не свободна от недостатков.

1.5 Классификация методов защиты информации, в том числе по характеру проводимых мероприятий

Здесь также возможны различные виды классификаций по различным классификационным признакам. Рассмотрим классификацию из [1].

Все методы защиты информации по характеру проводимых действий можно разделить на:

— законодательные (правовые);

— организационные;

— технические;

— комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

**Лекция 2 Правовое и нормативное обеспечение защиты информации**

2.1 Правовое и нормативное обеспечение защиты информации

Программно-технические методы защиты информации, какими бы совершенными они ни были, в полном объеме не решают задач комплексной защиты объектов информационной безопасности. Используемые при этом физические, аппаратные, программные, криптографические и иные логические и технические средства и методы защиты выполняются без участия человека по заранее предусмотренной процедуре. Для обеспечения комплексного подхода к обеспечению защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Основные правовые акты, регламентирующие защиту информации в Республике Беларусь:

*КОНЦЕПЦИЯ национальной безопасности  Республики Беларусь*, утв. Указом Президента РБ от 9 ноября 2010 г. №575

Закон РБ от 10 ноября 2008 г. N 455-З *«Об информации, информатизации и защите информации»,*

Закон РБ от 19 июля 2010 г. N 170-З "*О государственных секретах*",

Закон РБ от 3 декабря 1997 г. № 102‑З "*Об органах государственной безопасности Республики Беларусь*",

Постановление Совета Министров РБ от 15 февраля 1999 г. № 237 "*О служебной информации ограниченного распространения*",

Постановление Совета Министров РБ от 10 февраля 2000 г. № 186 "*О некоторых мерах по защите информации в Республике Беларусь*".

К нормативному обеспечению защиты информации относятся межнациональные и национальные стандарты и другие нормативные документы, например, профили защиты. Примеры межнациональных стандартов – стандарты [1], национальных – [1]. Рассмотрим более подробно правовое обеспечение защиты информации в Беларуси.

2.2.Концепция национальной безопасности. Законы «Об информации, информатизации и защите информации», «О государственных секретах», «Об органах государственной безопасности Республики Беларусь»

*2.2.1 Концепция национальной безопасности.* С точки зрения защиты информации наиболее важной главой Концепции является ГЛАВА 8 Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности, в том числе следующие статьи

49. В политической сфере нейтрализация внутренних источников угроз национальной безопасности обеспечивается…

50. Необходимым условием нейтрализации внутренних источников угроз национальной безопасности в экономической сфере…

54. В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий….

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность….

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия РБ в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий

2.2.2 *Закон «Об информации, информатизации и защите информации»* регулирует правоотношения, возникающие в процессе формирования и использования документированной информации информационных ресурсов; создания информационных технологий, автоматизированных или автоматических информационных систем и сетей; определяет порядок защиты информационного ресурса, а также прав и обязанностей субъектов, принимающих участие в процессах информатизации. Термины, используемые в Законе, и их определения приведены в прилагаемом к лекции тексте Закона. Ниже приведены названия наиболее важных глав и статей, которые содержатся в рассматриваемом Законе. Это:

Глава 7. ЗАЩИТА ИНФОРМАЦИИ, в том числе

Статья 27. Цели защиты информации

Статья 28. Основные требования по защите информации

Статья 29. Меры по защите информации

Статья 30. Организация защиты информации

Статья 31. Права и обязанности субъектов информационных отношений по защите информации

Глава 8. Права и обязанности субъектов информационных отношений. ответственность за нарушение требований законодательства об информации, информатизации и защите информации, в том числе

Статья 33. Права и обязанности обладателя информации

Статья 34. Права и обязанности пользователя информации

Статья 35. Права и обязанности пользователя информационной системы и (или) информационной сети

Статья 36. Права и обязанности собственника информационных ресурсов

Статья 41. Ответственность за нарушение законодательства об информации, информатизации и защите информации

КонсультантПлюс: примечание.

Ответственность за совершение административных правонарушений в области информации предусмотрена [гл. 22](consultantplus://offline/belorus?base=RLAW425;n=107480;fld=134;dst=101578) Кодекса Республики Беларусь об административных правонарушениях; ответственность за совершение преступлений против информационной безопасности предусмотрена [гл. 31](consultantplus://offline/belorus?base=RLAW425;n=108334;fld=134;dst=102037) Уголовного кодекса Республики Беларусь.

Нарушение законодательства об информации, информатизации и защите информации влечет ответственность в соответствии с законодательными актами Республики Беларусь.

Содержание вышеперечисленных статей приведено в прилагаемом к лекции тексте Закона

2.2.3 *Закон "О государственных секретах".* Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации по всем вопросам жизнедеятельности государства и общества. Наряду с этим требуется ограничение распространения определенных сведений, относящихся к обеспечению национальных интересов государства и общества, их безопасности и обороноспособности, преждевременное предание гласности которых может нанести ущерб Республике Беларусь.

Настоящий Закон определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь. Полный текст Закона прилагается.

Основные понятия, применяемые в законе: **Государственные секреты** — см. п. 1.3.1 этого конспекта лекций. Категории государственных секретов, а также определение понятий **«Государственная тайна» и**  «**Служебная тайна»** — см. п. 1.3.1 этого конспекта лекций.

Особый интерес в Законе представляет ГЛАВА 4 Сведения, которые могут быть отнесены либо не могут быть отнесены к государственным секретам. В частности, к государственным секретам могут быть отнесены:

сведения в области политики:

о стратегии и тактике внешней политики, а также внешнеэкономической деятельности;

о подготовке, заключении, содержании, выполнении, приостановлении или прекращении действия международных договоров Республики Беларусь;

об экспорте и импорте вооружения и военной техники; и т. д.

К государственным секретам не могут быть отнесены сведения:

являющиеся общедоступной информацией, доступ к которой, распространение и (или) предоставление которой не могут быть ограничены в соответствии с законодательными актами Республики Беларусь;

находящиеся в собственности иностранных государств, международных организаций, межгосударственных образований и переданные Республике Беларусь.

Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются следующие степени секретности:

для государственной тайны - "Особой важности", "Совершенно секретно";

для служебной тайны - "Секретно".Присвоение указанным носителям государственных секретов других ограничительных грифов, не предусмотренных настоящей статьей, запрещается.

В отсутствие этого закона двести лет назад одна очень известная француженка, имеющая отца-преуспевающего экономиста, высказалась о секретах и тайнах в российской империи, куда входила Беларусь, следующим образом:

В России все – секретно, и ничто не тайна.

*Мадам де Сталь*

(Анна Луиза Жермена де Сталь (1766–1817), французская писательница (романы «Джейн Грей» /1790/, «Дельфина» /1802/, «Коринна или Италия» /1807/), теоретик литературы, публицист (проблемы революции и литературы), рекомендовала главе французской Директории Баррасу претендента на должность министра иностранных дел (Талейрана), дочь известного французского финансиста, затем министра финансов Франции Жака Некера (1732–1804), который разбогател, работая в банке, с помощью умелых финансовых операций

2.2.4 Закон "Об органах государственной безопасности Республики Беларусь". Этот Закон определяет правовые основы, принципы, основные задачи и направления деятельности органов государственной безопасности Республики Беларусь:

Организация и обеспечение криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в Республике Беларусь и ее учреждениях за рубежом, осуществление государственного контроля за этой деятельностью;

Обеспечение государственных органов, предприятий, учреждений и организаций правительственной и оперативной связью, а также организация и обеспечение криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в Республике Беларусь и ее учреждениях за рубежом, осуществление государственного контроля за этой деятельностью.

Правительственная и оперативная связь (обеспечение). Правительственная (телефонная и документальная) и оперативная (телефонная) связь являются специальными системами электрической связи, обеспечивающими секретность передаваемой по ним информации. Правительственная связь организуется в интересах государственных органов. Оперативная связь организуется в интересах правоохранительных органов. Подразделения правительственной связи органов государственной безопасности обеспечивают государственные органы, предприятия, учреждения и организации правительственной и оперативной связью, а также организуют деятельность республиканских органов государственного управления, предприятий, учреждений и организаций по обеспечению криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в Республике Беларусь и ее учреждениях за рубежом, осуществляют государственный контроль за этой деятельностью. Они должны:

Осуществлять контроль в пределах своей компетенции за использованием на территории Республики Беларусь излучающих радиоэлектронных средств любого назначения и запрещать использование этих средств, работающих с нарушением установленных правил обращения с информацией, составляющей государственную тайну, либо создающих радиопомехи функционированию средств правительственной и оперативной радиосвязи;

Осуществлять государственный контроль за состоянием криптографической и инженерно-технической безопасности шифрованной, засекреченной и кодированной связи в государственных органах, на предприятиях, в учреждениях и организациях независимо от их ведомственной принадлежности, а также секретно-шифровальной работы в учреждениях Республики Беларусь, находящихся за рубежом.

2.3 Постановления Совета Министров РБ «О служебной информации ограниченного распространения», «О некоторых мерах по защите информации в Республике Беларусь», регулирующие защиту служебной информации и правовую защиту от компьютерных преступлений

2.3.1. Определение служебной информации ограниченного распространения и состав входящих в неё сведений в соответствии с Постановлением Совета Министров РБ «О служебной информации ограниченного распространения» приведены в п. 1.3.1 этого конспекта лекций.

*2.3.2 Постановление Совета Министров РБ* «О некоторых мерах по защите информации в Республике Беларусь» констатирует, что при обработке информации, отнесенной к госсекретам и служебной информации ограниченного распространения с использованием средств электронно-вычислительной техники, должны применяться защищенные по требованиям безопасности информации компьютерные системы, изготавливаемые, как правило, на предприятиях РБ. В обоснованных случаях могут применяться компьютерные системы импортного производства, прошедшие специальные исследования и обеспеченные защитой, необходимый уровень которой подтвержден сертификатом соответствия.

*2.3.3 Правовая защита от компьютерных преступлений*. В 1983 г. Международная организация экономического сотрудничества и развития определила под термином *"компьютерная преступность"* (или "связанная с компьютерами преступность") любые незаконные, неэтичные или неправомерные действия, связанные с автоматической обработкой данных и/или их передачей.

Данный термин, возникший первоначально как средство для обозначения появившихся новых способов совершения преступлений, по своему содержанию давно уже перерос в криминологическое понятие, обозначающее самостоятельный вид преступности. В настоящее время этот вид преступности включает в себя в зависимости от уголовно-правового регулирования в тех или иных странах уже целый перечень такого рода деяний и способов их совершения.

С целью унификации национальных законодательств в 1989 г. Комитетом министров Европейского Совета был согласован и утвержден Список правонарушений, рекомендованный странам - участницам ЕС для разработки единой уголовной стратегии по разработке законодательства, связанного с компьютерными преступлениями. Рекомендованный Европейским Советом Список компьютерных преступлений включает в себя так называемые “Минимальный” и “Необязательный списки нарушений”.

2.4. «Минимальный» и «необязательный список нарушений» в компьютерной сфере

"Минимальный список нарушений" содержит следующие восемь видов компьютерных преступлений:

2.4.1 *Компьютерное мошенничество*. Это ввод, изменение, стирание или повреждение данных ЭВМ или программ ЭВМ, или же другое вмешательство в ход обработки данных, которое влияет на результат обработки данных таким образом, что служит причиной экономических потерь или вызывает состояние потери имущества другого человека с намерением незаконного улучшения экономического положения для себя или другого человека (или как альтернатива с намерением к незаконному лишению этого человека его имущества).

2.4.2 *Подделка компьютерной информации.* Это несанкционированное стирание, повреждение, ухудшение или подавление данных ЭВМ или программ ЭВМ, или другое вмешательство в ход обработки данных различными способами, или создание таких условий, которые будут, согласно национальному законодательству, составлять такое правонарушение, как подделка в традиционном смысле такого нарушения.

2.4.3 *Повреждение данных ЭВМ или программ ЭВМ*. Это несанкционированное стирание, повреждение, ухудшение или подавление данных ЭВМ или программ ЭВМ.

2.4.4 *Компьютерный саботаж*. Это ввод, изменение, стирание, повреждение данных ЭВМ или программ ЭВМ, или вмешательство в системы ЭВМ с намерением препятствовать функционированию компьютера или системы передачи данных.

2.4.5 *Несанкционированный доступ*. Это несанкционированный доступ к системе ЭВМ через сеть с нарушением средств защиты.

2.4.6 *Несанкционированный перехват данных*. Это несанкционированный перехват данных с помощью технических средств связи как в пределах компьютера, системы или сети, так и извне.

2.4.7 Несанкционированное использование защищенных компьютерных программ. Это незаконное воспроизведение, распространение программ или связь с программой ЭВМ, которая защищена в соответствии с законом.

2.4.8 Несанкционированное воспроизведение схем. Это несанкционированное воспроизведение схемных решений, защищенных в соответствии с законом о полупроводниковых изделиях (программах), или коммерческая эксплуатация или незаконное импортирование для той же цели схемы или полупроводникового изделия как продукта, произведенного с использованием данных схем.

"Необязательный список нарушений" включает в себя следующие четыре вида компьютерных преступлений:

2.4.9 Незаконное изменение данных ЭВМ или программ ЭВМ.

2.4.10 Компьютерный шпионаж.

2.4.11 Приобретение с использованием незаконных средств или путем несанкционированного раскрытия, пересылка или использование торговых или коммерческих секретов при помощи подобных методов или других незаконных средств с тем или иным намерением, наносящим экономический ущерб человеку путем доступа к его секретам или позволяющим получить незаконное экономическое преимущество для себя или другого человека;

2.4.12 Неразрешенное использование ЭВМ. Использование системы ЭВМ или компьютерной сети без соответствующего разрешения является преступным, когда оно:

инкриминируется в условиях большого риска потерь, вызванных неизвестным лицом, использующим систему или наносящим вред системе или ее функционированию;

инкриминируется неизвестному лицу, имеющему намерение нанести ущерб и использующему для этого систему или наносящему вред системе или ее функционированию;

применяется в случае, когда теряется информация с помощью неизвестного автора, который использовал данную систему или нанес вред системе или ее функционированию.

Использование без разрешения защищенной программы ЭВМ или ее незаконное воспроизводство с намерением исправить программу таким образом, чтобы вызвать незаконную экономическую выгоду для себя или другого человека, или причинить вред законному владельцу данной программы, также является преступлением.

2.5 Глава «Преступления против информационной безопасности» модельного Уголовного Кодекса государств-участников СНГ

В 1995 г. рабочей группой Программного комитета СНГ был подготовлен модельный Уголовный кодекс для государств - участников СНГ, содержащий специальную главу "Преступления против информационной безопасности'". в которую были включены следующие составы компьютерных преступлений. Ниже приведены названия наиболее важных статей этой главы. Это:

Статья 286. Несанкционированный доступ к компьютерной информации

Статья 287. Модификация компьютерной информации

Статья 288. Компьютерный саботаж

Статья 289. Неправомерное завладение компьютерной информацией

Статья 290. Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Статья 291. Разработка, использование и распространение вредоносных программ

Статья 292. Нарушение правил эксплуатации компьютерной системы или сети

Некоторые из сформулированных в модельном Уголовном кодексе составов компьютерных преступлений нашли свое отражение в проектах Уголовных кодексов государств - участников СНГ. Так, в проект Уголовного кодекса Российской Федерации включена глава "Преступления против информационной безопасности", содержащая следующие составы преступлений.

Статья 62. Неправомерный доступ к компьютерной информации

Статья 63. Создание, использование и распространение вирусных программ

Статья 64. Нарушение правил эксплуатации компьютерной системы или сети

В новом Уголовном кодексе Республики Беларусь, принятом в 1999 году, в раздел XII "Преступления против информационной безопасности" включена глава 31 "Преступления против информационной безопасности", которая содержит следующие составы компьютерных преступлений.

Статья 349. Несанкционированный доступ к компьютерной информации

Статья 350. Модификации компьютерной информации

Статья 351. Компьютерный саботаж

Статья 352. Неправомерное завладение компьютерной информацией

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Статья 354. Разработка, использование либо распространение вредоносных программ

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

В раздел VIII нового Уголовного кодекса Республики Беларусь включена глава 24 "Преступления против собственности", которая содержит следующие составы компьютерных преступлений.

Статья 212. Хищение путем использования компьютерной техники

Статья 216. Причинение имущественного ущерба без признаков хищения

Содержание вышеперечисленных статей вышеназванных документов приведено в прилагаемой к конспекту книге В.Ф.Голикова 2004 г.

**Лекция 3 Организационные методы защиты информации**

3.1 Государственное регулирование в области защиты информации

В соответствии со статьёй 7 Закона «Об информации, информатизации и защите информации» государственное регулирование в области информации, информатизации и защиты информации включает:

обеспечение условий для реализации и защиты прав государственных органов, физических и юридических лиц;

создание системы информационной поддержки решения задач социально-экономического и научно-технического развития Республики Беларусь;

создание условий для развития и использования информационных технологий, информационных систем и информационных сетей на основе единых принципов технического нормирования и стандартизации, оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

формирование и осуществление единой научной, научно-технической, промышленной и инновационной политики в области информации, информатизации и защиты информации с учетом имеющегося научно-производственного потенциала и современного мирового уровня развития информационных технологий;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов в области информации, информатизации и защиты информации;

содействие развитию рынка информационных технологий и информационных услуг, обеспечение условий для формирования и развития всех видов информационных ресурсов, информационных систем и информационных сетей;

обеспечение условий для участия Республики Беларусь, административно-территориальных единиц Республики Беларусь, государственных органов, физических и юридических лиц в международном сотрудничестве, включая взаимодействие с международными организациями, обеспечение выполнения обязательств по международным договорам Республики Беларусь;

разработку и обеспечение реализации целевых программ создания информационных систем, применения информационных технологий;

совершенствование законодательства Республики Беларусь об информации, информатизации и защите информации;

иное государственное регулирование.

Государство занимает важное место в системе защиты информации в любой стране, в том числе и в Беларуси. Государственная политика обеспечения информационной безопасности исходит из следующих положений:

ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

юридические и физические лица, собирающие, накапливающие и обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

государство формирует национальную программу информационной безопасности и объединяет усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности страны;

государство формирует нормативно‑правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем;

государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации, и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов.

3.2 Государственная политика информационной безопасности

Согласно прилагаемой к конспекту книге В.Ф.Голикова 2004 г. первоочередные мероприятия по реализации государственной политики информационной безопасности должны включать:

создание нормативно‑правовой базы реализации государственной политики в области информационной безопасности, в том числе определение последовательности и порядка разработки законодательных и нормативно‑правовых актов, а также механизмов практической реализации принятого законодательства;

анализ технико-экономических параметров отечественных и зарубежных программно‑технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники;

формирование государственной научно‑технической программы совершенствования и развития методов и средств обеспечения информационной безопасности, предусматривающей их использование в национальных информационных и телекоммуникационных сетях и системах с учетом перспективы вхождения страны в глобальные информационные сети и системы;

создание системы сертификации на соответствие требованиям информационной безопасности отечественных и закупаемых импортных средств информатизации, используемых в государственных органах власти и управления.

Мероприятия по защите информации осуществляются как за счет бюджетных ассигнований, выделяемых целевым назначением, так и за счет средств предприятий, учреждений и организаций независимо от форм собственности. Финансирование НИОКР в области защиты информации, производства средств защиты информации и контроля эффективности защиты осуществляется за счет госбюджетных ассигнований, выделяемых целевым назначением гензаказчику, а также средств предприятий, учреждений и организаций различных форм собственности и частных лиц. Генеральным заказчиком технических, программных, программно-аппаратных и криптографических средств защиты информации, аппаратуры контроля эффективности защиты информации общего применения и научно-технической продукции по общесистемным исследованиям проблем защиты информации является Оперативно-аналитический центр при Президенте Республики Беларусь в области защиты информации (бывший ГЦБИ).

3.3 Состав государственной системы защиты информации РБ

Согласно прилагаемой к конспекту книге В.Ф.Голикова 2004 г. система информационной безопасности является составной частью общей системы национальной безопасности страны и представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих деятельность по обеспечению информационной безопасности. В систему входят:

органы государственной власти и управления, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

структурные и межотраслевые подразделения по защите информации органов государственной власти и управления, а также структурные подразделения предприятий, проводящие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся на проведении работ в области защиты информации;

научно-исследовательские, проектные и конструкторские организации, выполняющие работы по обеспечению информационной безопасности;

учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

Государственную систему защиты информации Республики Беларусь составляют:

Оперативно-аналитический центр при Президенте Республики Беларусь в области защиты информации (бывший Государственный центр безопасности информации при Совете Безопасности РБ, ГЦБИ);

структурные подразделения по защите информации органов государственного управления, предприятий, организация и учреждений;

головные предприятия (организации, учреждения) по направлениям защиты информации,

сертификационные и испытательные центры (лаборатории), предприятия, учреждения и организации различных форм собственности по оказанию услуг в области защиты информации.

Основными функциями системы информационной безопасности страны являются:

разработка и реализация стратегии обеспечения информационной безопасности;

оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения и нейтрализации этих угроз;

координация и контроль деятельности субъектов системы информационной безопасности.

3.4 Лицензирование деятельности юридических и физических лиц по защите информации

Согласно прилагаемой к конспекту книге В.Ф.Голикова 2004 г. деятельность юридических и физических лиц по защите информации лицензируется. Положение о лицензировании в области защиты информации разработано Оперативно-аналитическим центром при Президенте Республики Беларусь в области защиты информации. Эта же организация и выдает лицензии.

