Е. Г. Воробьев, С. В. Войцеховский, А. С. Марковский
под ред. Н. М. Михайлова

Специалист объекта информатизации по технической защите информации

Афина
Издательский дом

Е. Г. Воробьев, С. В. Войцеховский
под ред. Н. М. Михайлова

Специалист объекта информатизации по технической защите информации

ООО «Издательский дом «Афина», 194017, Санкт-Петербург, ул. Гданьская, 19-37
Факс: (812) 347-74-12, тел.: 347-74-12, 958-25-50, 921-68-24,
e-mail: magazine@inside-zi.ru, http://www.inside-zi.ru

Анонс к курсу «Специалист объекта информатизации по технической защите информации»

Неблагоприятная криминогенная обстановка, недобросовестная конкуренция, активизация действий террористов заставляют общество повернуться лицом к проблеме обеспечения безопасности, одним из важнейших аспектов которой является информационная безопасность.

Бурное развитие современных технологий и технических средств способствует постоянному расширению спектра возможных каналов утечки информации, поэтому блокирование каналов утечки становится все более актуальной и сложной задачей.

На эффективность систем безопасности существенно влияют характеристики каналов утечки информации, поэтому создание систем эффективной защиты должно происходить с учетом особенностей реальных каналов. Окончательный вывод об утечке информации может сделать только квалифицированный специалист, использующий специальные технические средства. С другой стороны, особенности реальных каналов утечки информации могут быть успешно использованы и злоумышленником для обеспечения несанкционированного доступа к информации, о чем необходимо постоянно помнить. Так, съем информации по акустическим каналам может быть осуществлен через стекла окон, строительные, сантехнические, вентиляционные, теплотехнические и газораспределительные конструкции, с использованием для передачи сигналов радио, радиотрансляционных, телефонных и компьютерных коммуникаций, антенных и телевизионных распределительных сетей, охранно-пожарной и тревожной сигнализации, сетей электропитания и электрочасов, громкоговорящей и диспетчерской связи, цепей заземления и т.п. Случайный пропуск хотя бы одного возможного канала утечки может свести к нулю все затраты и сделать систему защиты неэффективной.

Основные надежды специалисты связывают с внедрением интегральных подходов и технологий. Необходимым условием реализации интегрального подхода является блокирование всех технических каналов утечки и несанкционированного доступа к информации, поэтому для создания эффективных систем безопасности, в первую очередь, необходимо исследовать возможные каналы утечки и их характеристики, а также применить все имеющиеся средства технической защиты информации. К сожалению, в настоящее время имеется широкий выбор средств специальной техники, с помощью которых возможно попытаться получить несанкционированный доступ к информации. Для выбора возможных путей блокирования каналов утечки необходимо знать «противника в лицо».

Но, как правило, специалисты по компьютерной технике ничего не знают о технических средствах разведки и защиты, и наоборот, специалисты по ТЗИ слабо понимают возможности компьютерной техники по защите информации.

Кроме того, зачастую на промышленных предприятиях, в банковских и коммерческих структурах внештатными сотрудниками ФСТЭК назначают людей без специального образования.

Задачей данного курса является получение широким кругом руководящих работников, не имеющих предварительной подготовки и подчиненных им специалистов служб безопасности государственных и коммерческих предприятий знаний по широкому кругу вопросов в сфере защиты конфиденциальной информации.

Курс оптимально сочетает в себе изучение новейшего отечественного законодательства в области технической защиты информации, информацию о последних достижениях науки и техники в области существующих каналов утечки информации и организации защиты конфиденциальной информации на объектах информатизации.

Слушателям предоставляется специально разработанный учебник и иллюстрированный конспект. По результатам обучения выдается свидетельство учебного центра.

Курс «Специалист объекта информатизации по технической защите информации»

***Ориентирован на*:** IT-специалистов, менеджеров, администраторов безопасности систем, специалистов по корпоративной и физической безопасности, внутренних аудиторов и аудиторов информационных систем. Предварительный уровень подготовки: базовая подготовка в области информационных технологий. Подготовка в области информационной безопасности не требуется.
Продолжительность: 3 дня, 24 часа.