*3.4.1. Основные виды лицензируемой деятельности, состав, содержание работ и применяемые термины.* 3.4.1.1. Под "техническими средствами защиты и контроля защищенности информации" понимаются:

защищенные от модификации, разрушения и утечки информации средства вычислительной техники, связи, хранения, отображения и размножения информации, подлежащей защите;

технические средства защиты информации общепромышленного исполнения и специального назначения;

инструментальные средства контроля защищенности информации.

3.4.1.2. К терминам "разработка, производство технических средств" относится цикл от исследований, согласно техническому заданию, до сдачи заказчику технического средства, изготовленного по конструкторской документации.

3.4.1.3.  Термины "монтаж, наладка технических средств" включают установку, соединение (сборку) и приведение в рабочее состояние технических средств, устранение неисправностей в них.

3.4.1.4. К "специальным исследованиям технических средств" относится комплекс мероприятий по качественному и количественному исследованию возможностей утечки информации по техническим каналам и выработке рекомендаций по ее защите.

3.4.1.5. Под "проведением работ по контролю защищенности информации" понимается: постоянное или периодическое проведение комплекса работ, обеспечивающих проверку выполнения организационных и технических мероприятий по защите информации, исключающих ее разрушение, искажение или утечку по техническим каналам.

3.4.1.6. К терминам "разработка, производство программных средств защиты информации" относятся: разработка и производство специальных программ, с помощью которых осуществляются разграничение доступа к информации и предупреждение от несанкционированного ее использования.

3.4.1.7. К терминам "разработка, производство программно-аппаратных средств защиты информации" относятся: разработка и производство средств, содержащих в своем составе элементы, реализующие функции защиты информации, в которых программные (микропрограммные) и аппаратные части полностью взаимозависимы и неразделимы.

3.4.1.8. Термины "монтаж, наладка программных средств защиты информации" включают в себя:

установку, приведение в рабочее состояние и сопровождение на объектах заказчика программных средств защиты информации;

внедрение программных средств контроля эффективности мер по защите информации;

установку антивирусных программ.

3.4.1.9. Под термином "средства криптографии, реализованные в программных и программно-аппаратных комплексах защиты информации" подразумеваются средства:

обеспечения подлинности данных;

обеспечения целостности данных;

обеспечения конфиденциальности данных (шифрование);

управления ключевой системой (выполнение задач генерации, распределения, использования, хранения, уничтожения и восстановления ключей).

3.4.2. *Основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации.* Предъявляются требования по:

— уровню квалификации специалистов;

— наличию и качеству измерительной базы;

— наличию и качеству производственных помещений;

— наличию режимного органа и обеспечению охраны материальных ценностей и секретов заказчика (при необходимости);

— наличию нормативно-технической и методической документации в лицензируемой области деятельности.

Требования к помещениям, предназначенным для проведения измерений при специсследованиях, их техническая и технологическая оснащенность рассматриваются как совокупность требований к разработанной технологии проведения измерений, измерительной аппаратуре, стендам и т.п., а также к организации их содержания, обслуживания и поверки, выполнение которых позволяет организации, претендующей на проведение указанных в заявке работ, получить лицензию на право их проведения.

3.5 Национальная система сертификации Республики Беларусь, назначение и функции

В соответствии с прилагаемой к конспекту книгой В.Ф.Голикова 2004 г. технические и программные средства защиты информационных ресурсов подлежат обязательной сертификации в национальной системе сертификации Республики Беларусь соответствующим органом по сертификации. Документами, регламентирующими вопросы сертификации в РБ, являются:

ГОСТ РБ "Национальная система сертификации Республики Беларусь";

СТБ 5.1.01‑96 "Основные положения";

СТБ 5.1.02‑96 "Общие требования и порядок аккредитации";

СТБ 5.1.03‑96 "Органы по сертификации систем качества. Общие требования и порядок аккредитации";

СТБ 5.1.04‑96 "Порядок проведения сертификации продукции. Общие требования";

СТБ 5.1.05‑96 "Сертификация систем качества. Порядок проведения";

СТБ 5.1.06‑96 "Положение об экспертах‑аудиторах по качеству";

СТБ 5.1.07‑96 "Реестр. Общие требования и порядок ведения".

Органом по сертификации средств защиты информации в республике является Оперативно-аналитический центр при Президенте Республики Беларусь в области защиты информации. К числу основных задач органа по сертификации средств защиты информации могут быть отнесены:

разработка нормативных документов на средства защиты и классификация их по функциональным свойствам;

разработка нормативных документов на методы испытаний средств защиты и их гармонизация с аналогичными документами зарубежных фирм и организаций;

выбор способов подтверждения соответствия средств защиты информации требованиям нормативных документов;

сертификация средств защиты информации и выдача сертификатов на их применение;

ведение реестра сертифицированных средств защиты информации;

инспекционный контроль за качеством продукции, которой присвоен тот или иной класс (уровень) защитных свойств;

приостановка или отмена действия выданных сертификатов.

3.6 Структура и функции систем защиты информации в соответствии со стандартом ISO 7498-2 1989

дВ соответствии с прилагаемой к конспекту книгой В.Ф.Голикова 2004 г. Для интеграции систем защиты информации и удешевления их стоимости проектные решения по системам защиты информации должны быть стандартизированы в рамках международных организаций, отдельных государств, областей деятельности, конкретных организаций и фирм. Для решения этой задачи осуществляется гармонизация международных, национальных, отраслевых и фирменных нормативных документов по защите информации. Международной организацией по стандартизации ‑ ИСО/МЭК разработаны стандарты, связанные с защитой информации.

Основным нормативным документом-стандартом, определяющим структуру и функции систем защиты информации, является стандарт ISO 7498-2 1989 "*Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты*". В этом документе рассмотрены вопросы терминологии по защите информации, приводится общее описание служб и механизмов защиты, уделено внимание проблемам взаимодействия служб, механизмов и уровней защиты, рассмотрены вопросы управления защитой при взаимодействии систем.

3.7 Страхование как метод защиты информации

В соответствии с прилагаемой к конспекту книгой В.Ф.Голикова 2004 г. определение защитных свойств технических средств осуществляется путем непосредственных испытаний. Заключение (сертификат) банковского сертификационного центра должно явиться основой для системы страховых гарантий. Для предотвращения банковских информационных рисков необходимо страхование:

электронного документооборота при заключении и исполнении договоров с участием банков, при оформлении первичных платежных документов с применением цифровой (электронной) подписи;

от несанкционированного доступа в информационную сеть;

от разрушения или потери информации в результате программных или аппаратных сбоев;

от прямых убытков, связанных с незаконным использованием программных и аппаратных средств информационной системы;

от потерь рабочего времени и ухудшения качества обслуживания клиентов, вызванных поломками или некорректным функционированием аппаратных средств.

3.8 Организационно-административные методы защиты информации

В соответствии с прилагаемой к конспекту книгой В.Ф.Голикова 2004 г. организационно-административные методы защиты информации регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, чтобы несанкционированный доступ к информации становился либо невозможным, либо существенно затруднялся. Они охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем. К организационно-административным мероприятиям защиты информации относятся:

выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;

выделение специальных ЭВМ для обработки конфиденциальной информации;

организация хранения конфиденциальной информации на специальных промаркированных носителях информации;

использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;

организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;

организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;

установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;

постоянный контроль за соблюдением установленных требований по защите информации.

3.9 Организационно-технические методы защиты информации

В соответствии с прилагаемой к конспекту книгой В.Ф.Голикова 2004 г. организационно-технические методы защиты информации охватывают все структурные элементы автоматизированных информационных систем на всех этапах их жизненного цикла. Организационно-техническая защита информации обеспечивается осуществлением следующих мероприятий:

ограничение доступа посторонних лиц внутрь корпуса оборудования за счет установки механических запорных устройств или замков;

отключение ЭВМ от локальной вычислительной сети или сети удаленного доступа (региональные и глобальные вычислительные сети) при обработке на ней конфиденциальной информации, кроме случаев передачи этой информации по каналам связи;

использование для отображения конфиденциальной информации жидкокристаллических, а для печати — струйных принтеров или термопечати с целью снижения утечки информации по электромагнитному каналу. При использовании обычных дисплеев и принтеров с этой же целью рекомендуется включать устройства, создающие дополнительный шумовой эффект (фон), — генераторы шума, кондиционер, вентилятор, или обрабатывать другую информацию на рядом стоящей ЭВМ;

установка клавиатуры и печатающих устройств на мягкие прокладки с целью снижения утечки информации по акустическому каналу;

размещение оборудования для обработки конфиденциальной информации на расстоянии не менее 2,5 м от устройств освещения, кондиционирования, связи, металлических труб, теле- и радиоаппаратуры;

организация электропитания ЭВМ от отдельного блока питания (с защитой от побочных электромагнитных излучений или от общей электросети через фильтр напряжения);

использование бесперебойных источников питания (БИП) персональных компьютеров для силовых электрических сетей с неустойчивым напряжением и плавающей частотой. Основное назначение бесперебойных источников питания — поддержание работы компьютера после исчезновения напряжения в электрической сети. Это обеспечивается за счет встроенных аккумуляторов, которые подзаряжаются во время нормальной работы. БИП мгновенно предупредит своего владельца об аварии электропитания и позволит ему в течение некоторого времени (от нескольких минут до нескольких часов) аккуратно закрыть файлы и закончить работу. Кроме обычных для БИП функций они могут выполнять функцию высококлассного стабилизатора напряжения и электрического фильтра. Важной особенностью устройства является возможность непосредственной связи между ним и сетевой операционной системой

**Лекция 4 Политика безопасности (ПБ) информационного объекта**

Самое близкое по смыслу определение слова 'политика', которое можно найти в словаре - это: "план или курс действий, как для правительств, политических партий, или структур бизнеса, предназначенный, чтобы определить или повлиять на решения, действия и другие вопросы" (American Heritage Dictionary of the English language) В терминах же компьютерной безопасности политику можно определить как изданный документ (или свод документов), в котором рассмотрены вопросы философии, организации, стратегии, методов в отношении конфиденциальности, целостности и пригодности информации и информационных систем. Таким образом, ***ПБ ИО*** – это совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов [3]

Опыт показал, что одним из факторов для успеха в обеспечении информационной безопасности в пределах организации являются ПБ, задачи и действия, отражающие производственные цели, а также предоставление руководства по политике информационной безопасности и стандарта всем служащим и подрядчикам [2. c. VII]. Поэтому задача ПБ состоит в том [2. c. 1], чтобы сформулировать цели политики информационной безопасности и обеспечить ее поддержку руководством организации. Администрация должна поставить четкую цель и оказывать всестороннюю поддержку информационной безопасности посредством распространения политики безопасности среди сотрудников организации

Средства управления, считающиеся общепринятой, лучшей технологией информационной безопасности, должны обеспечивать, среди других положений, [2, c. VII] выдачу ***документа, содержащего описание политики безопасности организации***. Указанные средства управления информационной безопасностью, применимы в большинстве организаций и окружающих сред. Целесообразность выбора любого из средств управления должна определяться в свете конкретных рисков, присущих организации. Вышеупомянутый подход рассматривается как хорошая отправная база, но выбор средства управления должен основываться на оценке риска [2. c. VII].

4.1 Рекомендуемые области разработки ПБ

Институт SANS (www.sans.org) подготовил «The SANS Security Policy Project»,который содержит большой репозитарий готовых ПБ на разные случаи жизни, распространяемых бесплатно. Также здесь можно найти интересные ссылки на ресурсы, посвященные разработке ПБ. Среди готовых ПБ Института SANS имеются политики, охватывающие следующие области разработки ПБ:

* допустимое шифрование,
* допустимое использование,
* аудит безопасности,
* оценка рисков,
* классификация данных,
* управление паролями,
* использование ноутбуков,
* построение демилитаризованной зоны,
* построение Экстранет,
* безопасностей рабочих станций и серверов,
* антивирусная защита,
* безопасность маршрутизаторов и коммутаторов,
* безопасность беспроводного доступа,
* организация удалённого доступа,
* построение виртуальных частных сетей (VPN),
* безопасность периметра.

4.2 Основные требования к ПБ

ПБ должна придерживаться содержания, изложенного ниже в подразделе 4.5. Согласно [3] ПБ должна быть: а) реалистичной, б) выполнимой, в) краткой, г) понятной, д) не приводить к существенному снижению общей производительности бизнес-подразделений компании. На практическом занятии будут рассмотрены случаи, когда ПБ не отвечала перечисленным требованиям. По мнению специалистов компании CISCO желательно, чтобы описание ПБ занимало не более 2 (максимум 5) страниц. При этом важно учитывать, как ПБ будет влиять на уже существующие информационные системы компании. Как только ПБ утверждена, она должна быть представлена сотрудникам компании для ознакомления. Наконец, ПБ необходимо пересматривать ежегодно, чтобы отражать текущие изменения в развитии бизнеса компании. В организации должен быть [2. c. 2] ответственный за реализацию политики, ее поддержку и пересмотр в соответствии с определенным процессом пересмотра. Этот процесс должен гарантировать, что пересмотр политики осуществляется в ответ на изменения, затрагивающие основы первоначальной оценки риска, например, важные инциденты безопасности, новые уязвимые места или изменения организационной или технической инфраструктуры. Рекомендуется планировать и периодически пересматривать:

a) эффективность политики, которую можно оценить в природе количеством и силой воздействия зарегистрированных инцидентов безопасности;

b) стоимость средств управления и их влияние на производственную эффективность;

c) эффект от изменений технологий.

Ответственность [2. c. 2] за обеспечение информационной безопасности несут все члены руководства. Поэтому руководству организации рекомендуется регулярно проводить совещания по проблемам защиты информации, с целью выработки четких указаний по этому вопросу, а также оказания административной поддержки инициативам по обеспечению безопасности. Эти совещания должны содействовать реализации процесса защиты в организации посредством принятия соответствующих обязательств и предоставления адекватных ресурсов. Совещание может быть частью существующего органа управления. Обычно на подобных совещаниях рассматриваются следующие вопросы:

а) анализ и утверждение политики информационной безопасности, распределение общих обязанностей;

b) мониторинг основных угроз, которым подвергаются информационные ресурсы;

c) анализ и слежение за инцидентами в системе безопасности;

d) утверждение основных инициатив, направленных на усиление защиты информации.

За координацию действий по проведению политики безопасности в жизнь должен быть ответственен один из членов руководства [2. c. 2]

В ПБ необходимо [2. c. 3] четко определить обязанности по защите отдельных ресурсов и выполнению конкретных процессов обеспечения безопасности.

ПБ информационной безопасности (раздел 3) должна давать общие рекомендации по распределению функций и обязанностей по защите информации в организации. Там, где необходимо, следует дополнить эти рекомендации более подробными разъяснениями, касающимися конкретных систем или сервисов. Рекомендуется назначить ответственных за конкретные физические и информационные активы и процессы обеспечения защиты такие, как планирование бесперебойной работы организации.

Во многих организациях общая ответственность за развитие и реализацию безопасности, а также за поддержку управления безопасностью возлагается на руководителя службы информационной безопасности. Однако за распределение ресурсов и реализацию управления часто несут ответственность отдельные руководители. Общепринято назначение для каждого информационного актива владельца, ответственного за его повседневную безопасность. Владельцы информационных активов могут делегировать свои полномочия по безопасности отдельным руководителям или поставщикам по предоставлению услуг (сервис-провайдерам). Тем не менее, владелец активов в конечном счете остается ответственным за безопасность актива и должен контролировать корректность выполнения делегированной ответственности.

Важно четко определить зоны ответственности каждого администратора, в частности следует отразить следующие положения:

а) различные активы и процессы обеспечения безопасности, связанные с каждой системой, необходимо идентифицировать и четко определить;

b) кандидатура администратора, отвечающего за каждый актив или процесс обеспечения защиты, должна быть одобрена, а его обязанности документально оформлены;

c) уровни полномочий необходимо четко определить и документально оформить [2. c. 3].

4.3 Эффективность и методы её оценки

Эффективность действия ПБ на предприятии можно оценивать количественно и качественно.

В [2, c. 2] указано, что средства управления информационной безопасностью должны обеспечивать регистрацию инцидентов безопасности и выдачу отчётов о происшедших инцидентах. Формы журналов для регистрации указанных инцидентов в рукописном или электронном виде, а также отчётов о происшедших инцидентах, насколько нам известно, не регламентированы, поэтому студентам представляется возможность самостоятельной разработки таких журналов. Далее отчёты о происшедших инцидентах должны анализироваться службой безопасности и руководством организации. В этом случае эффективность ПБ можно оценить количеством и силой воздействия зарегистрированных инцидентов безопасности. Таким образом можно произвести количественную оценку эффективности ПБ.

При качественной оценке эффективности ПБ следует помнить, что эффективные ПБ определяют (здесь и далее до конца подраздела материал заимствован из [6]) необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации.

При разработке ПБ, которая «не рухнет под своим собственным весом», следует учитывать факторы, влияющие на успешность применения мер обеспечения безопасности. Очевидно, что меры безопасности накладывают ограничения на действия пользователей и администраторов ИС и в общем случае приводят к снижению производительности труда. Безопасность является затратной статьей для организации, как и любая другая форма страхования рисков.

Человеческая природа всегда порождает желание получения большего количества информации, упрощения доступа к ней и уменьшения времени реакции системы. Любые меры безопасности в определенной степени препятствуют осуществлению этих естественных желаний.

Представьте себе ситуацию ожидания переключения сигнала светофора. Очевидно, что светофор предназначен для обеспечения безопасности дорожного движения, однако если движение по пересекаемой дороге отсутствует, то это ожидание выглядит утомительной тратой времени. Человеческое терпение имеет предел  и если светофор долго не переключается, то у многих возникает желание проехать на красный. В конце концов, светофор может быть неисправен, либо дальнейшее ожидание является неприемлемым.

Аналогично, каждый пользователь ИС обладает ограниченным запасом терпения, в отношении следования правилам политики безопасности, достигнув которого он перестает эти правила выполнять, решив, что это явно не в его интересах (не в интересах дела). Политики, не учитывающие влияния, которое они оказывают на производительность труда пользователей и на бизнес-процессы, в лучшем случае могут привести к ложному чувству защищенности. В худшем случае такие политики создают дополнительные бреши в системе защиты, когда «кто-то начинает двигаться на красный свет». Поэтому следует учитывать и минимизировать влияние ПБ на производственный процесс, соблюдая принцип разумной достаточности.

4.4 Жизненный цикл ПБ

В лекциях по организации производства введено понятие жизненного цикла (ЖЦ) изделия. Схожее по своей сути понятие введено международным и национальным стандартом для ЖЦ программного обеспечения. Поэтому ничто не мешает использовать понятие ЖЦ для ПБ. Возможен следующий вариант структуры ЖЦ ПБ:

Разработка ПБ – длительный и трудоемкий процесс (процесс разработки подробно описан в подразделе 4.5.3), требующий высокого профессионализма, отличного знания нормативной базы в области ИБ и, помимо всего прочего, писательского таланта. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ. Эта ответственность обычно концентрируется на руководителе Отдела информационной безопасности, Главном офицере по информационной безопасности (CISO), Главном офицере безопасности (CSO), ИТ-директоре (CIO), либо на руководителе Отдела внутреннего аудита. Этот специалист координирует деятельность рабочей группы по разработке и внедрению ПБ на протяжении всего жизненного цикла, который состоит из пяти последовательных этапов, описанных ниже.

*4.4.1. Первоначальный аудит безопасности.* Аудит безопасности – это процесс, с которого начинаются любые планомерные действия по обеспечению ИБ в организации. Он включает в себя проведение обследования, идентификацию угроз безопасности, ресурсов, нуждающихся в защите и оценку рисков. В ходе аудита производится анализ текущего состояния ИБ, выявляются существующие уязвимости, наиболее критичные области функционирования и наиболее чувствительные к угрозам ИБ бизнес процессы.

*4.4.2. Разработка.* Аудит безопасности позволяет собрать и обобщить сведения, необходимые для разработки ПБ. На основании результатов аудита определяются основные условия, требования и базовая система мер по обеспечению ИБ в организации, позволяющих уменьшить риски до приемлемой величины, которые оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации.

Разработка ПБ с нуля не всегда является хорошей идеей. Во многих случаях можно воспользоваться существующими наработками, ограничившись адаптацией типового комплекта ПБ к специфическим условиям своей организации. Этот путь позволяет сэкономить многие месяцы работы и повысить качество разрабатываемых документов. Кроме того, он является единственно приемлемым в случае отсутствия в организации собственных ресурсов для квалифицированной разработки ПБ.

*4.4.3. Внедрение.* С наибольшими трудностями приходится сталкиваться на этапе внедрения ПБ, которое, как правило, связано с необходимостью решения технических, организационных и дисциплинарных проблем. Часть пользователей могут сознательно, либо бессознательно сопротивляться введению новых правил поведения, которым теперь необходимо следовать, а также программно-технических механизмов защиты информации, в той или иной степени неизбежно ограничивающих их свободный доступ к информации. Администраторов ИС может раздражать необходимость выполнения требований ПБ, усложняющих задачи администрирования. Помимо этого могут возникать и чисто технические проблемы, связанные, например, с отсутствием в используемом ПО функциональности, необходимой для реализации отдельных положений ПБ.

На этапе внедрения необходимо не просто довести содержание ПБ до сведения всех сотрудников организации, но также провести обучение и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по старому. Чтобы внедрение завершилось успешно, должна быть создана проектная группа по внедрению ПБ, действующая по согласованному плану в соответствии с установленными сроками выполнения работ.

*4.4.4. Аудит и контроль.* Соблюдение положений ПБ должно являться обязательным для всех сотрудников организации и должно непрерывно контролироваться. Рассмотрение различных форм и методов контроля, позволяющих оперативно выявлять нарушения безопасности и своевременно реагировать на них, выходят за рамки данной статьи.

Проведение планового аудита безопасности является одним из основных методов контроля  работоспособности ПБ, позволяющего оценить эффективность внедрения. Результаты аудита могут служить основанием для пересмотра некоторых положений ПБ и внесение в них необходимых корректировок.

*4.4.5. Пересмотр и корректировка.* Первая версия ПБ обычно не в полной мере отвечает потребностям организации, однако понимание этого приходит с опытом. Скорее всего, после наблюдения за процессом внедрения ПБ и оценки эффективности ее применения потребуется осуществить ряд доработок. В дополнение к этому, используемые технологии и организация бизнес процессов непрерывно изменяются, что приводит к необходимости корректировать существующие подходы к обеспечению ИБ. В большинстве случаев ежегодный пересмотр ПБ является нормой, которая устанавливается самой политикой.

4.5 Содержание ПБ

*4.5.1 Содержание ПБ.* ПБ должна содержать основные цели и задачи организации режима информационной безопасности, чёткое описание области действия политики, а также указывать ответственных за её выполнение и их обязанности [3]

Документ о политике информационной безопасности должен быть [2. c. 2] одобрен руководством, опубликован и доведен до сведения всех сотрудников. В нем необходимо сформулировать обязательство по управлению и изложить подход организации к управлению информационной безопасностью. В него обязательно следует включить следующие положения:

а) определение информационной безопасности, ее основные цели и область применения, а также значение безопасности как механизма, позволяющего коллективно использовать информацию;

b) изложение позиции руководства по вопросам реализации целей и принципов информационной безопасности;

c) разъяснение конкретных положений политики безопасности, принципов, стандартов и требований к ее соблюдению, включая:

1) выполнение правовых и договорных требований;

2) требования к обучению персонала правилам безопасности;

3) политику предупреждения и обнаружения вирусов, а также другого вредоносного программного обеспечения;

4) политику обеспечения бесперебойной работы организации;

5) последствия нарушения политики безопасности;

d) определение общих и конкретных обязанностей по обеспечению режима информационной безопасности;

c) разъяснение процесса уведомления о событиях, таящих угрозу безопасности.

Данная политика должна быть доведена до всех сотрудников организации в релевантной, доступной и понятной заинтересованному лицу форме [2. c. 2].

*4.5.2 Пример политики безопасности*. Эталонная ПБ предприятия может включать в себя следующие разделы:

1. Общие положения
2. Политика управления паролями
3. Идентификация пользователей
4. Полномочия пользователей
5. Защита информационных ресурсов ИС от компьютерных вирусов
6. Правила установки и контроля сетевых соединений
7. Правила политики безопасности по работе с системой электронной почты
8. Правила обеспечения безопасности информационных ресурсов

Ниже представлены первые два раздела вышеназванной эталонной ПБ.

**Раздел 1. Общие положения**

Обеспечение информационной безопасности является необходимым условием для осуществления деятельности Предприятия. Нарушение информационной безопасности может привести к серьезным последствиям, включая потерю доверия со стороны клиентов и снижение конкурентоспособности.

Основой мер по обеспечению режима информационной безопасности административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности. Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности Предприятия определяет основные направления и требования по обеспечению информационной безопасности Предприятия.

Обеспечение безопасности информации включает в себя любую деятельность, направленную на защиту информации и/или поддерживающей инфраструктуры. Настоящая политика информационной безопасности охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Предприятие. Положения настоящего документа относятся ко всему штатному персоналу, временным служащим и другим сотрудникам Предприятия, а также клиентам Предприятия и третьим лицам, имеющим доступ к автоматизированным и телекоммуникационным системам Предприятия.

**Раздел 2. Политика управления паролями**

Пользователи должны выбирать нестандартные пароли. Это означает, что пароли *не* должны быть связаны с занятиями или личной жизнью пользователей. Например, нельзя использовать в качестве пароля номер собственного автомобиля, имя супруги или часть адреса. Это также означает, что пароль не должен быть просто словом из словаря. Так, не должны использоваться в качестве паролей имена собственные, географические названия, технические термины и сленг. Если имеются соответствующие системные программные средства для осуществления контроля надежности назначаемых пользователям паролей, то необходимо использовать эти средства для того, чтобы запретить пользователям выбор легко угадываемых паролей.

Пользователи могут выбрать легко запоминающиеся пароли, которые в тоже время являются трудно угадываемыми для третьих лиц, если будет выполнено хотя бы одно из следующих условий:

* Несколько слов написаны слитно (такие пароли известны под названием «passphrases»);
* При наборе слова на клавиатуре использованы клавиши, смещенные относительно нужных, на один ряд вверх, вниз, вправо или влево;
* Слово набрано со смещением на определенное количество букв вверх или вниз по алфавиту;
* Комбинация цифр и обычного слова;
* Намеренно неправильное написание слова (но не обычная в данном слове орфографическая ошибка).

Рекомендуется, чтобы в пароле имелись не только буквы, но и другие символы, то есть цифры (0-9) и знаки пунктуации. Использование управляющих символов и прочих неотображаемых знаков не рекомендуется, поскольку из-за этого могут возникнуть проблемы при передаче данных по сети, неожиданно активизироваться определенные системные утилиты или возникнуть другие побочные эффекты.

Все пароли должны состоять не менее чем из шести символов. Длина паролей должна всегда автоматически проверяться в тот момент, когда пользователи создают или выбирают пароли. Пользователи не должны создавать пароли, которые идентичны или в значительной степени повторяют ранее используемые ими пароли. Если имеются соответствующие системные программные средства, необходимо запретить пользователям, повторно использовать свои предыдущие пароли.

Пароли не должны храниться в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ. Например, ни в каких приложениях пользователи не должны выбирать такую опцию конфигурации, как автоматическое сохранение пароля.

Нельзя записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя.

*4.5.3. Этапы разработки ПБ.* Этап 1. Разработка ПБ. Стадия 1.1. Разработка концепции политики информационной безопасности.

Концепция политики ИБ – документ, в котором в самом общем виде сформулированы цели и приоритеты организации в области ИБ, намечены общие пути достижения  этих целей. В результате выполнения этой стадии будет написан документ «Концепция политики ИБ», содержащий:

* общую характеристику объекта защиты (описание состава, функций и существующей технологии обработки информации);
* формулировку целей создания системы защиты, основных задач обеспечения информационной безопасности и путей достижения целей;
* основные классы угроз информационной безопасности, принимаемые во внимание при разработке подсистемы защиты;
* основные принципы и подходы к построению системы обеспечения информационной безопасности, меры, методы и средства достижения целей защиты.

Стадия 1.2. Описание границ системы и построение модели ИС с позиции безопасности

Описание границ системы выполняется по следующему плану:

* Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой (модернизацией) системы ИБ.
* Размещение средств СВТ и поддерживающей инфраструктуры.

Затем строится модель информационной системы с позиции ИБ:

* Описываются ресурсы информационной системы, подлежащие защите.
  + Рассматриваются ресурсы автоматизированной системы следующих классов: СВТ, данные, системное и прикладное ПО.
* Технология обработки информации и решаемые задачи.
  + Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

Исходными данными являются результаты обследования и ведомственные документы.

В результате выполнения этого этапа будет написан документ «Модель системы с позиции ИБ», содержащий следующие разделы:

* размещение средств СВТ и поддерживающей инфраструктуры
* описание информационных ресурсов, подлежащих защите, их категорирование;
* информационные процессы и их модель с позиции ИБ.

Стадия 1.3. Анализ рисков: формализация системы приоритетов организации в области информационной безопасности, выявление существующих рисков и оценка их параметров.

Содержание этой стадии рассмотрено на ПЗ 2.

Стадия 1.4. Анализ возможных вариантов контрмер и оценка их эффективности.

Содержание этой стадии рассмотрено на ПЗ 2.

Стадия 1.5. Выбор комплексной системы защиты на всех этапах жизненного цикла.

На этой стадии должны быть разработаны документы:

1.5.1 Организационно-распорядительные документы по обеспечению режима информационной безопасности.

*1.5.1.1 План обеспечения режима информационной безопасности*, содержащий:

* требования по организации и проведению работ по защите информации в АС,
* описание применяемых мер и средств защиты информации от рассматриваемых угроз, общих требований к настройкам применяемых средств защиты информации от НСД;
* распределение ответственности за реализацию "Плана " между должностными лицами и структурными подразделениями организации.

1.5.1.2 Категорирование информационных ресурсов и порядок обращения с ними:

* определение основных видов защищаемых информационных ресурсов;
* категории защищаемых ресурсов и критерии классификации ресурсов по требуемым степеням защищенности (категориям);
* определение мер и средств защиты информации, обязательных и рекомендуемых к применению на АРМ различных категорий;
* образец формуляра ЭВМ (для учета требуемой степени защищенности (категории), комплектации, конфигурации и перечня решаемых на ЭВМ задач);
* образец формуляра решаемых на ЭВМ АС функциональных задач (для учета их характеристик, категорий пользователей задач и их прав доступа к информационным ресурсам данных задач);
* общие вопросы организации учета, хранения и уничтожения носителей конфиденциальной информации;
* порядок передачи (предоставления) конфиденциальных сведений третьим лицам;
* определение ответственности за нарушение установленных правил обращения с защищаемой информацией;
* форма типового Соглашения (обязательства) сотрудника организации о соблюдении требований обращения с защищаемой информацией.

1.5.1.3 Положение об отделе защиты информации:

* общие положения, руководство отделом, основные задачи и функции отдела;
* права и обязанности начальника и сотрудников отдела, ответственность;
* типовую организационно-штатную структуру отдела.

1.5.1.4 Должностные инструкции:

* Обязанности администратора информационной безопасности;
* Обязанности персонала по обеспечению информационной безопасности
* Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам АС;
* Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС;
* Инструкция по организации парольной защиты;
* Инструкция по организации антивирусной защиты;

1.5.2. План обеспечения бесперебойной работы информационной системы, включающий:

* классификацию возможных (значимых) кризисных ситуаций и указание источников получения информации о возникновении кризисной ситуации;
* перечень основных мер и средств обеспечения непрерывности процесса функционирования АС и своевременности восстановления ее работоспособности;
* общие требования к подсистеме обеспечения непрерывной работы и восстановления;
* типовые формы для планирования резервирования ресурсов подсистем АС и определения конкретных мер и средств обеспечения их непрерывной работы и восстановления;
* порядок действий и обязанности персонала по обеспечению непрерывной работы и восстановлению работоспособности системы.

**Лекция 5 Пассивные методы защиты информации от утечки по электромагнитному и акустическому каналам**

5.1 Экранирование электромагнитных полей

Электрические токи различных частот, протекающие по элементам функционирующего средства обработки информации, создают побочные магнитные и электрические поля, являющиеся причиной возникновения электромагнитных и параметрических каналов утечки, а также наводок информационных сигналов в посторонних токоведущих линиях и конструкциях. Пассивное ослабление побочных электромагнитных излучений и наводок (ПЭМИН) осуществляется экранированием и заземлением средств и их соединительных линий, происходящее при излучении ПЭМИН просачивание в цепи электропитания и заземления предотвращается фильтрацией информационных сигналов. Кроме пассивного подавления ПЭМИН с помощью экранирования утечки информации по каналам ПЭМИН можно подавлять активными методами, о чём речь идёт в следующей лекции.

Следует различать 2 направления экранирования. Первое – это экранирование для подавления паразитных наводок в радиоэлектронной аппаратуре (РЭА). Паразитные наводки являются вредными помехами для функционирования аппаратуры. Сигналы, которые могут передавать эти наводки, как ПЭМИ не рассматриваются – рассматривается только вредное действие наводки. При этом РЭА может быть как источником, так и приёмником паразитных наводок, а также источником и приёмником одновременно. Функционирование различных устройств РЭА, расположенных недалеко друг от друга, в условиях действия паразитных наводок обеспечивается проектированием их по правилам электромагнитной совместимости. Одним из способов обеспечения электромагнитной совместимости является экранирование деталей, узлов и устройств РЭА. Этот вид экранирования изучается с 1930-х годов и хорошо описан в литературе.

Однако наводки могут служить и переносчиками полезных сигналов. Такими наводками являются ПЭМИН. Сходство между двумя видами наводок заключается, во-первых, в сходных источниках их излучения, во-вторых, в сходных методах борьбы с ними (экранирование и др.), и в-третьих, в одинаковых физических принципах возникновения тех и других наводок и в одинаковых теоретических способах борьбы с ними. Различаются же эти наводки способом использования – из ПЭМИН злоумышленники пытаются выделить полезный сигнал, паразитные наводки конструктора РЭА пытаются полностью уничтожить. В данном курсе будем изучать только ПЭМИН.

*5.1.1 Экранирование ПЭМИН* осуществляется с помощью специальных экранов или с помощью экранирующих покрытий. Экраны можно разделить на экраны для подавления каналов утечки информации и экраны для защиты человека от вредного воздействия ЭМИ на организм. Экраны для защиты человека от вредного воздействия ЭМИ на организм обычно устанавливают перед источником мощного электромагнитного излучения, например, компьютером. В этом случае экран не только ослабляет интенсивность излучения, но и гасит вредное воздействие электромагнитного излучения на организм человека-пользователя ПК. Утечка информации при установке экранов может возникнуть не только из-за низкого уровня поглощения электромагнитного излучения экраном, но и вследствие несовершенства экранов, приводящего к асимметрии магнитных линий относительно экрана и к возникновению в цепи между корпусом экрана и землей информативных токов.

В БГУИР на кафедре защиты информации ведётся большая работа по исследованию экранов и проектированию новых их модификаций. Коллектив разработчиков возглавляет заведующий кафедрой, доктор технических наук, профессор Леонид Михайлович Лыньков. Разработаны защищённые авторскими свидетельствами и патентами новые конструкции экранов для защиты человека от вредного воздействия ЭМИ на организм (например, экранов для ослабления ЭМИ от видеотерминала компьютера), новые конструкции средств индивидуальной защиты от ЭМИ - радиозащитных костюмов, халатов, комбинезонов и др, средств защиты слуха от ЭМИ мобильного телефона, маскирующих покрытий для военных целей. Изучаются экспресс-характеристики отражения экранов, особенности изготовления их многослойных конструкций, и материалы для экранирования (см. п. 5.2.9.

Проектируются новые экраны с уменьшенным коэффициентом отражения электромагнитной волны и сниженными массогабаритными характеристиками при обеспечении высокой эффективности защиты от электромагнитного излучения в широком диапазоне частот. Отдельное направление представляет собой исследование экранов на основе гибких радиопоглощающих материалов с различного рода наполнителями. Начаты работы по проектированию и исследованию экранов для защищённой от ЭМИ переноски смарт-карт различного назначения (банковских и др.).

*5.1.2 Защитные экранирующие покрытия помещений и оборудования.* Всё рабочее помещение, в котором установлен ИО, пытаются заэкранировать. При этом:

экранирование рабочих помещений осуществляется путем покрытия стен, пола и потолка металлизированными обоями, токопроводящей эмалью и штукатуркой, проволочными сетками или фольгой, установки загородок из токопроводящего кирпича, многослойных стальных, алюминиевых или из специальной пластмассы листов; листы толщиной не менее 1 мм соединяются пайкой и надёжно заземляются;

для защиты окон применяют металлизированные шторы и стекла с токопроводящим слоем; используется также сотовый фильтр – алюминиевая решётка с квадратными ячейками не более 1 см,

все отверстия закрывают металлической сеткой, соединяемой с шиной заземления или настенной экранировкой;

на вентиляционных каналах монтируют так называемые предельные магнитные ловушки, препятствующие распространению радиоволн.

на водопроводных, отопительных, газовых и других металлических трубах помещают разделительные диэлектрические вставки, которые осуществляют разрыв электромагнитной цепи. Экранированное помещение служит надёжным гарантом защиты конфиденциальной информации, но его монтаж из металлических листов является очень трудоёмким, требует больших затрат времени и, соответственно, дорого стоит.

5.2 Материалы для экранов

Основными материалами для экранирования электромагнитного излучения (ЭМИ) являются различные металлы, различные диэлектрики, стёкла с токопроводящим покрытием, специальные ткани и волокнистые изделия. Одними из новых материалов данной группы являются влагосодержащие композиционные материалы (влагосодержащее машинно-вязанное полотно, нетканый целлюлозный материал), текстильные волокна с осаждёнными на их поверхность металлосодержащими покрытиями, волокнистые материалы (волокна, нити, пряди, жгуты, войлок, ткани).

*5.2.1 Металлические материалы*. *2.3.1.1*. *Однослойные экраны.* Наибольшее распространение при экранировании получили металлические экраны в виде пластин или листов. Чаще всего используются железо, сталь, медь, латунь, алюминий. Эти материалы используются не только в виде листов, но и в виде сетки, решеток и металлических трубок. Металлические экраны при практически приемлемой толщине обеспечивают хорошую эффективность экранирования на всех частотах радиодиапазона, в том числе и на нижних частотах радиовещания.

## *5.2.2 Многослойные экраны.* Многослойные комбинированные конструкции экранов, состоящие из последовательно чередующихся немагнитных (медь, алюминий, латунь) и магнитных (сталь, пермаллой) слоев, применяются для получения высокой эффективности экранирования в широком частотном диапазоне, включая область низких частот, и обеспечения малых вносимых потерь в экранируемые цепи радиоэлектронной аппаратуры. Эффективность экранирования многослойного экрана зависит от применяемых материалов, их расположения и соотношения толщин. Например, сочетание сталь‑медь‑алюминий обеспечивает меньшую эффективность экранирования, чем медь‑сталь‑алюминий. Кроме того, за счет внутреннего слоя экрана, выполненного из немагнитного металла, уменьшаются вносимые потери в экранируемые цепи аппаратуры по сравнению со сплошным магнитным экраном такой же толщины. Многослойная конструкция экрана оказывается особенно эффективной при экранировании квазистатических магнитных полей большой напряженности. В случае однослойного магнитного экрана при большом значении напряженности магнитной составляющей поля материал экрана входит в насыщение и магнитная проницаемость его резко снижается.

5.2.3 *Сетчатые экраны.* Иногда по конструктивным соображениям удобно изготавливать и применять экраны не из сплошного листового материала, а из сетки. Экранирующие свойства листового металла выше, чем сетки, сетка же удобнее в конструктивном отношении, особенно при экранировании смотровых и вентиляционных отверстий, окон, дверей и т.д. Защитные свойства сетки зависят от величины ячейки и толщины проволоки: чем меньше величина ячеек, чем толще проволока, тем выше ее защитные свойства. Отрицательным свойством отражающих материалов является то, что они в некоторых случаях создают отраженные радиоволны, которые могут усилить облучение человека. В настоящее время для защиты от ЭМИ применяются средства индивидуальной защиты (СИЗ) - радиозащитные костюмы, халаты, комбинезоны, защитные маски, фартуки, очки и др. Ввиду того, что СИЗ стесняют движения работающего и несколько ухудшают гигиенические условия, их используют лишь в особых случаях, например, при ремонтных работах в аварийных ситуациях, во время кратковременных настроечных и измерительных работ с радиотехническим оборудованием и в антенном поле радиотехнических станций. Они изготавливаются из хлопчатобумажной ткани с микропроводом и, в принципе, представляют собой сетчатые экраны. Для изготовления экранных штор, драпировок, чехлов, специальной одежды применяются специальные ткани (например, "Ткань хлопчатобумажная с микропроводом арт. 7289"), в структуре которых тонкие металлические нити образуют сетку с размерами 0,5×0,5 мм. Эффективность подавления ЭМИ такими тканями падает с увеличением частоты, поэтому возникает необходимость разработки эффективных эластичных экранов для миллиметрового диапазона. Особую значимость приобретает проблема создания поглощающих материалов, ввиду невозможности применения в некоторых случаях отражающих экранов и необходимости создания маскирующих покрытий.

*5.2.4 Диэлектрики*. Более удобными материалами для экранировки являются радиопоглощающие материалы, в т. ч. диэлектрики. Листы поглощающих материалов могут быть одно- или многослойными. Многослойные - обеспечивают поглощение радиоволн в более широком диапазоне. Для улучшения экранирующего действия у многих типов радиопоглощающих материалов с одной стороны впрессована металлическая сетка или латунная фольга. При создании экранов эта сторона обращена в сторону, противоположную источнику излучения. Характеристики некоторых радиопоглощающих материалов приведены в табл. 5.1

Таблица 5.1 Характеристики некоторых радиопоглощающих диэлектриков

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование материалов | Тип марок | Диапазон поглощенных волн, см | Коэффициент отражения по мощности, % | Ослабление проходящей мощности, % |
| Резиновые коврики | В2Ф-2 | 0,8 - 4 | 1 - 2 | 98 - 99 |
| Магнитодиэлектри-ческие пластины | ХВ – 0,8 | 0,8 | 1 - 2 | 98 - 99 |
| Поглощающие покрытия на основе поролона | «Болото» | 0,8 – 100 | 1 - 2 | 98 - 99 |
| Ферритовые пластины | СВЧ - 0,68 | 15 – 200 | 3 - 4 | 96 - 97 |

*5.2.5 Стёкла с токопроводящим покрытием*. Радиоизлучения могут проникать в помещения, где находятся люди через оконные и дверные проемы. Для экранирования смотровых окон, окон помещений, застекления потолочных фонарей, перегородок применяется металлизированное стекло, обладающее экранирующими свойствами. Такое свойство стеклу придает тонкая прозрачная пленка либо окислов металлов, чаще всего олова, либо металлов - медь, никель, серебро и их сочетания. Пленка обладает достаточной оптической прозрачность и химической стойкостью. Будучи нанесенной на одну сторону поверхности стекла она ослабляет интенсивность излучения в диапазоне 0,8 – 150 см на 30 дБ (в 1000 раз). При нанесении пленки на обе поверхности стекла ослабление достигает 40 дБ (в 10000 раз).