***Содержание программы*:**

1. Организация защиты информации на объекте информатизации.
   - Актуальность проблемы, цели, задачи и содержание курса.
   - Основные термины и определения.
   - Обеспечение защиты конфиденциальной информации
2. Законодательство в области технической защиты информации.
   - Российское законодательство в области технической защиты информации
3. Особенности несанкционированного получения информации техническими средствами.
   - Анализ уязвимостей информации.
   - Особенности ведения разведки информации.
4. Выявление технических каналов утечки информации.
   - Классификация и общая характеристика технических каналов утечки информации
   - Физические принципы возникновения каналов утечки информации
   - Способы выявления каналов утечки информации
   - Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.
   - Методика оценки защищённости ОТСС от утечки конфиденциальной информации (КИ) за счёт наводок на токоведущие коммуникации, выходящие за пределы контролируемой зоны (КЗ).
   - Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований.
5. Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах.

Требования, рекомендации, порядок обеспечения защиты информации при эксплуатации АС, в ЛВС, на АРМ, при межсетевом взаимодействии, при работе с СУБД, при использовании съемных накопителей информации.

6. Рекомендации по обеспечению защиты конфиденциальной информации, при взаимодействии абонентов с Интернетом.
   - Условия, порядок подключения абонентов к сети.
   - Взаимодействие АП с сетью.
   - Рекомендации по обеспечению безопасности информации.
7. Средства технической защиты информации.
   - Способы применения средств акустической защиты.
   - Способы и средства противодействия несанкционированной аудио- и видеозаписи.
   - Правила организации экранирования и заземления.
   - Фильтрация информационных сигналов.
   - Пространственное и линейное зашумление.
   - Организация и средства защиты от утечки информации за счет ПЭМИН.
8. Средства защиты информации в автоматизированных системах.
   - Средства защиты от НСД.
   - Средства защиты операционных систем.
   - Штатные средства защиты СУБД.
   - Частные виртуальные сети. Межсетевые экраны.
   - Проблемы защиты информации при взаимодействии с сетью Интернет.
   - Антивирусная защита.

ОГЛАВЛЕНИЕ

1. Организация защиты информации на объекте информатизации

1.1. Основные термины и определения. Коммерческая тайна.

В настоящее время в России произошло разделение тайны на государственную и коммерческую. Таким образом, из области публичного права выделился институт частного права, который защищает интересы предпринимателей.

Коммерческая тайна перечнем определенных сведений не определена, поскольку она всегда разная применительно к различным предприятиям или фирмам и охраняется службой безопасности предприятия. При этом следует иметь в виду, что коммерческие секреты могут быть государственными секретами, однако государственные секреты не могут быть коммерческой тайной, поскольку в противном случае шла бы торговля государственными интересами.

В повседневной жизни коммерческая тайна всегда выступает в форме коммерческих секретов. Поэтому всякая тайна есть секрет, но не всякий секрет есть тайна. Исходя из этого, попробуем дать определение коммерческой тайны и коммерческого секрета.

Коммерческая тайна — преднамеренно скрываемые по коммерческим соображениям экономические интересы и сведения о различных сторонах и сферах производственно-хозяйственной, управленческой, научно-технической, финансовой деятельности фирмы, охрана которых обусловлена интересами конкуренции и возможными угрозами экономической безопасности фирмы. Коммерческая тайна возникает тогда, когда она представляет интерес для коммерции.

Коммерческие секреты — форма проявления коммерческой тайны. Представляют собой сведения в виде документов, схем, изделий, относящиеся к коммерческой тайне фирмы и подлежащие защите со стороны службы безопасности от возможных посягательств путем похищения, выведывания, утечки информации. Они различаются по следующим признакам:

- по природе коммерческой тайны (технологические, производственные, организационные, маркетинговые, интеллектуальные, рекламные);
- по принадлежности собственнику (собственность предприятия, группы предприятий, отдельного лица, группы лиц и т. д.);
- по назначению коммерческих секретов. Документы, содержащие коммерческие секреты, могут иметь гриф «Конфиденциально», «Строго конфиденциально», «Конфиденциально, только адресату» и другие.