Стекла с токопроводящим покрытием в основном используются в смотровых окнах и шкальных системах РЭС, в экранированных камерах с целью обеспечения доступа в них света. Замкнутый экран из стекол с токопроводящим покрытием используется и тогда, когда требуется наблюдать за происходящими внутри экрана процессами. В настоящее время имеется номенклатура стекол с токопроводящими покрытиями, имеющих поверхностное сопротивление не менее 6 Ом при ухудшении прозрачности не более чем на 20 %. Как показывают исследования, эффективность в 20дБ для рассматриваемого случая может быть получена только при незначительном переходном сопротивлении между поверхностью пленки и экраном, что возможно при соответствующем обеспечении надежного и тщательного соединения стекла с каркасом.

*5.2.6 Специальные ткани.* Имеется несколько видов специальных тканей (типа РТ и артикула 4381), [258, 259] с металлической нитью, отражающих электромагнитные волны. Ткань РТ изготавливается из капроновых нитей, скрученных с расплющенной и посеребренной медной проволокой диаметром 35 ... ... 50 мкм.

У ткани артикула 4381 нитка свита с эмалированным микропроводом ПЭЛ-0,06 (ГОСТ 2773). Число металлических ниток может быть 30Х30, 20х20, 10Х10 и 6х6 на 1 см2. Поскольку провод изолирован, то поверхностное сопротивление этой ткани велико. В сетке ткани электрический контакт отсутствует. Она предназначена для защиты от колебаний СВЧ. Из такой ткани обычно изготавливают специальные костюмы для индивидуальной биологической защиты

В последние годы в качестве радиоэкранирующих материалов начали использоваться металлизированные ткани на основе синтетических волокон. Их получают методом химической металлизации (из растворов) тканей различной структуры и плотности. Существующие методы получения позволяет регулировать количество наносимого металла в диапазоне от сотых долей до единиц мкм и изменять поверхностное удельное сопротивление тканей от десятков до долей Ом. Экранирующие текстильные материалы обладают малой толщиной, легкостью, гибкостью; они могут дублироваться другими материалами (тканями, кожей, пленками), хорошо совмещаются со смолами и латексами.

*5.2.7 Электропроводный клей* (ЭПК) Заполнение эпоксидной смолы тонкодисперсными металлическими порошками (железо, кобальт, никель, и др.) позволило получить электропроводный клей, обладающий прочностью на отрыв до 50 МПа (500 кГ/см2) с удельной электропроводностью до 10-6 (Ом⋅м)-1, стойкий не только к влаге, но и к различным агрессивным средам и обеспечивающий незначительную усадку после отвердения. Время отвердения может быть доведено до пяти минут, если этот процесс проводится с помощью токов высокой частоты.

Наряду с применением ЭПК взамен пайки, болтовых соединений и т. д., представляется целесообразным использовать его и в технике электромагнитного экранирования. Шовное соединение, крепление контактных систем и различных элементов экранов, заполнение щелей и малых отверстий, установка экрана на несущей конструкции - эти и другие операции успешно могут быть осуществлены с помощью ЭПК при высокой эффективности экранирования и сокращении объема монтажных работ.

Изменяя консистенцию ЭПК до состояния краски и сохраняя поверхностное сопротивление даже до 0,1 Ом на единицу площади, можно получить эффективность экранирования 60 ... 65 дБ, приближающуюся к эффективности металлов. В БГУИР предлагаются новые составы ЭПК. Например, в экранирующей структуре материал/металлический отражатель используется материал на основе силикогеля и связующий герметик из жидкого стекла и клея ПВА.

*5.2.8 Токопроводящие краски*. Токопроводящие краски создаются на основе диэлектрического плёнкообразующего материала с добавлением в него проводящих составляющих, пластификатора и отвердителя. В качестве токопроводящих пигментов используют коллоидное серебро, графит, сажу, оксиды металлов, порошковую медь, алюминий. Токопроводящие краски обычно устойчивы и сохраняют свои начальные свойства в условиях резких климатических изменений и механических нагрузок. В качестве токопроводящих пигментов в этих красках применяют коллоидное серебро, медь, графит, алюминий, порошкообразное золото. Обычная масляная краска обладает довольно большой отражающей способностью (до 30%), гораздо лучше в этом отношении известковое покрытие.

Использование токопроводящих красок для электромагнитного экранирования является весьма перспективным направлением, так как их применение исключает необходимость проведения сложных и трудоемких работ по монтажу экрана, соединению его листов и элементов между собой. С помощью токопроводящих красок экран любого назначения и на любой основе может быть быстро изготовлен даже не в производственных условиях. При этом может быть обеспечена электромагнитное экранирование не менее 30 дБ в широком диапазоне частот.

*5*.*2.9. Разработки новых материалов для экранов на кафедре защиты информации.* В БГУИР под руководством заведующего кафедрой защиты информации, доктора технических наук, профессора Леонида Михайловича Лынькова ведётся большая работа по исследованию экранов и проектированию новых их модификаций, Для устройства экранов исследованы свойства диоксида титана, шунгита и других материалов. По результатам работы только в последние годы защищены 2 докторских (В.А. Богуш, Т.В.Борботько), защищены 8 кандидатских диссертаций (А.В.Прудник, Н.В.Колбун-Насонова, Фан Н. Занг, И.С.Терех, Е.Криштопова, Хусейн Махмуд Альлябад, В.В.Маликов, Мохаммед аль Хатми), подготовлены к защите 1 кандидатская диссертация (С.Н.Петров). Отдельное направление представляет собой исследование экранов на основе гибких радиопоглощающих материалов с различного рода наполнителями. Активно исследуются композиционные металлосодержащие материалы для электромагнитных экранов СВЧ-диапазона

5.3 Заземление технических средств

Заземление — это устройство, состоящее из заземлителей и проводников, соединяющих заземлители с электронными и электрическими установками, приборами, машинами. Заземлителем называют проводник или группу проводников, выполненных из проводящего материала и находящихся в непосредственном соприкосновении с грунтом. Заземлители могут быть любой формы — в виде труб, стержня, полосы, листа проволоки и т. п. Заземлители в основном выполняют защитную функцию и предназначаются для соединения с землей приборов защиты. Отношение потенциала заземлителя Uз к стекающему с него току Iз называется **сопротивлением заземлителя** Rз. Значение сопротивления заземлителя зависит от удельного сопротивления грунта и площади соприкосновения заземлителей с землей.

Поскольку заземлители непосредственно соприкасаются с информационными объектами, по цепям заземления возможна утечка информации за счет наводок. Для контроля такой утечки принято измерять напряжения и (или) токи опасных сигналов в проводниках и других токопроводящих коммуникациях (цепях 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.

Борьба с утечкой информации по цепям заземления обычно проводится с помощью генераторов шума. Принцип действия генераторов заключается в подачу в цепь заземления сигнала шума, намного превышающего полезный сигнал тока или напряжения утечки. Выделить с помощью существующих средств перехвата полезный сигнал на уровне высокого, намного превышающего полезный сигнал шума, практически невозможно. Такие генераторы шума называются генераторами линейного зашумления, поскольку подают шум в линию ­ цепь заземления. Известны также генераторы, которые подают шум с помощью передающих антенн в окружающее пространство. Такие генераторы шума называются генераторами пространственного зашумления и используются для защиты информации от утечки по электромагнитному каналу.

5.4 Фильтрация

Акустическая энергия, возникающая при разговоре по телефону, может вызывать механические колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению электромагнитного излучения или к его изменению при определенных обстоятельствах. К пассивным методам защиты информации от утечки по электромагнитному каналу при телефонном разговоре является фильтрация (установка фильтров).

Простейшим *фильтром* является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов. Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного навязывания и не оказывать существенного влияния на полезные сигналы. Обычно для установки в звонковую цепь используются конденсаторы емкостью 1 мкФ, а для установки в микрофонную цепь – емкостью 0,01 мкФ. Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах (рис. 5.1) с ограничителем.

Возможность *ограничения* опасных сигналов основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используются два встречно включенных диода. Такие диоды имеют большое сопротивление (сотни кОм) для токов малой амплитуды и единицы Ом и менее – для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды полезных сигналов. Диодные ограничители включаются последовательно в линию звонка или непосредственно в каждую из телефонных линий (рис. 5.1).

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель. К ним относятся: устройства «Экран», «Гранит-8», «Корунд», «Грань-300» и др. Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от «высокочастотного навязывания».

|  |  |
| --- | --- |
| лаб1вар1  Вариант 1 | лаб1вар2  Вариант 2 |
| лаб1вар3  Вариант 3 | лаб1вар4  Вариант 4 |

Рис. 5.1 – Схемы простейших фильтров

5.5 Согласованные нагрузки волноводных, коаксиальных и волоконно‑оптических линий

*5.5.1 Поглощающие согласованные нагрузки* используются в целях полного поглощения энергии электромагнитных колебаний. Волноводные нагрузки низкого уровня мощности (до десятков ватт), как правило, представляют собой отрезки короткозамкнутых волноводов с помещенными внутрь поглотителями (СВЧ-резисторами). В поглотителях происходит преобразование электромагнитной энергии в тепло. В СВЧ диапазоне такое преобразование может происходить на поверхности поглотителя за счет токов проводимости и в толще диэлектрика (с большими потерями).

В качестве твердых объемных поглотителей используются смеси полупроводящих окислов из мелкодисперсного карбонильного железа с твердыми наполнителями (полистирол, эпоксидная смола, различные виды керамики с примесью проводящих веществ). Поглощающие нагрузки применяются в качестве эквивалентов антенн излучающих радиоэлектронных средств, а также для других целей (в циркуляторах, переключателях, делителях мощности и т.д.). Эквиваленты антенн используются при проведении различного рода измерений в высокочастотных трактах радиотехнических средств специального назначения в процессе их разработки, испытаний и эксплуатации, а также при проведении регламентных работ на этих средствах.

*5.5.2 Антенные насадки* используются при проведении испытаний радиотехнических средств методом закрытых трактов. В этом случае радиоканал (антенна передающего устройства — среда распространения радиосигнала — антенна приемного устройства) замещается антенной насадкой, исключающей (или существенно ослабляющей) излучение радиосигнала в окружающее пространство. Использование антенной насадки позволяет локализовать радиоизлучение в пределах ее рабочего объема и существенно ослабить (на 30—40 дБ) уровень радиоизлучений.

*5.5.3 Соединители волноводных, коаксиальных и оптических трактов.* Соединителями волноводных трактов называют элементы, обеспечивающие соединение отдельных отрезков волноводов и узлов друг с другом. От качества электрического контакта в местах соединения зависит такая важная характеристика как электрогерметичность тракта. Если в месте соединения контакт ненадежен, то возможно излучение электромагнитного поля из щелей в окружающее пространство. В настоящее время используют два основных типа соединения волноводов — контактные и дроссельные. Контактное соединение может быть неразъемным и разъемным. Неразъемное соединение можно осуществить, например, с помощью внешних муфт. Возможна реализация неразъемных контактных соединений путем стыковки и холодной сварки торцов волноводов.

Разъемные контактные соединения выполняются с помощью специальных контактных фланцев. Плоские контактные фланцы за счет соприкосновения тщательно обработанных торцевых поверхностей обеспечивают непосредственный электрический контакт между соединяемыми волноводами. Контактные поверхности фланцев стягиваются между собой болтами или струбцинами. Соединение гибких и жестких коаксиальных волноводов осуществляется с помощью специальных разъемов. Разъемные соединительные устройства обычно используются в оконечной аппаратуре.

5.6 Звукоизоляция помещений

Основная идея пассивных средств защиты акустической информации - это снижение соотношения сигнал/шум в возможных точках перехвата информации за счет снижения информативного сигнала. При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо:

— в качестве перекрытий использовать акустически неоднородные конструкции;

— в качестве полов использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;

— потолки выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

— в качестве стен и перегородок использовать многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т.п.).

Прохождение звуковых волн через препятствия осуществляется различными путями:

— через поры, окна, щели, двери и т.д. (путем воздушного переноса):

— через материал стен, по трубам тепло-, водо- и газоснабжения и т.д. за счет их продольных колебаний (путем материального переноса);

— через материал стен и перегородок помещения за счет из поперечных колебаний (путем мембранного переноса).

Выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому (ограждающие конструкции, трубопроводы) каналам. Для сплошных, однородных, строительных конструкций ослабление акустического сигнала, характеризующее качество звукоизоляции на средних частотах, рассчитывается по формуле:

|  |  |
| --- | --- |
|  | (5.1) |

где qог, - масса 1 м2 ограждения, кг; f - частота звука, Гц.

Во временно используемых помещениях применяют складные экраны. Применение звукопоглощающих материалов, преобразующих кинетическую энергию звуковой волны в тепловую, имеет некоторые особенности, связанные с необходимостью создания оптимального соотношения прямого и отраженного от преграды акустических сигналов. Чрезмерное звукопоглощение снижает уровень сигнала, большое время реверберации приводит к ухудшению разборчивости речи.

Поглощающие материалы могут быть сплошными и пористыми. Обычно пористые материалы используют в сочетании со сплошными. Один из распространенных видов пористых материалов — облицовочные звукопоглощающие материалы. Их изготавливают в виде плоских плит или рельефных конструкций (пирамид, клиньев и т.д.), располагаемых или вплотную, или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т.п.).

Отдельную группу звукопоглощающих материалов составляют резонансные поглотители. Они подразделяются на мембранные и резонаторные. Мембранные поглотители представляют собой натянутый холст (ткань), тонкий фанерный (картонный) лист, под которым располагают хорошо демпфирующий материал (материал с большой вязкостью — например, поролон, губчатую резину, строительный войлок и т.д.). В такого рода поглотителях максимум поглощения достигается на резонансных частотах.

Повышение звукоизоляции стен и перегородок помещений достигается применением слоистых или раздельных их конструкций. В многослойных перегородках и стенах целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например, бетон—поролон).

Звукоизолирующая способность сложных стен, имеющих дверные и оконные проемы, зависит от звукоизоляции дверей и окон. Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна дверей к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д. При недостаточной звукоизоляции однослойных дверей используются двойные двери с тамбуром, облицованные звукопоглощающим материалом.

Звукопоглощающая способность окон, так же как и дверей, зависит главным образом от поверхностной плотности стекла и прижатия притворов. Обычные окна с двойными переплетами обладают более высокой (на 4—5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. В случаях, когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20—40 мм и с воздушным зазором между стеклами не менее 100 мм). Повышенное звукопоглощение обеспечивается применением конструкции окон на основе стеклопакетов с герметизацией и заполнением зазора между стеклами различными газовыми смесями.

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т.д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы. Их надежная звукоизоляция обеспечивается применением специальных гильз, прокладок, глушителей, вязкоупругих заполнителей и т.д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием сложных акустических фильтров и глушителей.

5.7 Защита от высокочастотного навязывания

Наиболее часто такой способ используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. Технический канал утечки информации путем «высокочастотного навязывания» может быть осуществлен путем несанкционированного контактного введения токов высокой частоты в цепи с нелинейными или параметрическими элементами, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах появляется вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться в окружающее пространство, где он может быть перехвачен и расшифрован злоумышленником.

**Лекция 6 Активные методы защиты информации от утечки по электромагнитному и акустическому каналам**

На сегодняшний день виброакустическая защита помещений от прослушивания представляет собой одну из наиболее динамично развивающихся областей защиты информации. В первую очередь это обусловлено уникальными особенностями речевой информации, циркулирующей в помещениях: большим объемом и оперативностью обмена, высокой конфиденциальностью некоторых сообщений, возможностью идентификации личности человека, делающего сообщение, и даже возможностью определения личного отношения говорящего к озвучиваемой информации и составления его психологического портрета. Все это делает проблему защиты акустической информации чрезвычайно важной. В настоящее время на рынке спецтехники разработчиками представлено несколько десятков систем активной защиты акустической информации.

6.1 Пространственное зашумление

В большинстве случаев для активной защиты воздушных каналов используют системы виброзашумления, к выходам которых подключают громкоговорители. Так, в комплекте системы виброакустической защиты АNG-2000 (фирма RЕI) поставляется акустический излучатель ОМS-2000. Однако применение динамиков создает не только маскирующий эффект, но и помехи нормальной повседневной работе персонала в защищаемом помещении.

Малогабаритный (111 × 70 × 22 мм) генератор WNG-023 диапазона 100...12000 Гц в небольшом замкнутом пространстве создает помеху мощностью до 1 Вт, снижающую разборчивость записанной или переданной по радиоканалу речи. Эффективность систем и устройств виброакустического зашумления определяется свойствами применяемых электроакустических преобразователей (вибродатчиков), трансформирующих электрические колебания в упругие колебания (вибрации) твердых сред. Качество преобразования зависит от реализуемого физического принципа, конструктивно-технологического решения и условий согласования вибродатчика со средой.

Как было отмечено, источники маскирующих воздействий должны иметь частотный диапазон, соответствующий ширине спектра речевого сигнала (200...5000 Гц), поэтому особую важность приобретает выполнение условий согласования преобразователя в широкой полосе частот. Условия широкополосного согласования с ограждающими конструкциями, имеющими высокое акустическое сопротивление (кирпичная стена, бетонное перекрытие) наилучшим образом выполняются при использовании вибродатчиков с высоким механическим импендансом подвижной части, каковыми на сегодняшний день являются пьезокерамические преобразователи.

Во время работы вибродатчиков возникают паразитные акустические шумы, вносящие дискомфорт и нарушающие нормальные условия труда в защищаемом помещении. В зависимости от механизма образования различают акустические шумы, переизлученные твердой средой, и звуковые колебания, генерируемые собственно преобразователем. В этом случае соотношение акустических сопротивлений имеет вид:

|  |  |
| --- | --- |
| . | (6.1) |

Как следует из соотношения (4.3), в силу большой разницы акустических сопротивлений уровень шумов, переизлученных средой в воздух, весьма незначителен, поэтому основным источником паразитных акустических шумов является вибродатчик. На рис. 6.1 приведены амплитудно-частотные характеристики акустических помех, создаваемых при работе систем виброакустического зашумления. Внешний вид изделий приведен на рис. 6.2.

Монтаж вибродатчиков, как правило, сопряжен с необходимостью выполнения трудоемких строительно-монтажных работ – сверлением, установкой дюбелей, выравниванием поверхностей, приклеиванием и т.п.

|  |
| --- |
| АЧХ_ГШ  Рис. 6.1 – Амплитудно-частотные характеристики акустических помех: 1 – А1G-2000+TRN-2000; 2 – VNG-006DМ; 3 – VNG-006 (1997 г.); 4 – Заслон-АМ и Порог-2М; 5 – фоновые акустические шумы помещения |
| 1 2 3 4  а б в г  5 6  д е  Рис. 6.2. Внешний вид систем виброакустического зашумления: вибродатчики: а – КВП-2; б – КВП-6; в – КВП-7; г – КВП-8; д – Шорох-1; е – Шорох-2 |

Увеличение мощности помехи создает повышение уровня паразитного акустического шума, что вызывает дискомфорт у работающих в помещении людей. Это приводит к отключению системы в наиболее ответственные моменты, создавая предпосылки к утечке конфиденциальных сведений.

Эксплуатационно-технические параметры современных систем виброакустического зашумления приведены в табл.6.1–6.2.

Таблица 6.1 – Параметры современных систем виброакустического зашумления

|  |  |  |  |
| --- | --- | --- | --- |
| Характеристика | Шорох-1 | Шорох-2 | АМВ-2000 |
| Количество независимых генераторов | 3 | 1 | 1 |
| Рабочий диапазон частот, кГц | 0,2...5,0 | 0,2...5,0 | 0,25...8,0 |
| Наличие эквалайзера | Есть | Есть | Нет |
| Максимальное количество вибродатчиков | 72 | 24 | 18 |
| Радиус действия стеновых вибродатчиков на перекрытии толщиной 0,25 м, м | 6 | 6 | 5 |
| Радиус действия оконных вибродатчиков на стекле толщиной 4 мм, м | 1,5 | 1,5 | - |
| Возможность акустического зашумления | Есть | Есть | Есть |

Система «Шорох-2» обеспечивает защиту от следующих технических средств съема информации:

* устройств, использующих контактные микрофоны (электронные, проводные и радиостетоскопы);
* устройств дистанционного съема информации (лазерные микрофоны, направленные микрофоны);
* закладных устройств, установленных в строительных конструкциях.

Таблица 6.2 – Характеристики генератора

|  |  |
| --- | --- |
| Вид генерируемой помехи | Аналоговый шум с нормальным распределением плотности вероятности |
| Действующее значение напряжения помехи | Не менее 100 В |
| Диапазон генерируемых частот | 157...5600 Гц |
| Регулировка спектра генерируемой помехи | Пятиполосный,  октавный эквалайзер |
| Центральные частоты полос регулировки спектра | 250, 500,1000, 2000, 4000 Гц |
| Глубина регулировки спектра по полосам, не менее | ± 20 дБ |

Система «Шорох-2» обеспечивает защиту таких элементов строительных конструкций, как:

* внешние стены и внутренние стены жесткости, выполненные из монолитного железобетона, железобетонных панелей и кирпичной кладки толщиной до 500 мм;
* плиты перекрытий, в том числе и покрытые слоем отсыпки и стяжки;
* внутренние перегородки из различных материалов;
* остекленные оконные проемы;
* трубы отопления, водоснабжения, электропроводки;
* короба систем вентиляции;
* тамбуры.

Электроакустические преобразователи устанавливаются на стекла оконных проемов, внутренние и внешние стены, плиты перекрытий, трубы инженерных коммуникаций. Радиус действия одного преобразователя в зависимости от вида (КВП-2, КВП-6, КВП-7, КВП-8) от 1,5 до 6±1 м. Диапазон эффективно воспроизводимых частот 175...6300 Гц. Преобразование электрических колебаний в механические (вибрационные) происходит по пьезоэлектрическому принципу.

6.2 Методы защиты информации путём наложения маскирующего сигнала

Системы для защиты речевой информации в помещениях в основном построены на принципе маскирования речевого сигнала с помощью широкополосных шумовых сигналов, причем маскирующий сигнал, в правильно спроектированной системе защиты речевой информации имеет максимальное значение в местах утечки речевой информации (например вентиляционные каналы, коммуникации и т.п.). При этом шум должен превышать речевой сигнал на столько, чтобы исключить утечку информации с заданной степенью вероятности. Необходимая величина превышения шума над сигналом определяется соответствующими нормативными документами. Однако повышение уровня маскирующего сигнала не всегда возможно, так как, с одной стороны, приводит к возникновению дискомфорта в защищаемом помещении, с другой – повышается энергоемкость системы, увеличивается ее стоимость. Как показывает опыт эксплуатации известных систем защиты речевой информации, повысить их эффективность, не увеличивая энергоемкость, а следовательно, габариты вес и стоимость, можно, оптимизируя вид маскирующего сигнала. Однако в настоящее время вопросы выбора наиболее оптимального маскирующего сигнала для применения в системах защиты речевой информации остаются открытыми.

*Виды маскирующего сигнала: белый и розовый шум, речевая смесь.* К акустическим сигналам относятся в ряде случаев и акустические шумы: «белый», «розовый» и «речевой». Термин «*белый*» относится к шумам, имеющим одинаковую спектральную плотность во всем частотном диапазоне, «*розовый*» – к шумам с тенденцией спада плотности на 3 дБ/окт в сторону высоких частот. *Речевые* шумы – шумы, создаваемые одновременным разговором нескольких человек.

В технике связи широко исследуется влияние шумов и помех на характеристики звуков речи. Под действием шумов и помех изменяются огибающие спектра звуков речи, временные огибающие как в отдельных полосках частотного диапазона, так и во всем диапазоне. Из опыта передачи речевых сообщений по каналам линий связи по восприятию на слух, по результатам экспертных оценок наибольшим эффектом в отношении искажения характеристик звуков речи обладает речевая помеха, так как она по своим данным наиболее близка к речи.

6.3 Основные принципы акустической маскировки, используемые сигналы и их спектры

*6.3.1 Маскировкой* называют явление, выражающееся в том, что восприятие звуков, несущих определенную информацию, ухудшается при одновременном звучании других, мешающих звуков. В результате возникает потеря части или даже всей информации. Маскировка непосредственно связана со свойством слухового аппарата – его нелинейностью. Для маскирования речевого сигнала необходимо создать достаточный уровень шумового сигнала. Нелинейность слуха проявляется в том, что при воздействии на барабанные перепонки достаточно громкого синусоидального сигнала с частотой f1 в слуховом аппарате зарождаются гармоники этого звука с частотами 2f1, 3f1 и т. д. Поскольку в первичном воздействующем тоне этих гармоник нет, они получили название субъективных гармоник. Установлено, что при уровнях интенсивности менее 40 дБ субъективные гармоники не возникают, так что ощущение чистого тона возможно лишь при интенсивности менее 40 дБ.

Количественно маскировка оценивается путем определения порога слышимости синусоидальных звуков (или узкополосных шумов) в присутствии мешающего сигнала. Однако эффект маскировки сложных сигналов (например речи или музыки) нельзя определить по изменению порога слышимости, так как эта величина имеет смысл лишь в том случае, когда может быть отнесена к какой-либо частоте. Для сложного сигнала маскирующее действие можно определить по величине потери информации.

Например для речи такой мерой может служить понятие разборчивость речи. Под *разборчивостью речи* подразумевается отношение числа элементов речи, правильно принятых слушателями, к общему числу элементов, переданных по тракту. В качестве передаваемых элементов речи используют звуки, слоги, слова, цифры, фразы. В связи с этим различают звуковую, слоговую, словесную, цифровую или фразовую разборчивость речи. Между всеми этими видами разборчивости речи есть вполне определенные статистические взаимосвязи, имеющие свое различие для разных языков.

Следует учитывать, что в настоящее время существуют способы очистки зашумленных речевых сигналов с помощью специального оборудования и применения специальных систем распознавания и идентификации речи с использованием ПК. Такие системы обладают большими возможностями для очистки речевого сигнала от шума. Эти методы широко применяются в криминалистике, а также спецслужбами для идентификации личности говорящего или для восстановления речевой информации. Можно считать, что в ряде случаев, вопрос очистки речевого сигнала от шумов является вопросом времени и имеющихся средств. Поэтому создание маскирующих сигналов является задачей с компромиссным решением и зависит от требований поставленного задания. Возникает задача создания маскирующих сигналов, удовлетворяющих каким-то определенным требованиям, например для защиты от простого прослушивания, для защиты от прослушивания с записью на диктофон и дальнейшей обработке, для защиты от прослушивания с применением специальных методов обработки.

*6.3.2 Параметры маскирующего сигнала.* Идея использования в качестве помех маскирующего сигнала, в основе которых лежат речь или музыкальная фонограмма, в последнее время не только интенсивно рекламируется, но и нашла уже техническое воплощение. Основным достоинством этой идеи считается возможность снижения уровня помехового сигнала на 4–10 дБ по сравнению с использованием широкополосной шумовой помехи. Это позволяет существенно снизить уровень паразитных акустических шумов, излучаемых преобразователями, и увеличить комфортность ведения переговоров при сохранении необходимого уровня защиты.

Однако следует обратить внимание на следующий аспект. Формантный метод определения разборчивости речи основан на следующем положении:

|  |  |
| --- | --- |
|  | (6.2) |

где АФ – формантная разборчивость (однозначно связанная со слоговой и словесной); Wn – коэффициент разборчивости для каждой полосы равной разборчивости, зависящий от соотношения сигнал/шум (S/N) для этой же полосы.

Отсюда видно, что разборчивость речевой информации зависит только от соотношения сигнал/помеха в каждой полосе равной разборчивости и никак не зависит от типа помехи, формирующей данное соотношение (речевая, шумовая, реверберационная). Более того, следует отметить, что речь и музыка являются существенно нестационарными процессами. Так, например колебания уровня в фонограмме дикторской речи составляют 25–35 дБ, а в фонограмме симфонического произведения – 65–75 дБ. Таким образом, даже если средний уровень речевой или музыкальной помехи будет достаточен для закрытия информации, в отдельные моменты времени такая помеха будет иметь неоправданно высокий уровень, а в другие – информация окажется незащищенной. Повысить стационарность речевой помехи можно путем многократного наложения различных фонограмм, причем, чем больше количество используемых при этом фонограмм, тем выше качество сигнала помехи. Нет необходимости самостоятельно осуществлять этот процесс: такие фонограммы, составленные в соответствии с ГОСТом, широко используются в практике акустических измерений, а записанный на них сигнал называется речевым хором. Спектральные, временные и статистические характеристики речевого хора довольно точно соответствуют аналогичным характеристикам стандартного розового шума (шум, спектр которого спадает с ростом частоты со скоростью 3 дБ/окт), что показано на рис. 6.3. Поэтому, если правильно ограничить частотную полосу розового шума, его вполне можно использовать вместо речевого хора.

|  |
| --- |
| Рис. 6.3 – Спектральные характеристики «речевого хора» и розового шума |

Таким образом, для защиты речевой информации наиболее целесообразно использовать помеховый сигнал в виде стандартного речевого хора или розового шума.

6.4 Электромагнитное зашумление

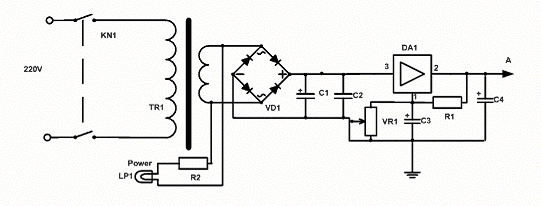
В подразделах 6.1-6.3 рассматривались активные методы защиты информации от утечки по акустическому каналу. Рассмотрим такие же методы защиты информации от утечки по электромагнитному каналу. Основной из них – электромагнитное зашумление.

Технические средства (ТС) электромагнитного зашумления выполняют одну и ту же задачу: обеспечивают защиту ИО или помещения, где находится ИО, от утечки информации за счет ПЭМИН. Эта защита обеспечивается внесением в каналы утечки такого зашумляющего сигнала, на фоне которого выделить полезный информативный сигнал становится невозможным. Кроме того, названные ТС затрудняют работу радиомикрофонов и блокируют работу радиомикрофонов с дистанционным включением, блокируют работу сотовых телефонов. Угрозу информационной безопасности за счёт перехвата информации по каналу ПЭМИН называют TEMPEST (Telecommunications Electronics Material Protected From Emanating Spurious Transmissions) – атакой.

Классическим случаем TEMPEST – атаки является пример, опубликованный в книге воспоминаний бывшего сотрудника английской разведки МI-5 Питера Райта (Peter Wright), "Шпионский улов" ("Spycatcher") в 1986 году. В конце 60-х Англия вела переговоры о вступлении в ЕЭС, и английскому правительству очень важна была информация о позиции Франции в этом вопросе. Сотрудники МИ-5 вели постоянный перехват зашифрованных сообщений французской дипломатии, но все усилия МИ-5 по вскрытию шифра не увенчались успехом. Тем не менее, Питер при анализе излучений заметил, что наряду с основным сигналом присутствует и другой, очень слабый сигнал. Инженерам удалось настроить приемную аппаратуру на этот сигнал и демодулировать его. К их удивлению, это было открытое незашифрованное сообщение. Оказалось, что шифровальная машина французов, впрочем, как и любая другая электрическая машина, имела побочное ЭМИ, которое модулировалось информационным сигналом еще до момента его кодирования. Таким образом, путем перехвата и анализа побочных излучений французской шифровальной машины, английское правительство, даже не имея ключа для расшифровки кодированных сообщений, получало всю необходимую информацию. Задача, стоящая перед МИ-5, была решена. Безусловно, это далеко не единственный пример результативного применения TEMPEST-атаки, но шпионские организации не стремятся поделиться своими тайнами с широкой общественностью. Более того, TEMPEST-атаки по отношению друг к другу стали применять и конкурирующие коммерческие фирмы, и криминальные структуры

Анализируя успехи отдела МИ-5 английской разведки, можно сделать вывод, что при использовании французами эффективных зашумляющих ТС никаких успехов у англичан не было бы. Малогабаритные и маломощные ТС электромагнитного зашумления, обеспечивающие защиту небольшого ИО, называют генераторами шума. Более мощные ТС, способные обеспечить защиту целого помещения или группы помещений, называют системами пространственного зашумления. Во многих случаях генераторы шума и системы пространственного зашумления дополнены некоторыми другими функциями помимо зашумления – например, функциями маскировки информативных побочных электромагнитных излучений ПЭВМ и периферийного оборудования, а также радиомикрофонов (генератор шума [**SEL SP 21 B1**](http://www.zinfo.ru/item/374/)). Генератор шума «Купол-4М» кроме зашумления может блокировать каналы дистанционного управления радиоуправляемых взрывных устройств. Разделение зашумляющих устройств на генераторы шума и системы пространственного зашумления является довольно условным – точной площади зашумлённого помещения, начиная с которой вместо генератора шума следует применять системы пространственного зашумления никто не установил. Условимся в дальнейшем устройства стоимостью свыше 1000 $ (примерно 30000 – 35000 рублей РФ) именовать системами пространственного зашумления, более дешёвые устройства – генераторами шума.

Схема генераторами шума, показанная на рис. 6.4, – классическая. Данное решение применено в таких генераторах как "ГНОМ-3", "ГШК", часто приводится в Интернет ресурсах и в радиолюбительской литературе. Несмотря на простоту, схема выдержала испытания временем, а приборы "Гном" и "ГШК" сертифицированы. Подробно останавливаться на схемном решении прибора нецелесообразно. Однако следует отметить некоторые конструктивные особенности. В целом прибор на рис. 6.4 состоит из трёх основных частей, собранных в одном корпусе. Это блок питания с малой величиной пульсаций выходного напряжения, позволяющий из сетевого напряжения 220 В 50 Гц получить постоянное напряжение 10-18 В, работающий от этого постоянного напряжения мультивибратор (он является собственно генератором шума), и блок фильтров. Вместо мультивибратора может быть использован любой другой генератор несинусоидальных колебаний – автогенератор, блокинг-генератор, то же на микросхемах, а не на транзисторах, и т.д. Генерируемые несинусоидальные колебания, как и любые другие несинусоидальные колебания, можно разложить в ряд Фурье. При этом исходное несинусоидальное колебание будет представлено суммой гармоник – первой на частоте исходного колебания, затем 2-й (на удвоенной частоте), затем 3-ей (на утроенной частоте исходного колебания), и.т.д. С



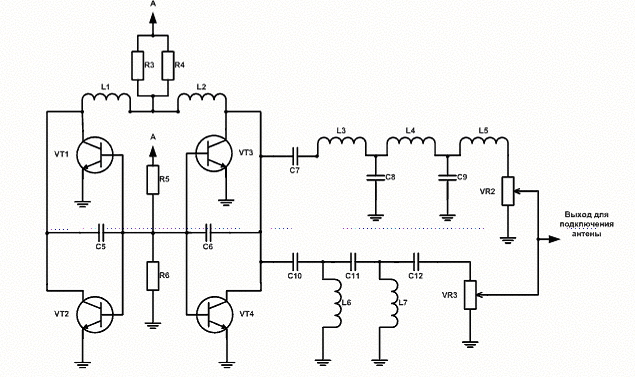


Рис. 6.4 – Схема радиочастотного шумогенератора

ростом частоты амплитуда гармоник будет уменьшаться, в пределе давая гармонику с бесконечной частотой и нулевой амплитудой. Каждый отдельный фильтр блока фильтров представляет собой в общем случае полосовой фильтр, выделяющий закреплённую за ним полосу частот. Гармоники этой полосы частот и есть выходной сигнал шумогенератора в заданном частотном диапазоне.

В приборе применён регулируемый блок питания, позволяющий изменять питание генератора от 1.5 V до 18 V при токе до 2А. Пользоваться данной регулировкой можно для оптимизации выходной мощности. Регулировку следует проводить с применением индикатора поля, измеряя при этом ток потребления (ток не должен превышать в данном случае 2А). Рассматривая подробнее блок питания, видно, что схема выпрямителя на трансформаторе TR1 и диодном мостике VD1 – классическая.

Одним из наиболее распространённых переносных генераторов шума является ГНОМ-3, внешний вид которого показан на рис. 6.5

Рис. 6.5 – ГНОМ – 3. Внешний вид

ГНОМ-3М является усовершенствованной моделью ГНОМа 3. Краткие технико-экономические характеристики генераторов ГНОМ-3М и зарубежного его аналога NGR-900 приведены в табл. 6.3

Таблица 6.3

Краткие технико-экономические характеристики генераторов ГНОМ-3М и NGR-900

|  |  |  |
| --- | --- | --- |
|  | ГНОМ-3М | NGR-900 |
| Диапазон частот, мГц, в т.ч. на выходах Ф1, Ф2, Ф3 | 0,15 – 1000 | 0,15 – 1000 |
| на выходе Ф1 | 0,15 – 30 | 0,15 – 30 |
| на выходе Ф2 | 30 – 400 | 30 – 1000 |
| на выходе Ф3 | 400 – 1000 |  |
| Уровень сигнала на выходах Ф1, Ф2, Ф3, дБ, не менее |  |  |
| на выходе Ф1 | 70/50\* | 30 |
| на выходе Ф2 | 75/50 | 40 |
| на выходе Ф3 | 45/50 |  |
| Максимальная потребляемая мощность, Вт | 40 | 30 |
| Габариты, мм | 300х192х56 | 210х155х60 |
| Масса, кг, не более | 3,0 | 1,7 |
| Питание | 220 В, 50 Гц или трёхфаз-ное 380 В | 220 В, 50 Гц |
| Время непрерывной работы, ч | 24 | 8 |

\* – В числителе указан уровень сигнала на выходах, предназначенных для подключения антенн, в знаменателе – уровень на выходах Ф1, Ф2, Ф3, предназначенных для подключения генератора к трёхфазной сети переменного тока 380 В (на нагрузке 400 мА).

На рис. 6.6 приведено фото внутренней конструкции генератора шума ГНОМ-3

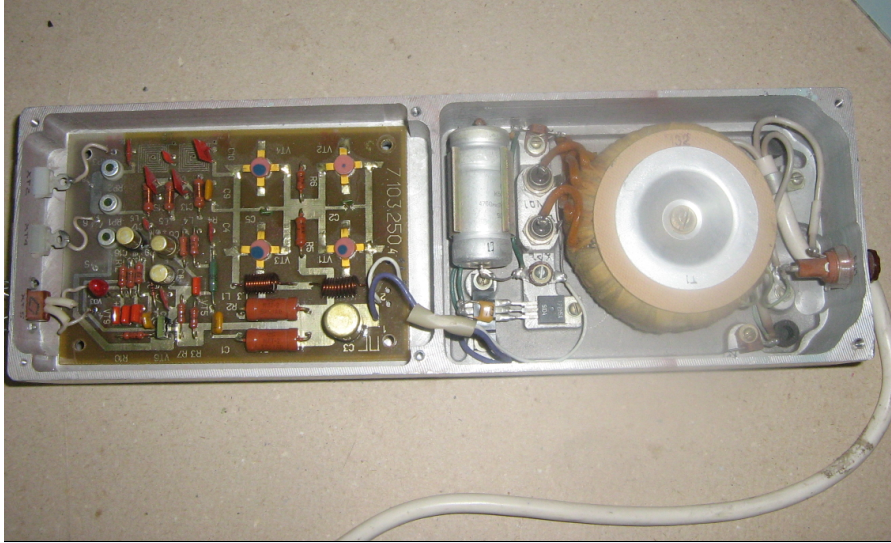


Рис. 6.6 – Фото внутренней конструкции генератора шума ГНОМ-3

6.5 Выжигатели телефонных закладных устройств

Подслушивающие устройства, подключённые к телефонной сети, называются телефонными закладными устройствами (закладками). Для их устранения используется метод «выжигания». Метод реализуется путем подачи в линию высоковольтных (напряжение более 1500 В) импульсов, мощностью 15-50 ВА, приводящих к электрическому "выжиганию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии. Подача высоковольтных импульсов осуществляется при отключении телефонного аппарата от линии. При этом для уничтожения параллельно подключенных устройств подача высоковольтных импульсов осуществляется при разомкнутой, а последовательно подключенных устройств – при "закороченной" (как правило, в телефонной коробке или щите) телефонной линии.

Данный метод реализуют приборы, называемые «выжигателями» (рис. 6.7).



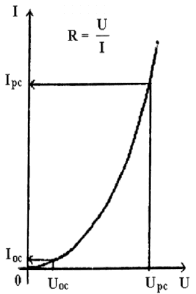
Рис. 6.7 – выжигатель устройств съёма информации ГИ-1500

Основные характеристики "выжигателей" телефонных закладных устройств

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование характеристик | Тип устройства | | |
| "Кобра" | КС-1300 | КС-1303 |
| Напряжение на выходе, В | 1600 |  |  |
| Мощность импульса, ВА |  | 15 | 50 |
| Режимы работы | Автоматический Ручной | Автоматический Ручной | Ручной |
| Время непрерывной работы в автоматическом режиме | 20 с | 24 часа | - |
| Время непрерывной работы в ручном режиме | 10 мин |  |  |
| Временные интервалы, устанавливаемые таймером |  | от 10 мин до 2 суток |  |
| Габаритные размеры, мм | 65? 170х185 | 170х180х70 | 170х180х70 |
| Напряжение питания, В | 220 | 220 | 220 |
| Количество подключаемых телефонных линий | 1 | 2 | 2 |

6.6 Средства комплексной защиты телефонных линий

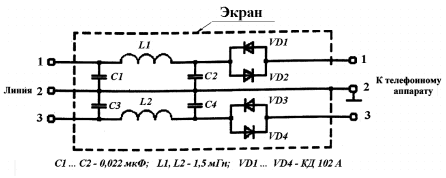
Для защиты телефонного аппарата от утечки речевой информации по электроакустическому каналу используются как пассивные, так и активные методы и средства. К наиболее широко применяемым **пассивным методам защиты** относятся:  *ограничение опасных сигналов; фильтрация опасных сигналов; отключение источников (преобразователей) опасных сигналов.* К **активным методам защиты** можно отнести: *метод низкочастотной маскирующей помехи; метод высокочастотной широкополосной маскирующей помехи.*

Возможность **ограничения опасных сигналов** основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используются два встречновключенных диода, имеющих вольт-амперную характеристику (зависимость значения протекающего по диоду электрического тока от приложенного к нему напряжения), показанную на рис. 6.8. Такие диоды имеют большое сопротивление (сотни кОм) для токов малой амплитуды и единицы Ом и менее - для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияния на прохождение через диоды полезных сигналов.  
  
  
Рис. 6.8 – Вольтамперная характеристика диода VD

Диодные ограничители включаются последовательно в линию звонка или непосредственно в каждую из телефонных линий (рис. 6.9).

**Фильтрация опасных сигналов** используется главным образом для защиты телефонных аппаратов от "высокочастотного навязывания" и рассмотрена в предыдущей лекции.

Для пассивной защиты телефонных аппаратов, как правило, используются комплексные устройства, сочетающие фильтр и ограничитель. К ним относятся устройства типа "Экран", "Гранит-8", "Грань-300" и др. (рис. 6.9). Эти устройства обеспечивают подавление информационного НЧ сигнала более чем на 80 дБ и вносят затухание для ВЧ в полосе частот от 30 кГц до 30 МГц более 70 дБ.