Носитель коммерческого секрета — лицо, осведомленное о коммерческих секретах предприятия или фирмы (руководители и допущенные к коммерческим секретам исполнители).

Носителей коммерческих секретов следует отличать от источников закрытой коммерческой информации («ноу-хау», схемы, документы, технологии, изделия, образцы).

Секретность в условиях рыночного хозяйствования защищает производителя от недобросовестной конкуренции, к которой относятся различные противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т. п. Не последнее место в этом ряду занимает «промышленный шпионаж».

Сегодня стало почти массовым явлением беззастенчивое заимствование интеллектуальной и промышленной собственности: сотрудники предприятий, являясь одновременно членами кооперативов, малых предприятий или совместных предприятий, используют методики, программы и технологии, разработанные на отечественных предприятиях и являющиеся их интеллектуальным капиталом. Западные партнеры стремятся незаконным путем получить закрытую информацию, представляющую для них экономический интерес. Поэтому обеспечение экономической безопасности предприятия, фирмы и любой другой формы хозяйствования требует защиты коммерческой тайны.

В США, ФРГ, КНР, Японии и других странах защита коммерческой тайны обеспечивается системой промышленной секретности, которая базируется на соответствующей правовой базе. При этом основную роль в обеспечении ее сохранности играют сами фирмы, а не государственные органы.

В Соединенных Штатах, имеющих наиболее совершенное законодательство в области защиты информации, Закон о коммерческой тайне или по принятой там терминологии — «фирменных секретов» («секретов производства») — был принят только в 1979 году, и то не всеми штатами. Согласно этому закону коммерческой тайной является информация, которая:

- имеет самостоятельную экономическую стоимость благодаря тому, что не является общеизвестной или доступной людям, которые могут ее использовать в коммерческих целях;
- является объектом разумных усилий по защите. Разумеется, если что-то названо коммерческой тайной, то это действительно должно ею быть, что бывает непросто доказать юридически. Поэтому закон рекомендует:
- указать ценность информации (какие средства затрачены на получение информации и во что обойдется Вам ее несанкционированное обнародование);
- назвать, какие меры защиты данного секрета были предприняты.

В ФРГ действует закон о недобросовестной конкуренции, в котором выделяются два вида тайн — производственная и коммерческая. Данный закон устанавливает уголовную ответственность до трех лет тюремного заключения за сообщение коммерческой или производственной тайны посторонним лицам, а также за ее выведывание.

К производственной тайне в ФРГ относятся сведения организационного и технического характера, которые касаются способа производства, технологии, организации труда, а также технические открытия, изобретения либо сведения о характере и целях исследовательских работ и т. д.

Коммерческой тайной, в отличие от производственной, являются сведения, которые касаются торговых отношений фирм: организация и размеры оборота, состояние рынков сбыта, сведения о поставщиках и потребителях, сведения о банковских операциях.

Госсовет КНР в 1988 году утвердил Положение о коммерческих службах безопасности, не входящих в структуру государственных правоохранительных органов.

Коммерческие службы безопасности являются хозрасчетными организациями и выполняют определенный вид работ и услуг согласно контрактам, заключаемым с госучреждениями, кооперативами, частными предприятиями, а также с предприятиями, основанными на смешанном китайском и иностранных капиталах. Решение о том, какие секреты необходимо защищать на каждом предприятии, в каждой организации принимается на основе договоренности и строится на экономическом расчете.

В Японии нет ни законов, ни каких-либо других нормативных актов, предусматривающих ответственность за разглашение коммерческой тайны. Там эта проблема решается следующим образом: на департаменты кадров, имеющихся в каждой японской фирме, возлагается контроль за неукоснительным соблюдением режима секретности, который основывается на кодексе поведения служащих. В нем содержатся положения, запрещающие:

- передавать посторонним лицам сведения, содержащие коммерческую тайну;
- заключать сделки, которые могут подорвать доверие к компании со стороны клиентов;
- устраиваться без разрешения руководства на работу по совместительству;
- умышленно наносить экономический ущерб;
- давать и получать взятки.