Рис. 6.9 – Схема комплексного устройства защиты телефонных аппаратов "Гранит-8"

**Отключение телефонных аппаратов от линии** при ведении в помещении конфиденциальных разговоров является наиболее эффективным методом защиты информации. Самый простой способ реализации этого метода защиты заключается в установке в корпусе телефонного аппарата или телефонной линии специального выключателя, включаемого и выключаемого вручную. Более удобным в эксплуатации является установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке. К типовым устройствам, реализующим данный метод защиты, относится изделие "Барьер-М1". Устройство имеет следующие режимы работы: дежурный режим, режим передачи сигналов вызова и рабочий режим

**Активные методы защиты** телефонных аппаратов от утечки информации по электроакустическому каналу заключаются в подаче в телефонную линию при положенной телефонной трубке маскирующего низкочастотного (диапазон частот от 100 Гц до 10 кГц) шумового сигнала (**метод низкочастотной маскирующей помехи**). Устройства защиты, реализующие метод низкочастотной маскирующей помехи, часто называют средствами линейного зашумления. Они подключаются в разрыв телефонной линии, как правило, непосредственно у корпуса телефонного аппарата. Шумовой сигнал подается в линию в режиме, когда телефонный аппарат не используется (трубка положена). При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается. К сертифицированным средствам линейного зашумления относятся устройства типа МП-1А (защита аналоговых телефонных аппаратов) и МП-1Ц (защита цифровых телефонных аппаратов) и др.

**Метод высокочастотной широкополосной маскирующей** помехи заключаются в подаче в телефонную линию при положенной телефонной трубке маскирующего высокочастотного широкополосного (в диапазоне часто от 20 кГц до 30 МГц) шумового сигнала. Прослушивание телефонных разговоров осуществляется с использованием электронных устройств перехвата речевой информации, подключаемых к телефонным линиям последовательно (в разрыв одного из проводов), параллельно (одновременно к двум проводам) и с помощью индукционного датчика (бесконтактное подключение).

Для активной защиты телефонных линий используются как простые устройства, реализующие один метод защиты, так и сложные, обеспечивающие комплексную защиту линий различными методами, включая защиту от утечки информации по электроакустическому каналу. К последним относятся устройстве "Цикада-М", "Прокруст", "Протон»

6.7 Технические средства защиты информации от утечки по электромагнитному каналу

К ТС защиты информации от утечки по электромагнитному каналу относятся пассивные устройства (экраны) и активные устройства (генераторы шума и системы зашумления. Все перечисленные устройства рассмотрены выше

6.8 Методы и средства обнаружения и подавления закладных устройств

Наиболее информативным и легко измеряемым параметром телефонной линии является напряжение в ней при положенной и поднятой трубке. Это обусловлено тем, что в состоянии, когда телефонная трубка положена, в линию подается постоянное напряжение в пределах 60–64 В (для отечественных АТС) или 25–36 В (для импортных мини АТС) При поднятии трубки в линию от АТС поступает сигнал, преобразуемый в телефонной трубке в длинный гудок, а напряжение в линии уменьшается до 10–12 В. Если к линии будет подключено закладное устройство, то эти параметры изменятся (напряжение будет отличаться от типового для данного телефонного аппарата).

Кроме того, возможен анализ переменной составляющей сигнала на линии. Например, при появлении сигнала с частотой более 50 кГц может быть сделан вывод о том, что к линии, возможно, подключена аппаратура ВЧ навязывания, или по линии передается модулированный высокочастотный сигнал. На основе измерений перечисленных параметров и их анализа прибор «принимает» решение о наличии несанкционированных подключений, сигнализирует об изменении параметра линии или наличии в ней посторонних сигналов. Есть приборы, которые кроме блока измерения и анализа параметров, имеют в своем составе и блок для постановки активной заградительной помехи. Примером анализатора телефонных линий является прибор на рис. 6.10. Подавление обнаруженной телефонной закладки кроме постановки заградительной помехи может быть проведено также методом выжигания.



Рис. 6.12 –Индикатор состояния телефонных линий SEC-2004

6.9 Классификация поисковых работ по выявлению закладных устройств

Поисковые работы по выявлению закладных устройств делятся на работы по обнаружению закладок в телефонных линиях (подраздел 6.8, см выше) и работы по обнаружению радиозакладок (работающих и неработающих радиомикрофонов и микропередатчиков, сожженных радиомикрофов, тайно установленных диктофонов, усилителей, микрофонов с усилителями и т.п.). Последние можно классифицировать по критерию применяемых для проведения этих работ методов. Наиболее используемыми являются метод нелинейной локации (НЛ) (подраздел 6.10, см ниже) и метод сканирования (подраздел 6.11, см ниже)

6.10 Метод нелинейной локации

НЛ решает проблемы обнаружения дистанционно-управляемых и включающихся по голосовому сигналу радиомикрофонов, которые излучают сигнал только во время съема информации; а также обнаружения скрытно установленных записывающих устройств – обычно специальная техника для их обнаружения имеет очень небольшой радиус действия и эффективна для обнаружения только активной техники. В целом же, НЛ может быть использован для обнаружения активных и неиспользуемых, работающих и неработающих радиомикрофонов и телефонных микропередатчиков, сожженных радиомикрофов, тайно установленных диктофонов, усилителей, микрофонов с усилителями и т.п.

Принцип действия НЛ основан на физическом свойстве всех нелинейных компонентов (транзисторов, диодов и проч.) радиоэлектронных устройств излучать в эфир при их облучении сверхвысокочастотными сигналами, гармонические составляющие, кратные частоте облучения. НЛ облучает подозреваемую область подобным сигналом (обычно около 900 МГц), после чего различные гармонические частоты анализируются на наличие гармонического сигнала. При этом процесс преобразования не зависит от того, включен или выключен исследуемый объект, также не существенно функциональное назначение радиоэлектронного устройства. Это свойство позволяет обнаруживать радиоэлектронные устройства буквально "сквозь стены". В случае получения положительных результатов обследования окончательное решение о наличии подслушивающих устройств может быть принято после проведения физического обследования, или применения металлодетектора или рентгеновского оборудования.

Эффективность выявления радиоэлектронных устройств по признаку наличия нелинейных элементов определяется не только техническими параметрами аппаратуры, но и свойствами обследуемого объекта - перекрытия, стены, мебель и т.п. Практика применения НЛ показала, что отклики на гармониках сигнала облучения создаются не только специальными полупроводниковыми приборами, но и различными металлическими элементами конструкций, которые контактируют между собой.

Наиболее типичными структурами, создающими помехи, являются металлический каркас и арматура железобетонных зданий, металлические конструкции оконных и двер­ных коробок, арматура подвесных потолков и пр. Образующиеся нелинейные элементы выявляются НЛ аналогично "настоящим" полупроводникам

6.11 Технические средства выявления сигналов подслушивающих устройств

Сканирующие приемники – это приборы имеющие возможность принимать радиосигналы в очень широком диапазоне частот и в различных видах модуляции. Поэтому сканирующие приемники нашли широкое применение в качестве поисковых приборов для обнаружения средств радиопрослушивания. Сканирующие приемники перекрывают практически все «популярные» для подслушивающих радиопередатчиков частоты и являются незаменимым средством аудиовизуального обнаружения. Немаловажной чертой некоторых сканирующих приемников является возможность управления с компьютера, поскольку использование сканирующего приемника с различными программами радиомониторинга значительно расширяет возможности обнаружения подслушивающих устройств.

Современные сканирующие приемники широко используются для решения задач радиоразведки и радиоконтроля, а также поиска несанкционированных средств перехвата информации, использующих для передачи информации радиоканал. **Сканирующие приемники** можно разделить на две группы: переносимые сканирующие приемники и перевозимые портативные сканирующие приемники.

К переносимым относятся малогабаритные сканирующие приемники весом 150...350 г. (IC-R1, IC-R10, DJ-X1 D, AR-1500, AR-2700, AR-8000, MVT-700, MVT-7100, MVT-7200, PR-1300A, HSC-050 и т.д.). Они имеют автономные аккумуляторные источники питания и свободно умещаются во внутреннем кармане пиджака. Несмотря на малые размеры и вес, подобные приемники позволяют вести разведку и контроль в диапазоне частот от 100...500 кГц до 1300 МГц, а некоторые типы приемников - до 1900 МГц ('AR-8000') и даже - до 2060 МГц ('HSC-050'). Они обеспечивают прием с амплитудной (АМ), узкополосной (NFM) и широкополосной (WFM) частотной модуляцией. Приемники 'AR-8000' и 'HSC-050' кроме указанных типов принимают сигналы с амплитудной однополосной модуляцией (SSB) в режиме приема верхней боковой полосы (USB) и нижней боковой полосы (LSB), а также телеграфных сигналов (CW). При этом чувствительность приемников при отношении сигнал/шум равном 10 дБ (относительно 1 мкВ) составляет: при приеме сигналов с NFM модуляцией - 0,35...1 мкВ, с WFM модуляцией - 1...6 мкВ. Избирательность на уровне минус 6 дБ составляет 12...15 и 150...180 кГц соответственно. Портативные сканирующие приемники имеют от 100 до 1000 каналов памяти и обеспечивают скорость сканирования от 20 до 30 каналов за секунду при шаге перестройки от 50...500 Гц до 50...1000 кГц. Некоторые типы приемников, например AR-2700, AR-8000, IC-R10 могут управляться компьютером. Перевозимые сканирующие приемники (IC-R100, AR-3030, AR-3000A, AR-5000, IC-R72, IC-R7100, IC-R8500, IC-R9000, AX-700B, EB-100 и др.) отличаются от переносимых несколько большим весом от 1,2 до 6,8 кг, габаритами и конечно большими возможностями. Они, как правило, устанавливаются или в помещениях, или в автомашинах. Почти все перевозимые сканирующие приемники имеют возможность управления с ПЭВМ.

**Лекция 7** **Программные методы защиты информации**

7.1 Защита информации в электронных платёжных системах

Электронная платёжная система (ЭПС) [8] – это система проведения расчётов между финансовыми и бизнес-организациями (с одной стороны), и Интернет-пользователями ( с другой стороны) в процессе покупки-продажи товаров и услуг через Интернет. Именно ЭПС позволяет превратить службу по обработке заказов или электронную витрину в полноценный магазин со всеми стандартными атрибутами: выбрав товар или услугу на сайте продавца, покупатель может осуществить платёж, не отходя от компьютера. ЭПС представляет собой электронную версию традиционных платёжных систем.

В системе электронной коммерции платежи осуществляются при соблюдении следующих условий:

*А. Соблюдение конфиденциальности*. При проведения расчётов через Интернет покупатель хочет, чтобы его данные (например, номер кредитной карты) были известны только организациям, имеющим на это законное право.

*Б*. *Сохранение целостности информации*. Информация о покупке никем не может быть изменена.

*В. Аутентификация*. См п. 7.2.

*Г. Средства оплаты*. Возможность оплаты любыми доступными покупателю платёжными средствами.

*Д. Авторизация*. См п. 7.2.

*Е. Гарантии рисков продавца*. Осуществляя торговлю в Интернете, продавец подвержен множеству рисков, связанных с отказами от товара и недобросовестностью покупателя. Величина рисков должна быть связана с провайдером платёжной системы и другими организациями, включённым в торговые цепочки посредством специальных соглашений.

*Ж*. *Минимизация платы за транзакцию.* Плата за обработку транзакций заказа т оплаты товара входит, естественно, в их стоимость. Поэтому снижение цены транзакции снижает себестоимость и увеличивает себестоимость товара. Важно отметить, что цена транзакции должна быть оплачена в любом случае, даже при отказе покупателя от заказа.

7.2 Идентификация, аутентификация и авторизация

***7.2.1 Идентификация*** (от позднелат. identifico — отождествляю), признание тождественности, отождествление объектов, опознание.  **Идентификация** широко применяется в математике, технике и других науках (право и т.д.), например в алгоритмических языках используют символы-идентификаторы операций, в кассовых автоматах осуществляется **Идентификация** монет по их массе и форме и др. К основным задачам **Идентификация** относятся: распознавание образов, образование аналогий, обобщений и их классификация, анализ знаковых систем и др. **Идентификация** устанавливает соответствие распознаваемого предмета своему образу — предмету, называемому идентификатором. Идентификаторы, как правило, являются знаками взаимосоответствующих предметов; идентичные предметы считают равнозначными, то есть имеющими одинаковый смысл и значение.

*7.2.2 Аутентификация* – – процедура установления соответствия параметров, характеризующих пользователя, процесс или данные, заданным критериям. Аутентификация, как правило, применяется для проверки права доступа пользователя к тем или иным ресурсам, программам, данным. В качестве критерия соответствия обычно используется совпадение заранее введенной в систему и поступающей в процессе аутентификации информации, например, о пароле пользователя, его отпечатке пальца или структуре сетчатки глаза. В электронных платёжных системах аутентификация – это процедура, позволяющая продавцу и покупателю быть уверенными, что все стороны, участвующие в сделке, являются теми, за кого они себя выдают.

*7.2.3 Авторизация* – это процедура, в процессе которой вы вводите свое имя, например, при [регистрации](http://wiki.liveinternet.ru/ServisDnevnikovLiveInternet/Registracija?v=uld) на сайте «одноклассники»(никнейм) и пароль, который вы также указываете при [регистрации](http://wiki.liveinternet.ru/ServisDnevnikovLiveInternet/Registracija?v=uld). После авторизации сервис сайта «узнаёт вас» именно под этим именем, предоставляя вам доступ на те страницы и к тем функциям, которые доступны для введенного имени. Авторизация в локальной сети выполняет те же функции.

7.3 Обеспечение безопасности банкоматов

Что такое банкомат и каковы его функции – общеизвестно. Средства обеспечения безопасности банкоматов обеспечивают многоуровневую защиту операций – организационную, механическую, оптическую, электронную, программную – вплоть до установки системы сигнализации с видеокамерой (оптическая защита). Возможна установка видеокамеры с видеомагнитофоном, которые фиксируют все действия пользователей с банкоматом.

Программная защита банкомата обеспечивается пин-кодом карточки и программным обеспечением для его распознавания. Организационная защита заключается в размещении части банкомата, где хранятся кассеты с банкнотами, в видном месте операционного зала или другого хорошо просматриваемого места либо в изолированном помещении. Заправка кассет проводится инкассаторами либо в конце рабочего дня, когда нет клиентов, либо при удалении клиентов из операционного зала. Для защиты от вандализма применяются специальные кабины, например, фирмы DIEBOLD. Кабина, в которой устанавливается один или несколько банкоматов, запираются с помощью электронных замков. Замки пропускают в кабину только владельцев карточек и защищаются системой сигнализации.

Механическая защита обеспечивается хранением кассет с банкнотами в сейфах различных конструкций (UL 291, RAL-RG 626/3, C1/C2). Они различаются габаритами, толщиной стенок, весом. Запираются сейфы различными замками с ключами, с одинарным или двойным цифровым ключом, с электронным ключом (электронная защита).

Для предотвращения взлома банкомата применяются датчики различного назначения с системой сигнализации. Тепловые датчики, например, выявляют попытки плазменной резки металла. Сейсмические датчики выявляют попытки увоза банкомата (электронная защита).

7.4 Обеспечение безопасности электронных платежей через сеть Интернет

ЭПС делятся на дебетовые и кредитные. Дебетовые ЭПС работают с электронными чеками и цифровой наличностью. Чеки (электронные деньги, например, деньги на счетах в банке), выпускает эмитент, управляющий ЭПС-мой. Используя выпущенные чеки, пользователи производят и принимают платежи в Интернет. Чек (аналог бумажного чека) – это электронное предписание клиента своему банку о перечислении денег. Внизу электронного чека – электронная цифровая подпись (ЭЦП). Защита информации в дебетовых ЭПС осуществляется именно с помощью ЭЦП, в которой используется система шифрования с открытым ключом.

Кредитные ЭПС используют кредитные карты, работа с которыми аналогична работе с картами в других системах. Отличие – все транзакции в кредитных ЭПС проводятся через Интернет. Поэтому в кредитных ЭПС также есть возможность перехвата в сети реквизитов карты злоумышленником. Защиту информации в кредитных ЭПС проводят защищёнными протоколами транзакций (например, протокол SSL (Secure Sockets Layer)), а также стандартом SET (Secure Electronic Transaction), призванным со временем заменить SSL при обработке транзакций, связанных с расчётами за покупки по кредитным картам через Интернет.

7.5 Программное обеспечение для защиты информации, хранящейся на персональных компьютерах

Большинство компьютеров в настоящее время подключено к Интернету. Кроме полезной информации в компьютер из Интернета может проникать и вредная информация. И если спам только засоряет компьютер, то Интернет может быть источником вирусов, хакерских атак на компьютер и другого вредоносного ПО. Для защиты информации, хранящейся на персональных компьютерах, от вредоносного ПО, служат различные антивирусные программы (АП), файрволлы, антихакеры, антитрояны. Основными из них являются АП и файрволлы. АП подробно рассмотрены в подразделе 7.8.

Файрволл (firewall), он же брандмауэр или сетевой экран - это программа, которая обеспечивает фильтрацию сетевых пакетов на различных уровнях, в соответствии с заданными правилами. Основная задача файрволла - это защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Сетевой экран не пропускает пакеты, которые не подходят по критериям, определённым в конфигурации, т.е. задерживает вредоносное ПО от проникновения в компьютер. В Минске находится филиал, насчитывающий примерно 70 программистов (20% общей численности) известного разработчика брандмауэров – фирмы Check Point.

7.6 Методы организации разграничения доступа

Основными функциями системы разграничения доступа (СРД) являются:

— реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

— реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

— изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

— управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

— реализация правил обмена данными между субъектами для автоматизированных систем (АС) и средств вычислительной техники, построенных по сетевым принципам.

Функционирование СРД опирается на выбранный способ разграничения доступа. Наиболее прямой способ гарантировать защиту данных — это предоставить каждому пользователю вычислительную систему как его собственную. В многопользовательской системе похожих результатов можно добиться использованием модели виртуальной ЭВМ.

При этом каждый пользователь имеет собственную копию операционной системы. Монитор виртуального персонального компьютера для каждой копии операционной системы будет создавать иллюзию, что никаких других копий нет и что объекты, к которым пользователь имеет доступ, являются только его объектами. Однако при разделении пользователей неэффективно используются ресурсы автоматизированной системы (АС).

В АС, допускающих совместное использование объектов доступа, существует проблема распределения полномочий субъектов по отношению к объектам. Наиболее полной моделью распределения полномочий является матрица доступа. Матрица доступа является абстрактной моделью для описания системы предоставления полномочий.

Строки матрицы соответствуют субъектам, а столбцы — объектам; элементы матрицы характеризуют право доступа (читать, добавлять информацию, изменять информацию, выполнять программу и т.д.). Чтобы изменять права доступа, модель может, например, содержать специальные права владения и управления. Если субъект владеет объектом, он имеет право изменять права доступа других субъектов к этому объекту. Если некоторый субъект управляет другим субъектом, он может удалить права доступа этого субъекта или передать свои права доступа этому субъекту. Для того чтобы реализовать функцию управления, субъекты в матрице доступа должны быть также определены в качестве объектов.

Элементы матрицы установления полномочий (матрицы доступа) могут содержать указатели на специальные процедуры, которые должны выполняться при каждой попытке доступа данного субъекта к объекту и принимать решение о возможности доступа. Основами таких процедур могут служить следующие правила:

— решение о доступе основывается на истории доступов других объектов;

— решение о доступе основывается на динамике состояния системы (права доступа субъекта зависят от текущих прав других субъектов);

— решение о доступе основывается на значении определенных внутрисистемных переменных, например значений времени и т.п.

В наиболее важных АС целесообразно использование процедур, в которых решение принимается на основе значений внутрисистемных переменных (время доступа, номера терминалов и т.д.), так как эти процедуры сужают права доступа.

Матрицы доступа реализуются обычно двумя основными методами — либо в виде списков доступа, либо мандатных списков. Список доступа приписывается каждому объекту, и он идентичен столбцу матрицы доступа, соответствующей этому объекту. Списки доступа часто размещаются в словарях файлов. Мандатный список приписывается каждому субъекту, и он равносилен строке матрицы доступа, соответствующей этому субъекту. Когда субъект имеет права доступа по отношению к объекту, то пара (объект — права доступа) называется мандатом объекта.

На практике списки доступа используются при создании новых объектов и определении порядка их использования или изменении прав доступа к объектам. С другой стороны, мандатные списки объединяют все права доступа субъекта. Когда, например, выполняется программа, операционная система должна быть способна эффективно выявлять полномочия программы. В этом случае списки возможностей более удобны для реализации механизма предоставления полномочий.

Некоторые операционные системы поддерживают как списки доступа, так и мандатные списки. В начале работы, когда пользователь входит в сеть или начинает выполнение программы, используются только списки доступа. Когда субъект пытается получить доступ к объекту в первый раз, список доступа анализируется и проверяются права субъекта на доступ к объекту. Если права есть, то они приписываются в мандатный список субъекта и права доступа проверяются в дальнейшем проверкой этого списка.

При использовании обоих видов списков список доступа часто размещается в словаре файлов, а мандатный список — в оперативной памяти, когда субъект активен. С целью повышения эффективности в техническом обеспечении может использоваться регистр мандатов.

Третий метод реализации матрицы доступа — так называемый механизм замков и ключей. Каждому субъекту приписывается пара (А, К), где А— определенный тип доступа, а К— достаточно длинная последовательность символов, называемая замком. Каждому субъекту также предписывается последовательность символов, называемая ключом. Если субъект захочет получить доступ типа А к некоторому объекту, то необходимо проверить, что субъект владеет ключом к паре (А, К), приписываемой конкретному объекту.