Следует отметить, что японский бизнес менее всего страдает от утечки информации. Это связано с присущей этой стране системой «пожизненного найма» и воспитанием у сотрудников чувства патернализма, когда они считают себя членами одной семьи.

Руководитель фирмы «SONY» Акио Морита утверждает, что «...когда нет преданности, которая приходит с долгосрочной занятостью, нет возможности положить конец утечке информации и воровству, от которых повседневно страдает бизнес на Западе» .

Понятие «коммерческая тайна» совсем недавно появилось в нашем законодательстве. Если быть точным, то это признано 12 июня 1990 года, когда был принят Закон «О предприятиях и предпринимательской деятельности».

Согласно ст. 139 Гражданского кодекса РФ, принятого 21.10.94 Государственной Думой, «информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности».

Разглашение коммерческой тайны может ухудшить экономическое положение предприятия или фирмы. Чтобы этого не произошло, следует перевести такую информацию в разряд охраняемой. У нас это делается приказом руководителя фирмы, в котором перечисляются сведения, относящиеся к коммерческой тайне. Однако он не вправе отнести к ней сведения, 'подпадающие под категорию государственной тайны, так как они имеют свой, специальный режим охраны. Кроме того, руководитель фирмы не может отнести к коммерческой тайне сведения о видах деятельности фирмы, поскольку это может привести к сокрытию сведений о загрязнении окружающей среды и другой негативной деятельности, способной нанести ущерб обществу.

В Российской Федерации введен закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ. Этот закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

В законе используются следующие основные понятия:

1) *коммерческая тайна* – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

2) *информация, составляющая коммерческую тайну*, – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

3) *режим коммерческой тайны* - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;

4) *обладатель информации, составляющей коммерческую тайну*, – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

5) *доступ к информации, составляющей коммерческую тайну*, – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

6) *передача информации, составляющей коммерческую тайну*, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

7) *контрагент* – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

8) *предоставление информации, составляющей коммерческую тайну*, – передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

9) разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации, либо вопреки трудовому или гражданско-правовому договору.

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

оглавление
1
2
3
4
5
6
7
8

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Опираясь на опыт международных коммерческих организаций можно добавить следующие рекомендации:

1. При засекречивании информации надо исходить из принципа экономической выгоды и безопасности фирмы.

Причем, объявляя ту или иную информацию коммерческой тайной, важно соблюсти «золотую середину». Чрезмерное засекречивание деятельности фирмы может обернуться потерей прибылей, так как условия рынка требуют широкой рекламы производимой продукции и услуг. Те же результаты может вызвать пренебрежительное отношение к коммерческой тайне, так как рынок — это всегда конкуренция. Американские предприниматели считают, что угроза 20 % информации приводит к разорению фирмы в течение месяца в шестидесяти случаях из ста.

2. Информация типа «ноу-хау», безусловно, должна быть отнесена к разряду коммерческой тайны. Ее надо охранять и от собственного персонала, ибо всегда существует опасность, что тот или иной сотрудник уволится и устроится на работу в конкурирующую фирму. Сведения же, которыми он владеет, не могут быть у него изъяты.

За рубежом существует практика подписания с сотрудником соглашения, по которому ему после увольнения запрещается работать в конкурирующей фирме. Правда, такого рода соглашения действуют лишь в течение определенного срока после расторжения договора о найме. Кроме того, во время действия подобного ограничения этому лицу должно выплачиваться вознаграждение. В нашей практике такие соглашения пока неизвестны.

3. Информация о рационализаторском предложении, изобретении и т. п., находящегося на стадии разработки, несомненно, относится к коммерческой тайне.

Рационализаторское предложение даже после его оформления и выдачи авторского свидетельства может оставаться коммерческой тайной, поскольку представляет собой техническое решение задачи, новое для данной фирмы.

Изобретение после выдачи на него патента имеет специальную правовую охрану и поэтому не нуждается в защите при помощи коммерческой тайны. Другое дело, если по соглашению с автором изобретения фирма примет решение не подавать заявку в Госпатент Российской Федерации. Тогда охрана информации полностью возлагается ни фирму. Следует подчеркнуть, что решение не подавать заявку на изобретение на патентоспособное техническое решение возможно только по договоренности с автором, так как по существующему правилу, если работодатель в течение трех месяцев с мо-

мента уведомления его автором о сделанном изобретении не подаст заявку не него, автор вправе сам подать заявку и получить патент.

До недавнего времени 90 % авторских свидетельств получали гриф «Для служебного пользования». Вместо авторского свидетельства теперь выдают патент.

Основным принципом патента является его обязательная открытость, что способствует ускорению научно-технического прогресса. Патент — тот же товар изобретателя, но государство продолжает засекречивать патенты, т. е. нарушает права изобретателей. Государство же должно не отбирать у человека право на его интеллектуальную собственность, а выкупать его, причем по рыночной стоимости.

4. Особое внимание следует уделить охране договоров, заключаемых предприятием. Большая их часть, безусловно, относится к коммерческой тайне. Причем в определенных случаях охране подлежит не только текст договора, но и сам факт его заключения.

1.2. Обеспечение защиты конфиденциальной информации

Промышленный шпионаж в настоящее время приобрел поистине гигантский размах во всем мире.

По оценке экспертов, ежегодный урон американского бизнеса от кражи производственных и торговых секретов превышает четыре миллиарда долларов.

Кроме прямого похищения, происходит и утечка информации, при этом наиболее вероятными ее источниками являются:

- персонал, имеющий доступ к информации;
- документы, содержащие эту информацию;
- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

Итак, персонал — один из главных каналов утечки информации. Зная это, следует более тщательно изучать биографии особо важных сотрудников. Следует обратить пристальное внимание как на вновь пришедших на работу, так и на тех, кто подлежит увольнению. Эти люди находятся в ситуации, наиболее благоприятных для утечки информации.

Возможными источниками утечки интеллектуальной собственности могут стать конгрессы, конференции, симпозиумы, торговые выставки, демонстрации созданной техники, ярмарки, реклама и т. п. Профессионалов промышленного шпионажа привлекают и различные съезды специалистов, потому что они знают: самые лучшие источники коммерческой и научно-технической информации — болтуны.

Утечка информации охватывает широкий круг различных действий. Это и утрата информации из компьютера, и пропажа документов. Утратой считается и тайное копирование информации конфиденциального характера с дискеты на дискету, снятая «лично для себя» копия документа, содержащего коммерческую тайну.

Существуют три общепринятых метода защиты интеллектуальной собственности: *патент*, *авторское право* и *коммерческая тайна*.

Патентом оформляется право изобретателя «законно монополизировать» использование изобретения в течение установленного периода времени. Основами гражданского законодательства срок действия патента определен в 20 лет. Патент является способом защиты промышленной, а не коммерческой информации.

Авторское право, напротив, защищает только форму, в которой выражена конкретная идея, а не саму идею. Это отличает авторское право и от патента, и от коммерческой тайны, которые относятся к сущности, содержанию идеи. Оригинальные мысли, содержащиеся в книгах и научных статьях, после их прочтения уже принадлежат каждому. Ими можно свободно пользоваться. Однако при использовании этих идей в новых публикациях необходимо делать ссылки на конкретного автора, иначе будут нарушены авторские права. Это относится в большей степени к литературному творчеству, музыке, программному обеспечению.

Коммерческая тайна как форма интеллектуальной собственности в нашей стране не охвачена правовым регулированием, поэтому для защиты коммерческой информации применение законодательных мер значительно осложнено, и здесь большое значение приобретают другие меры защиты.