К недостаткам применения матриц доступа со всеми субъектами и объектами доступа можно отнести большую размерность матриц. Для уменьшения размерности матриц установления полномочий применяют различные методы сжатия:

— установление групп пользователей, каждая из которых представляет собой группу пользователей с идентичными полномочиями;

— распределение терминалов по классам полномочий;

— группировка элементов защищаемых данных в некоторое число категорий с точки зрения безопасности информации (например, по уровням конфиденциальности).

По характеру управления доступом системы разграничения разделяют на дискреционные и мандатные.

Дискреционное управление доступом дает возможность контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам и т.п.). Например, владельцам объектов предоставляется право ограничивать доступ к этому объекту других пользователей. При таком управлении доступом для каждой пары (субъект—объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта к данному объекту. Однако имеются и другие задачи управления доступом, которые не могут быть решены только дискреционным управлением. Одна из таких задач — позволить администратору АС контролировать формирование владельцами объектов списков управления доступом.

Мандатное управление доступом позволяет разделить информацию на некоторые классы и управлять потоками информации при пересечениях границ этих классов.

Во многих системах реализуется как мандатное, так и дискреционное управление доступом. При этом дискреционные правила разграничения доступа являются дополнением мандатных. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

Обеспечивающие средства для системы разграничения доступа выполняют следующие функции:

— идентификацию и опознавание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

— регистрацию действий субъекта и его процесса;

— предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

— реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление системы защиты после НСД;

— тестирование всех функций защиты информации специальными программными средствами;

— очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными путем двукратной произвольной записи;

— учет выходных печатных и графических форм и твердых копий в АС;

— контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Для каждого события должна регистрироваться следующая информация, дата и время; субъект, осуществляющий регистрируемое действие; тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа); успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выдача печатных документов должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе общего количества листов (страниц). Вместе с выдачей документа может автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа.

Автоматическому учету подлежат создаваемые защищаемые файлы, каталоги, тома, области оперативной памяти персонального компьютера, выделяемые для обработки защищаемых файлов, внешних устройств и каналов связи.

Такие средства, как защищаемые носители информации, должны учитываться документально, с использованием журналов или картотек, с регистрацией выдачи носителей. Кроме того, может проводиться несколько дублирующих видов учета.

Реакция на попытки несанкционированного доступа (НСД) может иметь несколько вариантов действий:

— исключение субъекта НСД из работы АС при первой попытке нарушения ПРД или после превышения определенного числа разрешенных ошибок;

— работа субъекта НСД прекращается, а информация о несанкционированном действии поступает администратору АС и подключает к работе специальную программу работы с нарушителем, которая имитирует работу АС и позволяет администрации сети локализовать место попытки НСД.

Реализация системы разграничения доступа может осуществляться как программными, так и аппаратными методами или их сочетанием. В последнее время аппаратные методы защиты информации от НСД интенсивно развиваются благодаря тому, что: во-первых, интенсивно развивается элементная база, во-вторых, стоимость аппаратных средств постоянно снижается и, наконец, в-третьих, аппаратная реализация защиты эффективнее по быстродействию, чем программная.

7.7 Контроль целостности информации

Целостность информации – это отсутствие признаков её уничтожения или искажения. Целостность информации означает, что данные полны. Целостность – это условие того, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление К задаче контроля целостности необходимо подходить с двух позиций. Во-первых, необходимо дать ответ на вопрос, с какой целью реализуется контроль целостности. Дело в том, что при корректном реализации разграничительной политики доступа к ресурсам их целостность не может быть несанкционированно нарушена. Отсюда напрашивается вывод, что целостность ресурсов следует контролировать в том случае, когда невозможно осуществить корректное разграничение доступа (например, запуск приложения с внешнего накопителя – для внешних накопителей замкнутость программной среды уже не реализовать), либо в предположении, что разграничительная политика может быть преодолена злоумышленником. Это вполне резонное предположение, т.к. СЗИ от НСД, обеспечивающую 100% защиту, построить невозможно даже теоретически. Во-вторых, необходимо понимать, что контроль целостности – это весьма ресурсоемкий механизм, поэтому на практике допустим контроль (а тем более с высокой интенсивностью, в противном случае, данный контроль не имеет смысла) лишь весьма ограниченных по объему объектов [10].

Принципиальная особенность защиты информации на прикладном уровне состоит в том, что реализация какой-либо разграничительной политики доступа к ресурсам (основная задача СЗИ от НСД) на этом уровне не допустима (потенциально легко преодолевается злоумышленником). На этом уровне могут решаться только задачи контроля, основанные на реализации функций сравнения с эталоном. При этом априори предполагается, что с эталоном могут сравниваться уже произошедшие события. Т.е. задача защиты на прикладном уровне состоит не в предотвращении несанкционированного события, а в выявлении и в фиксировании факта того, что несанкционированное событие произошло.

Рассмотрим достоинства и недостатки защиты на прикладном уровне, по сравнению с защитой на системном уровне. Основной недостаток состоит в том, что на прикладном уровне в общем случае невозможно предотвратить несанкционированное событие, т.к. контролируется сам факт того, что событие произошло, поэтому на подобное событие лишь можно отреагировать (максимально оперативно), с целью минимизаций его последствий.

Основное достоинство состоит в том, что факт того, что произошло несанкционированное событие, может быть зарегистрирован практически всегда, вне зависимости от того, с какими причинами связано его возникновение (так как регистрируется сам факт подобного события). Проиллюстрируем сказанное простым примером. Один из основных механизмов защиты в составе СЗИ от НСД является механизм обеспечения замкнутости программной среды (суть – не дать запускать любые сторонние процессы и приложения, вне зависимости от способа их внедрения на компьютер). Данная задача должна решаться на системном уровне. При решении задачи на системном уровне, драйвер средства защиты перехватывает все запросы на запуск исполняемого файла и анализирует их, обеспечивая возможность запуска лишь разрешенных процессов и приложений. При решении же аналогичной задачи на прикладном уровне осуществляется анализ того, какие процессы и приложения запущены, и если выявляется, что запущен несанкционированный процесс (приложение), он завершается средством защиты (реакция СЗИ от НСД на несанкционированное событие). Как видим, преимуществом реализации на системном уровне является то, что при этом должен в принципе предотвращаться запуск несанкционированных процессов (приложений), при реализации же на прикладном уровне, событие фиксируется по факту совершения, т.е. в данном случае – уже после того, как процесс запущен, как следствие, до момента его завершения средством защиты (если установлена такая реакция на такое событие), данным процессом может быть выполнено какое-либо несанкционированное действие (по крайней мере, его часть, почему важнейшим условием здесь и становится оперативное реагирование на обнаруженное событие). С другой стороны, а кто может гарантировать, что системный драйвер, решает данную задачу защиты корректно и в полном объеме, а потенциальная опасность, связанная с ошибками и закладками в системном и прикладном ПО и т.д.? Другими словами, никогда нельзя гарантировать, что системный драйвер не может быть обойден злоумышленником при определенных условиях. Что мы получим в первом случае – администратор даже не узнает о том, что совершен факт НСД. При реализации же решения задачи на прикладном уровне, уже не важна причина, приведшая к возникновению несанкционированного события, так как фиксируется сам факт проявления данного события (даже, если оно вызвано использованием ошибок и закладок ПО). В этом случае, мы зарегистрируем, что событие произошло, однако, не сумеем его предотвратить в полном объеме, лишь можем попытаться минимизировать последствия.

С учетом сказанного можем сделать следующий важный вывод. Механизмы защиты, призванные решать одну и ту же задачу на системном и на прикладном уровнях, ни в коем случае нельзя рассматривать в качестве альтернативных решений. Эти решения дополняют друг друга, так как предоставляют совершенно различные свойства защиты. Следовательно, при реализации эффективной защиты (в первую очередь, речь идет о корпоративных приложениях) наиболее критичные задачи должны решаться одновременно обоими способами: и на системном, и на прикладном уровнях.

7.8 Методы защиты от компьютерных вирусов

Точного термина, определяющего вирусную (вредоносную) программу (ВП, «компьютерный вирус») в науке до сих пор не существует. Впервые этот термин употребил сотрудник Лехайского университета (США) доктор Fred Cohen (Фрэд Коэн) в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Определение, которое дал вирусу доктор Фрэд Коэн, звучало так – «Компьютерный вирус – это последовательность символов на ленте машины Тьюринга: «программа, которая способна инфицировать другие программы, изменяя их, чтобы внедрить в них максимально идентичную копию себя». Термин «компьютерный вирус» в западной литературе звучит как: «Самокопирующаяся программа, которая может «инфицировать» другие программы, изменяя их или их окружение так, что запрос к «инфицированной» программе подразумевает запрос к максимально идентичной, а в большинстве случаев - функционально подобной, копии «вируса».

Информация о первой ВП также отсутствует. Известно только, что в конце 60х — начале 70х годов 20-го столетия на машине Univac 1108 была создана очень популярная игра «ANIMAL», которая создавала свои копии в системных библиотеках. Об угрозах компьютерной безопасности за счёт вирусов мы уже беседовали на первом практическом занятии. Для парирования этих угроз существуют специальные антивирусные программы (АВ). Разработан специальный стандарт – СТБ П 34.101.8 «Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования». Согласно СТБ П 34.101.8 ВП – это программный код (исполняемый или интерпретируемый), обладающий свойством несанкционированного воздействия на «объект информационной технологии».

Виды вирусов. А. Троянская программа (trojan) – ВП, которая не способна создавать свои копии и не способна распространять свое тело в «объектах информационной технологии». Б. Дроппер (dropper) – ВП, которая не способна создавать свои копии, но внедряет в «объект информационной технологии» другую «вредоносную программу», бестелесые черви и др. (см. в презентации). Классификацию компьютерных вирусов **по среде обитания** см. в презентации.

Наиболее широко в Минске распространены следующие антивирусные программы (АВ) – Антивирус Касперского,например, Kaspersky Internet Security до версии 11, антивирус Bit Defender Internet Security, Panda Internet Security, Avast! Free Antivirus 5.0 Final, Avira AntiVir Personal Edition 10.0.0, антивирус Dr Web 6.0, АП ООО «Вирус БлокАда». Однако современные АП имеют целый ряд проблем, которые делятся на идеологические и технические.

Идеологические проблемы связаны, во-первых, с увеличением объема работ по анализу кода вируса из-за расширения понятия ВП, а во-вторых, со сложностью классификации ПО, которая зависит либо от конфигурации ПО либо от способа установки ПО. Принятие решения по устранению проблем с вирусами перекладывается в этом случае на пользователя.

Технические проблемы заключаются в постоянном появлении новых сложных ВП, а также в задержке детектирования ВП. Появление сложных ВП вызывает усложнение алгоритмов обнаружения и обезвреживания вирусов. Это, в свою очередь, приводит к перераспределению ресурсов компьютера: увеличение на АВ защиту, уменьшение на прикладные задачи. Разрулирование этой проблемы проводится обновлением парка компьютеров, а также оптимизацией алгоритмов АВ. Для реализации последнего мероприятия необходима реализация эмулятора процессора на языке ассемблера, а также использование динамического транслятора.

Для устранения задержки детектирования ВП изобретена технология MalwareScope, позволяющая детектировать неизвестных представителей известных семейств ВП без обновления антивирусных баз. Можно использовать также эвристический анализ, выявляющий наличие ошибок “false positive” и “false negative”. Метод этот, однако, характеризуется высокой трудоемкостью выявления типовых для семейства ВП фрагментов кода вируса. Для снижения трудоемкости разработан программный робот, автоматизирующий процесс корректировки эвристических записей. Кроме эвристического анализа ошибок можно использовать также поведенческие анализаторы/блокираторы, которые применимы однако только для защиты объекта, на котором установлены.

**Лекция 8 Защита объектов от несанкционированного доступа**

8.1 Интегральные системы безопасности

Под **интегральной безопасностью** понимается такое состояние условий функционирования человека, объектов и технических средств, при котором они надежно защищены от всех возможных видов угроз в ходе непрерывного процесса подготовки, хранения, передачи и обработки информации. Интегральная безопасность информационных систем включает в себя следующие составляющие:

— физическая безопасность (защита зданий, помещений, подвижных средств, людей, а также аппаратных средств — компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);

— безопасность связи (защита каналов связи от внешних воздействий любого рода);

— безопасность программного обеспечения (защита от вирусов, логических бомб, несанкционированного изменения конфигурации);

— безопасность данных (обеспечение конфиденциальности, целостности и доступности данных).

Интегральный подход основан на объединении различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности, как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т.п.).

Современный комплекс защиты территории охраняемых объектов должен включать в себя следующие основные компоненты:

— механическую систему защиты;

— систему оповещения о попытках вторжения;

— оптическую (обычно телевизионную) систему опознавания нарушителей;

— оборонительную систему (звуковую и световую сигнализацию, применение в случае необходимости оружия);

— связную инфраструктуру;

— центральный пост охраны, осуществляющий сбор, анализ, регистрацию и отображение поступающих данных, а также управление периферийными устройствами;

— персонал охраны (патрули, дежурные на центральном посту).

Состав и структура перечисленных основных компонентов комплекса защиты территории охраняемых объектов, именуемого также интегральным комплексом физической защиты охраняемых объектов, показан на рис. 8.1. На этом рисунке представлена блок-схема комплекса, обеспечивающего функционирование всех рассмотренных выше систем. Отличительной особенностью подобных комплексов является интеграция различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Необходимо отметить, что в рассматриваемой блок-схеме технические средства скомпонованы по системам достаточно условно для того, чтобы схема приобрела более логичную форму и была бы более понятна. На самом деле одни и те же средства выполняют различные функции для разных систем обеспечения безопасности

|  |
| --- |
| graphics  Рис. 8.1 – Структурная схема интегральной системы безопасности объекта |

Краткому описанию систем оповещения о попытках вторжения и систем опознавания нарушителей, а также связной инфраструктуры, посвящены пп. 8.4, 8.5, 8.7 настоящей лекции. Остальные компоненты комплекса защиты территории охраняемых объектов описаны ниже.

*8.1.1. Механические системы защиты.* Основой любой механической системы зашиты являются механические или строительные элементы, создающие для лица, пытающегося проникнуть на охраняемую территорию, реальное физическое препятствие. Важнейшей характеристикой механической системы защиты является время сопротивления, то есть время, которое требуется злоумышленнику для ее преодоления. Исходя из требуемой величины названной характеристики должен производиться и выбор типа механической системы защиты. Как правило, механическими или строительными элементами служат стены и ограды. Если позволяют условия, могут применяться рвы и ограждения из колючей проволоки.

При использовании многорядных механических систем защиты датчики оповещения о попытке вторжения целесообразно располагать между внутренним и внешним ограждением. При этом внутреннее ограждение должно обладать повышенным временем сопротивления.

*8.1.2 Оборонительные системы*. Для предотвращения развития вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные или звуковые установки. В обоих случаях субъект, пытающийся проникнуть на охраняемую территорию, информируется о том, что он обнаружен охраной. Таким образом, на него оказывается целенаправленное психологическое воздействие. Кроме того, использование осветительных установок обеспечивает благоприятные условия для действий охраны.

Для задержания преступника охрана предпринимает соответствующие оперативные меры или вызывает милицию (полицию). Если злоумышленнику удалось скрыться, то для успеха последующего расследования важное значение приобретает информация, которая может быть получена с помощью рассмотренной выше системы опознавания. В особых случаях функции оборонительной системы выполняет специальное ограждение, через которое пропущен ток высокого напряжения.

*8.1.3 Центральный пост и персонал охраны*. Сложные комплексы защиты охраняемых территорий, состоящие, как правило, из нескольких систем, могут эффективно функционировать только при условии, что работа всех технических установок постоянно контролируется и управляется с центрального поста охраны. Учитывая повышенную психологическую нагрузку на дежурных охранников центрального поста, необходимость оперативной выработки и реализации оптимальных решений в случае тревоги, к центральным устройствам комплексов защиты предъявляются особые требования. Так, они должны обеспечивать автоматическую регистрацию и отображение всех поступающих в центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур. Важную роль играет и уровень эргономики аппаратуры, которой оснащаются рабочие места дежурных охранников.

8.2 Системы контроля доступа

**Системы контроля доступа (СКД)** — это эффективное средство от несанкционированного проникновения посторонних лиц на территорию предприятия, а также разграничения доступа сотрудников в его внутренние помещения. Обычно **СКД** является одним из элементов интегрированной системы безопасности, наряду с системой видеонаблюдения и охранно-пожарной сигнализацией. Особенностями современных СКД являются:

* работа в автономном режиме без постоянной связи с компьютером;
* энергонезависимое хранение списков доступа и списков событий в контроллерах;
* разграничение прав доступа по помещениям, по времени, по статусу карты;
* поддержка недельных и сменных графиков доступа;
* защита от передачи карты (Antipassback);
* постановка помещений на системную охрану.

Данные, получаемые от систем контроля доступа, могут быть в дальнейшем использованы в системах повышения эффективности для обеспечения трудовой дисциплины и с целью автоматизировать [учет рабочего времени](http://www.perco.ru/products/sistemy-povyshenija-ehffektivnosti/uchet-rabochego-vremeni/).

На рис. 8.1 показана часть технических средств СКД. В качестве исполнительных устройств в СКД используются [**электромеханические турникеты**](http://www.perco.ru/products/turnstiles/)**,** калитки, электромеханические и электромагнитные замки.

8.3 Идентификация и аутентификация

Определения и пояснения к понятиям **Идентификация** и **Аутентификация** рассмотрены в подразделе 7.2. Применительно к СКД идентификация означает опознание лица, которому разрешён доступ на объект («своего»). Все злоумышленники («чужие») с помощью СКД не должны быть допущены на объект. Аутентификация применительно к СКД используется для проверки права доступа на объект.

8.4 Системы и средства наблюдения

Наиболее широкое распространение в системах оповещения получили телевизионные установки дистанционного наблюдения. Несомненно, что объект со стационарными постами охраны обладает более высокой защищенностью, однако при этом значительно возрастают затраты на его охрану. Так, при необходимости круглосуточного наблюдения требуется трехсменная работа персонала охраны. В этих условиях телевизионная техника становится средством повышения эффективности работы персонала охраны, прежде всего при организации наблюдения в удаленных, опасных или труднодоступных зонах.

Вся контролируемая системой оповещения зона разграничивается на отдельные участки протяженностью не более 100 м, на которых устанавливается, по крайней мере, одна передающая телекамера. При срабатывании датчиков системы оповещения, установленных на определенном участке контролируемой зоны, изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны. Кроме того, при необходимости должно быть обеспечено дополнительное освещение данного участка. Немаловажно, чтобы внимание дежурного охранника было быстрее привлечено к выведенному на экран монитора изображению.

В ряде телесистем наблюдения применены передающие камеры, ориентация которых может дистанционно меняться дежурным охранником. При включении сигнализации тревоги служащий охраны должен ориентировать телекамеру на участок, где сработали датчики системы оповещения. Практический опыт показывает, однако что такие телеустановки менее эффективны по сравнению с жестко ориентированными передающими телекамерами.

Отличительной особенностью некоторых объектов является их большая протяженность. Большое количество площадок таких объектов может быть расположено на значительном удалении друг от друга, что серьезно удорожает монтаж и эксплуатацию оборудования. В этих случаях можно применить систему малокадрового телевидения типа Slowscan. Она функционирует на больших дальностях, имеет невысокую стоимость и совместима с любой существующей замкнутой телевизионной системой, которая уже установлена на объекте. Для передачи видеокадров и команд в этой системе используется телефонная сеть общего пользования.

Особые преимущества в системах охраны имеют камеры на приборах с зарядовой связью (ПЗС). По сравнению с обычными трубочными камерами они обладают меньшими габаритами, более высокой надежностью, практически не нуждаются в техническом обслуживании, отлично работают в условиях низкой освещенности, обладают чувствительностью в инфракрасной области спектра. Однако, наиболее важным является то, что видеоинформация на чувствительном элементе указанной камеры сразу представлена в цифровой форме и без дополнительных преобразований пригодна для дальнейшей обработки. Это дает возможность легко идентифицировать различия или изменения элементов изображения, реализовать в камере встроенный датчик перемещений. Подобная камера со встроенным детектором и маломощным ИК-осветителем может вести наблюдение охраняемой территории и при появлении нарушителя в поле зрения распознавать изменения элементов изображения и подавать сигнал тревоги.

8.5 Система оповещения и опознавания

*8.5.1. В современных системах* *оповещения* (системах тревожной сигнализации) о попытках вторжения на охраняемую территорию находят применение датчики нескольких типов.

В системах защиты периметра территории без ограды используются микроволновые, инфракрасные, емкостные, электрические и магнитные датчики.

С помощью датчиков первых двух типов формируется протяженная контрольная зона барьерного типа. Действие систем с микроволновыми датчиками основывается на контроле интенсивности высокочастотного направленного излучения передатчика, которое воспринимается приемником. Срабатывание сигнализации происходит при прерывании этого направленного излучения. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, воздействием растительности, атмосферных осадков, передвижением транспортных средств, а также воздействием посторонних передатчиков.

При использовании инфракрасных систем оповещения между передатчиком и приемником появляется монохроматическое световое излучение в невидимой области спектра. Срабатывание сигнализации происходит при прерывании одного или нескольких световых лучей. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, сильным туманом или снегопадом.