Немаловажную роль в защите информации играют морально-этические нормы, которые не являются обязательными, однако их несоблюдение ведет к потере авторитета (престижа) человека, группы лиц либо всей организации.

При охране информации от прямого хищения или уничтожения нередко прибегают к мерам физической защиты. Это — замки на дверях, решетки на окнах, различные механические, электромеханические и электронные устройства охраны здания, лаборатории, других помещений фирмы.

Физические меры защиты, как правило, применяются в совокупности с административными мероприятиями. К ним относятся: организация соответствующего режима секретности, пропускного и внутреннего режима, создание службы безопасности, обучение и инструктаж персонала.

Технические системы охраны включают в себя электромеханические, акустические, емкостные, радиотехнические, магнитометрические средства.

Криптографические меры защиты позволяют шифровать информацию таким образом, чтобы ее содержание могло стать доступным только при предъявлении специфической информации (ключа). Специалисты считают криптографическое закрытие информации наиболее эффективным и надежным средством.

В качестве потенциальных угроз безопасности информации могут выступать стихийные бедствия, неблагоприятная внешняя среда, катастрофы, политическая нестабильность, ошибки и неисправности программы, компьютерная преступность. Исходя из характера угрозы, применяются различные меры противодействия.

Для защиты коммерческих секретов следует соблюдать следующие правила:

- обеспечение безопасности всегда и везде — дело профессионалов, потому что для этого требуются специальные знания;
- предпринимаемые превентивные меры должны предусматривать специальную программу по дезинформации промышленных шпионов;
- система превентивных мер должна включать в себя такой важнейший элемент, как организация движения охраняемой информации, исключив при этом возможность ее утечки;
- система превентивных мер должна быть основана на материальной заинтересованности сотрудников, а для этого надо адекватно оплачивать их труд. В нашей стране такую систему превентивных мер по защите коммерческой тайны могут позволить себе пока что немногие частные фирмы.

Объективные потребности фирмы, банка, страховой компании и т. п. в обеспечении сохранности коммерческой тайны определяются рядом факторов, а именно:

- обострением конкурентной борьбы на рынке товаров и услуг;
- важностью сохранения секретной информации в течение определённого времени;
- возможностью проверить каждый из вероятных каналов утечки информации, и в первую очередь по конкретным служащим.

Последние два фактора должны быть тщательно просчитаны по затратам: стоит ли овчинка выделки?

На начальной стадии создания фирмы, когда ее штат ограничен несколькими сотрудниками, а финансовые возможности не позволяют осуществить весь комплекс мер по защите информации, складывается ситуация, при которой любые действия конкурентов несут реальную угрозу гибели фирмы. На этой стадии необходимо осуществить хотя бы минимально возможный комплекс мер:

- предусмотреть, чтобы служащие в заявлениях о приеме на работу, в трудовых соглашениях и контрактах принимали на себя четко выраженные письменные обязательства не разглашать тайны фирмы и иные сведения, ею охраняемые;
- определиться с потоками информации и все документы, содержащие коммерческую тайну, снабдить соответствующим грифом, отражающим степень их секретности. Сюда относятся, прежде всего, документы с планами предстоящей деятельности фирмы, технологическая документация, списки поставщиков и покупателей;
- предусмотреть вопросы защиты коммерческой тайны в типовых соглашениях с заказчиками, покупателями изделий и услуг фирмы, продавцами, торговыми агентами и др.

Разрабатывая меры по защите коммерческой тайны фирмы, необходимо экономически обосновать целесообразность засекречивания той или иной информации.

В первую очередь выделяется информация, утечка которой может привести вашу фирму к банкротству. Это строго конфиденциальная информация. В мире бизнеса это, как правило, «ноу-хау». К конфиденциальной информации относятся сведения о перспективах развития фирмы, ее клиентах, сроках и сумме кредитования. Огласка этих сведений, конечно же, не приведет к краху, но лишит фирму на какое-то время устойчивой прибыли.