Принцип действия емкостной системы оповещения основывается на формировании электростатического поля между параллельно расположенными, так называемыми, передающими и воспринимающими проволочными элементами специального ограждения. Срабатывание сигнализации происходит при регистрации определенного изменения электростатического поля, имеющего место при приближении человека к элементам ограждения. Ложные срабатывания могут быть обусловлены перемещением животных, воздействием растительности, обледенением элементов ограждения, атмосферными воздействиями или загрязнением изоляторов.

Электрические системы оповещения базируются на использовании специального ограждения с токопроводящими проволочными элементами. Критерием срабатывания сигнализации является регистрация изменений электрического сопротивления токопроводящих элементов при прикосновении к ним. Ложные срабатывания могут быть вызваны животными, растительностью или загрязнением изоляторов.

Принцип действия систем с магнитными датчиками предполагает контроль параметров магнитного поля. Срабатывание сигнализации происходит при регистрации искажений, которые обусловлены появлением в зоне действия датчиков предметов из ферромагнитного материала. Ложное срабатывание может иметь место из-за изменений характеристик почвы, обусловленных, например, продолжительным дождем.

При наличии механической системы защиты территории (например, ограды, расположенной по периметру) находят применение системы оповещения с вибрационными датчиками, датчиками звука, распространяющегося по твердым телам, акустическими датчиками, электрическими переключателями, а также системы с электрическими проволочными петлями.

Вибрационные датчики закрепляются непосредственно на элементах ограды. Срабатывание сигнализации происходит при появлении на выходе датчиков сигналов, которые обусловлены вибрациями элементов ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем или градом.

Датчики звука также устанавливаются непосредственно на элементы ограды и контролируют распространение по ним звуковых колебаний. Срабатывание сигнализации происходит при регистрации так называемых шумов прикосновения к элементам ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом или срывающимися с элементов ограды сосульками.

В системах оповещения с акустическими датчиками контролируются звуковые колебания, передаваемые через воздушную среду. Срабатывание сигнализации происходит при регистрации акустических сигналов, имеющих место при попытках перерезать проволочные элементы ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом, а также различными посторонними шумами.

Действие систем с электрическими переключателями основано на регистрации изменения состояния переключателей, вмонтированных в ограду, которое происходит при соответствующем изменении натяжения проволочных элементов или нагрузки на направляющие трубки ограды. Ложные срабатывания сигнализации могут быть вызваны очень сильным ветром при недостаточном натяжении элементов ограды.

Если в системах оповещения в качестве чувствительных элементов применяются изолированные токопроводящие проволочные элементы, срабатывание сигнализации происходит при перерезании или деформации этих элементов. Ложные срабатывания могут произойти при возникновении неисправности в сети электропитания.

Для контроля участков почвы по периметру охраняемой территории находят применение системы оповещения с датчиками звука, распространяющегося по твердым телам, а также с датчиками давления.

В системах первого типа регистрируются звуковые, сейсмические колебания. Срабатывание сигнализации происходит при регистрации сотрясений почвы, например, ударного шума. Ложные срабатывания могут быть обусловлены перемещением достаточно крупных животных, движением транспорта вблизи охраняемой территории.

В системах второго типа используются пневматические или емкостные датчики давления, позволяющие регистрировать изменения нагрузки на почву. Срабатывание сигнализации происходит при регистрации соответствующего роста давления, например, ударного. Ложные срабатывания возможны из-за перемещений достаточно крупных животных, разгерметизации пневматических датчиков или коррозии.

Повышение вероятности обнаружения нарушителя системой оповещения обязательно сопровождается увеличением числа ложных срабатываний. Таким образом, разработка систем оповещения связана, прежде всего, с поиском рационального компромисса относительно соотношения величин названных показателей. Из этого следует, что дальнейшее совершенствование систем оповещения должно обеспечить прежде всего повышение вероятности обнаружения и снижение интенсивности ложных срабатываний путем использования нескольких систем оповещения различного принципа действия в едином комплексе и применения в этих системах микропроцессорных анализаторов.

*8.5.2. Системы опознавания.* Современный комплекс защиты территории охраняемых объектов обязательно включает в свой состав оптическую (обычно телевизионную) систему опознавания нарушителей. Эта телевизионная система обычно совмещена с телевизионной системой наблюдения (см. п. 8.4). Обязательным условием надежного функционирования всего комплекса защиты охраняемой территории является последующий анализ поступающих сообщений о проникновении для точного определения их вида и причин появления. Названное условие может быть выполнено посредством использования систем опознавания. При этом сбор первичной информации о проникновении на охраняемую территорию злоумышленника может быть проведен с помощью систем оповещения различного типа (см. п. 8.8.1) или систем наблюдения (см. п. 8.4). Анализ поступающих сообщений о проникновении проводится дежурным охранником.

8.6 Сигнализация

Сигнализация различных типов также помогает дежурному охраннику получать точную информацию о проникновении нарушителя на охраняемую территорию. Срабатывание сигнализации происходит при срабатывании систем оповещения различных видов (см. п. 8.5.1) о проникновении нарушителя Фактические причины срабатывания сигнализации во многих случаях могут быть идентифицированы только при условии достаточно высокой оперативности дежурного охранника. Важно, что данное положение, прежде всего, имеет место при действительных попытках вторжения на охраняемую территорию и при преднамеренных обманных действиях злоумышленников. Одним из перспективных путей выполнения выше сформулированного условия является применение устройства видеопамяти, которое обеспечивает автоматическую запись изображения сразу же после срабатывания сигнализации. При этом дежурному охраннику предоставляется возможность вывести из устройства памяти на экран монитора первые кадры изображения и идентифицировать причину срабатывания датчиков системы оповещения.

8.7 Связная инфраструктура

Современный рынок технических средств предоставляет разработчикам широкие возможности выбора аппаратуры и каналов связи. Однако, с учетом интегрального подхода, в качестве связной инфраструктуры целесообразно использовать структурированные кабельные системы (СКС). СКС – это физическая основа информационной инфраструктуры предприятия, позволяющая свести в единую систему множество информационных сервисов разного назначения: локальные вычислительные и телефонные сети, системы безопасности, [видеонаблюдения](http://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B4%D0%B5%D0%BE%D0%BD%D0%B0%D0%B1%D0%BB%D1%8E%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5) и т. д. СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. Она состоит из набора медных и [оптических кабелей](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C), кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Кабельная система — это [система](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), элементами которой являются кабели и компоненты, которые связаны с кабелем. К кабельным компонентам относится все пассивное коммутационное оборудование, служащее для соединения или физического окончания (терминирования) кабеля — телекоммуникационные розетки на рабочих местах, кроссовые и [коммутационные панели](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%B0%D0%BD%D0%B5%D0%BB%D1%8C) (жаргон: «патч-панели») в телекоммуникационных помещениях, муфты и сплайсы;

Структурированная. Структура — это любой набор или комбинация связанных и зависимых составляющих частей. Термин «структурированная» означает, с одной стороны, способность системы поддерживать различные телекоммуникационные приложения (передачу речи, данных и видеоизображений), с другой — возможность применения различных компонентов и продукции различных производителей, и с третьей — способность к реализации так называемой мультимедийной среды, в которой используются несколько типов передающих сред — [коаксиальный кабель](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B0%D0%BA%D1%81%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C), [UTP](http://ru.wikipedia.org/wiki/UTP), [STP](http://ru.wikipedia.org/w/index.php?title=Screened_Fully_Shielded_Twisted_Pair&action=edit&redlink=1) и [оптическое волокно](http://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BD%D0%BE). Структуру кабельной системы определяет инфраструктура информационных технологий, IT (Information Technology), именно она диктует содержание конкретного проекта кабельной системы в соответствии с требованиями конечного пользователя, независимо от активного оборудования, которое может применяться впоследствии.

8.8 Противодействие техническим средствам разведки

Противодействие техническим средствам разведки (ТСР) представляет собой совокупность согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания охраняемых сведений с помощью технических средств.

Добывание информации предполагает наличие информационных потоков от физических носителей охраняемых сведений к системе управления. При использовании TCP такие информационные потоки образуются за счет перехвата и анализа сигналов и полей различной физической природы. Источниками информации для технической разведки являются содержащие охраняемые сведения объекты. Это позволяет непосредственно влиять на качество добываемой злоумышленником информации и в целом на эффективность его деятельности путем скрытия истинного положения и навязывания ложного представления об охраняемых сведениях.

Искажение или снижение качества получаемой информации непосредственно влияет на принимаемые злоумышленником решения и, через его систему управления, на способы и приемы исполнения решения. Непосредственный контакт принципиально необходим на этапах добывания информации и исполнения решения, причем добывание информации должно предшествовать принятию решения и его исполнению злоумышленником. Поэтому противодействие ТСР должно носить упреждающий характер и реализовываться заблаговременно.

Любая система технической разведки (рис. 8.1) содержит следующие основные элементы:

— технические средства разведки (TCP);

— каналы передачи информации (КПИ);

— центры сбора и обработки информации (ЦСОИ).

Технические средства разведки представляют собой (рис. 8.2) совокупность разведывательной аппаратуры, предназначенной для обнаружения демаскирующих признаков, предварительной обработки, регистрации перехваченной информации и ее передачи через КПИ в ЦСОИ. В ЦСОИ информация от различных TCP накапливается, классифицируется, анализируется и предоставляется потребителям (автоматизированным системам управления или лицам, принимающим решения

|  |
| --- |
| 39  Рис. 8.2 – Упрощенная структурная схема системы технической разведки |

8.9 Классификация средств коммерческой разведки и их демаскирующие признаки

*8.9.1. Классификация средств технической и коммерческой разведки.* Техническая и коммерческая радиоэлектронная разведка (РЭР) – это получение информации путем приема и анализа электромагнитного излучения радиодиапазона, создаваемого различными радиоэлектронными средствами (РЭС). Названная разведка включает а) РР – радиоразведку б) РТР - радиотехническуюразведку. Обе ониотносятся к к пассивным разновидностям РЭР. Различия между РР и РТР заключаются в объектах, на которые они нацелены. Объектами РР являются: средства радиосвязи, радиотелеметрии и радионавигации. Объектами РТР являются: радиотехнические устройства различного назначения, а также ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т.п.).

*8.9.2. Демаскирующие признаки средств технической и коммерческой разведки*. Процесс ведения разведки состоит из двух этапов: а) обнаружение объекта; б) распознавание обнаруженного объекта. Основным признаком, по которому обнаруживается объект, является его контраст на окружающем фоне.

Процесс распознавания - это отнесение обнаруженного объекта к одному из классов объектов по характерным признакам, присущим данному классу, или по демаскирующим признакам объекта при его распознавании. Все демаскирующие признаки (ДП), по которым распознается объект, можно разделить на следующие группы:

1. признаки, характеризующие физические свойства вещества объекта, например, тепло(определяет тепловой контраст), электропроводность (определяет радиолокационный контраст), структура;
2. признаки, характеризующие свойства физических полей, создаваемых объектом (к таким физическим полям можно отнести электромагнитное поле, акустическое поле, радиационное поле, гравитационное поле);
3. признаки, характеризующие форму, цвет, размеры объекта;
4. признаки, характеризующие пространственное положение (координаты) объекта и производные от координат, если объект перемещается;
5. признаки, характеризующие наличие определенных связей между элементами объекта, если объект носит комплексный (сложный) характер;
6. признаки, характеризующие результаты функционирования объекта, например, следы объекта на грунте, задымленность, запыленность, химическое загрязнение среды.

Делить ДП можно также на количественные (длительность импульса и т.п.) и качественные (форма, цвет и т.п.). В системах технической и коммерческойразведки реализуется обнаружение и анализ целого ряда демаскирующих признаков (ДП). Обнаружение ДП по физической сути заключается в выполнении следующих операций:

— поиск и обнаружение энергии ДП в пространстве, во времени, по спектру и т.д.;

— выделение ДП из искусственных и естественных помех.

Физический смысл анализа ДП раскрывают следующие операции:

— разделение ДП различных объектов;

— оценка параметров ДП (определение их объективных характеристик);

— сокращение избыточности информации;

— регистрация, накопление и классификация ДП;

— нахождение местоположения источника ДП;

— распознавание смыслового содержания ДП;

— выявление охраняемых сведений.

8.10 Скрытие сигналов технических средств обработки информации

В зависимости от финансового обеспечения, а также возможностей доступа к тем или иным средствам разведки, злоумышленник имеет различные возможности по перехвату информации. Например, для перехвата могут использоваться средства разведки побочных электромагнитных излучений и наводок, электронные устройства перехвата информации, внедряемые в технические средства, и др. [8]. Для обеспечения дифференцированного подхода к организации скрытия сигналов технических средств обработки информации (ТСОИ) защищаемые объекты должны быть отнесены к соответствующим категориям и классам.

*8.10.1 Классификация объектов* проводится по задачам технической защиты информации и устанавливает требования к объему и характеру комплекса мероприятий, направленных на защиту конфиденциальной информации от утечки по техническим каналам в процессе эксплуатации защищаемого объекта.

Защищаемые объекты целесообразно разделить на два класса защиты (табл. 8.1).

**К** **классу защиты А** относятся объекты, на которых осуществляется полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте).

**К классу защиты Б** относятся объекты, на которых осуществляется скрытие параметров информационных сигналов, возникающих при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте).

Таблица 8.1 – Классы защиты объектов информатизации и выделенных помещений

|  |  |
| --- | --- |
| Задача технической защиты информации | Установленный класс защиты |
| Полное скрытие информационных сигналов, которые возникают при обработке информации или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте) | А |
| Скрытие параметров информационных сигналов, которые возникают при обработке информации или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте) | Б |

При установлении категории защищаемого объекта учитываются класс его защиты, а также финансовые возможности предприятия по закрытию потенциальных технических каналов утечки информации. Защищаемые объекты целесообразно разделить на три категории (табл. 8.2).

Таблица 8.2 – Категории объектов информатизации и выделенных помещений

|  |  |  |
| --- | --- | --- |
| Задача технической защиты информации | Закрываемые технические каналы утечки информации | Установленная категория объекта защиты |
| Полное скрытие информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров (скрытие факта обработки конфиденциальной информации на объекте) | все потенциальные технические каналы утечки информации | 1 |
| Скрытие параметров информационных сигналов, возникающих при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте) | все потенциальные технические каналы утечки информации | 2 |
| Скрытие параметров информационных сигналов**,** возникающих при обработке информации техническим средством или ведении переговоров, по которым возможно восстановление конфиденциальной информации (скрытие информации, обрабатываемой на объекте) | наиболее опасные технические каналы утечки информации | 3 |

*8.10.2 Категорирование защищаемых объектов* информатизации и выделенных помещений проводится комиссиями, назначенными руководителями предприятий, в ведении которых они находятся. В состав комиссий, как правило, включаются представители подразделений, ответственных за обеспечение безопасности информации, и представители подразделений, эксплуатирующих защищаемые объекты. Категорирование защищаемых объектов проводится в следующем порядке:

* определяются объекты информатизации и выделенные помещения, подлежащие защите;
* определяется уровень конфиденциальности информации, обрабатываемой ТСОИ или обсуждаемой в выделенном помещении, и производится оценка стоимости ущерба, который может быть нанесен предприятию (организации, фирме) вследствие ее утечки;
* для каждого объекта защиты устанавливается класс защиты (А или Б) и определяются потенциальные технические каналы утечки информации и специальные технические средства, которые могут использоваться для перехвата информации;
* определяется рациональный состав средств защиты, а также разрабатываются организационные мероприятия по закрытию конкретного технического канала утечки информации для каждого объекта защиты;
* для информации, отнесенной к конфиденциальной и предоставленной другой стороной, определяется достаточность мер, принятых по ее защите (меры или нормы по защите информации определяются соответствующим договором);
* проводится оценка стоимости мероприятий (организационных и технических) по закрытию конкретного технического канала утечки информации для каждого объекта защиты;
* с учетом оценки возможностей вероятного противника (конкурента, злоумышленника) по использованию для перехвата информации тех или иных технических средств разведки, а также с учетом стоимости закрытия каждого канала утечки информации и стоимости ущерба, который может быть нанесен предприятию вследствие ее утечки, определяется целесообразность закрытия тех или иных технических каналов утечки информации;
* после принятия решения о том, какие технические каналы утечки информации необходимо закрывать, устанавливается категория объекта информатизации или выделенного помещения (табл. 8.2). Результаты работы комиссии оформляются актом, который утверждается должностным лицом, назначившим комиссию.

К ТСОИ относятся средства ЭВТ (электронно-вычислительной техники), информационные системы, средства радиопередачи, звуко- и видеозаписи и воспроизведения, охранной сигнализации, электрические часы, множительная техника. При работе ТСОИ возникает ряд технических каналов, по которым возможна утечка секретной информации. К таким каналам относятся электромагнитные (ЭМ) поля, возникающие при работе ТСОИ, ЭМ наводки на соседние провода, которые уходят за пределы охраняемой территории, токи заземления, сети питания, паразитная генерация, возникающая при самовозбуждении усилителей различных систем, акустические информационные поля, воздействующие на электродинамические системы различных устройств. Для предотвращения утечки закрытой информации по этим каналам реализуется комплекс организационных мероприятий и технических мер.

К организационным мероприятиям относятся:

1. отключение телефонов и динамиков от линии
2. изъятие электронных часов
3. отключение систем селекторной и диспетчерской связи.

Технические меры:

1. -экранирование устройств, излучающих ЭМ энергию
2. контуры заземления в пределах охраняемой территории
3. установка спец/устройств в телефоны
4. питание ЭВТ от мотор-генераторов.

8.11 Техническая дезинформация

Следующим основным направлением противодействия (ПД) техническим средствам разведки является техническая дезинформация, которая объединяет все организационно-технические меры противодействия, направленные на затруднение анализа демаскирующих признаков (ДП) и навязывание противнику ложной информации.

Скрытие, обеспечивая противодействие обнаружению, всегда затрудняет или исключает возможность проведения анализа демаскирующего признака. Техническая дезинформация, наоборот, затрудняя анализ, как правило, не влияет на возможность обнаружения объекта разведки.

Некоторые ТСР предназначены для обеспечения активного воздействия на любые объекты, чьи сигналы оказываются в заданных диапазонах поиска и обнаружения. Техническая дезинформация в такой ситуации может оказаться неэффективной. Поэтому реализация стратегии скрытия объекта является более радикальным направлением противодействия TCP, чем техническая дезинформация.

Однако на практике часто встречаются ситуации, когда невозможно обеспечить при ограниченных ресурсах надежное скрытие объекта (например, крупного здания или сооружения) или отдельных демаскирующих признаков (таких, как мощные непрерывные электромагнитные излучения радиоэлектронных и оптических систем на открытой местности). В подобных ситуациях цели противодействия техническим средствам разведки могут достигаться только применением методов и средств технической дезинформации.

Кроме рассмотренных мер ПД TCP, предполагающих нормальное функционирование всех составных частей системы разведки, возможно проведение активных действий по выявлению и выведению из строя элементов системы разведки.

8.12 Контроль эффективности противодействия

Комплексный технический контроль эффективности противодействия техническим средствам разведки — это контроль за состоянием функционирования своих технических и организационных средств защиты от технических средств разведки противника. Включает контроль эффективности всех вышеперечисленных способов ПД ТСР – скрытие своих демаскирующих признаков, включая скрытие сигналов своих средств передачи и обработки [информации](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F), применение методов и средств технической дезинформации, проведение активных действий по выявлению и выведению из строя элементов системы разведки. Качественная и количественная оценка эффективности контроля противодействия техническим средствам разведки как совокупности согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания охраняемых сведений с помощью технических средств, может проводиться различными способами. Можно использовать метод экспертных оценок, можно рассчитывать риски информационной безопасности и т.д.

Технический контроль предназначен для оценки эффективности и надежности принятых мер защиты от технической разведки. Технический контроль проводится по различным физическим полям скрываемого объекта и включает несколько этапов:

1. подготовка исходных данных для контроля:
2. ознакомление с объектом;
3. анализ его демаскирующих признаков;
4. уточнение видов и средств технической разведки, которым необходимо противодействовать;
5. расчет возможных зон разведдоступности объекта;
6. подготовка и проверка контрольно-измерительной аппаратуры (КИА);
7. измерение технических характеристик скрываемого физического поля объекта;
8. оценка эффективности принятых мер защиты путем сравнения измеренных параметров с нормативными показателями;
9. разработка рекомендаций по устранению выявленных недостатков и совершенствованию систем защиты объектов; написание акта технического контроля.

Для качественного проведения технического контроля необходимо наличие трех элементов:

1. нормы эффективности защиты от технической разведки;
2. методики проведения технического контроля;
3. КИА с требуемыми характеристиками.

Нормы эффективности - это максимально допустимые значения контролируемых параметров физического поля на границе охраняемой территории. Под методиками технического контроля понимается совокупность измерительных и расчетных операций и порядок их проведения в процессе проведения контроля. КИА должна удовлетворять следующим требованиям:

1. обеспечивать непосредственное измерение контролируемого параметра;
2. чувствительность аппаратуры должна быть не хуже установленных норм.

В зависимости от содержания выполняемых операций технический контроль можно разделить на 3 разновидности:

1. *инструментальный контроль* (когда контролируемый параметр определяется непосредственно в процессе измерения);
2. *инструментально-расчетный контроль* (когда контролируемый параметр определяется путем расчета по исходным данным, полученным в процессе измерения);
3. *расчетный контроль* (когда контролируемые параметры определяются путем расчета по исходным данным, которые содержатся в руководящей и справочной документации.

Инструментальный контроль является основным и используется в тех случаях, когда КИА имеет требуемые характеристики. Инструментально-расчетный контроль используется в тех случаях, когда КИА либо имеет недостаточную чувствительность, либо не позволяет измерить непосредственно контролируемый параметр. Расчетный контроль используется в тех случаях, когда отсутствует КИА.