Не подлежит огласке информация, раскрытие которой может привести к неблагоприятным последствиям. К ней относятся: номера домашних телефонов, адреса руководителей и сотрудников фирмы, текущие планы работы, информация о конфликтных ситуациях в коллективе и т. п.

Остальные сведения относятся к открытым, то есть доступным всем. Но следует иметь в виду, что неправильно поданная информация может помочь аналитикам из конкурирующей фирмы обнаружить ваши уязвимые места.

Руководитель фирмы должен установить строгий порядок хранения первых экземпляров договоров и работы с ними. Их следует хранить в определенном месте у ответственного лица и выдавать только под расписку с письменного разрешения руководителя фирмы. На лица, ответственные за хранение договоров и работу с ними, возлагается персональная ответственность за утерю договоров или утечку информации из них. Все это необходимо потому, что деятельность коммерческих структур строится в большей степени на договорных началах, и конкурент или партнер по переговорам, обладая информацией в этой сфере, может составить довольно полную картину производственного и финансового положения фирмы. Пропажа (похищение) первых экземпляров ведет к значительным затруднениям и даже невозможности доказывать те или иные положения при возникновении спора и его разрешения в судебном порядке. При подписании договора рекомендуется, чтобы представители сторон ставили подписи не только в конце договора, но и на каждом листе во избежание замены одного текста другим.

Следует отметить, что затраты зарубежных фирм на охрану своей коммерческой тайны составляют 10-15 процентов всех расходов на процесс производства. Поэтому в наиболее расчетливые предприниматели пытаются на этом сэкономить, переложив затраты на плечи государства. Каким образом? Путем получения госзаказов оборонного характера. Помимо прочих преимуществ, госзаказы позволяют пользоваться защитой государственных правоохранительных органов и, в первую очередь, контрразведки.

Традиционная проверка граждан США, получающих доступ к секретной информации, обычно включает:

- обязательную проверку на детекторе лжи (полиграфе);
- глубокое и всестороннее изучение досье кандидата на работу, проверка его биографических данных за последние 10 лет;
- выяснение целей и обстоятельств поездок за рубеж;
- исследование финансового положения. В ходе проверки служащего полученные сведения сопоставляются с данными Национального банка информации о секретоносителях, где на каждого существует электронное досье. В нем содержатся данные предыдущих проверок его фотография, фонограмма его голоса, сведения об изменениях в его финансовом положении, о его поездках за границу.

В Америке служащие многих фирм и всех специальных учреждений проходят проверку на детекторе не реже одного раза в полгода, причем всегда неожиданно. Это обязательное условие оговорено в контракте. По уже сложившейся традиции первым подвергает себя проверке глава фирмы.

Сейчас полиграфы стали предметом многочисленных споров. После того, как в производстве появились бесконтактные детекторы, определяющие состояние исследуемого на расстоянии по голосу, многие заговорили о правах человека. В 1996 году проверки на полиграфе в той или иной мере применялись в 57 странах мира. Но отношение к нему на Западе неоднозначное. В ФРГ, например, он запрещен законом. Видимо, на то есть свои причины. В России же официальные лица делают вид, что детектора лжи у нас не существует. Он не запрещен и не разрешен никакими документами, хотя определенные подвижки к его официальному применению уже имеются.

В опубликованной 24 июня 1996 года «Федеральной целевой программе по усилению борьбы с преступностью на 1996-1997 годы» предусматривается «оснастить оперативно-технические и опе-

ративные подразделения республиканских, краевых, областных органов внутренних дел специальными техническими средствами (полиграфами, стресс-детекторами по голосу, тензометрическими платформами) для оценки психофизического состояния человека».

Мировой опыт в области защиты производственных секретов показывает, что чисто административные меры не гарантируют результат, поэтому предприниматели, не отказываясь от административных мер, переходят к совмещению их с активным вовлечением в процесс защиты конфиденциальной информации всех сотрудников фирмы.

Главное место в организации надежной защиты конфиденциальной информации должно отводиться работе с кадрами. Специалисты считают, что сохранность секретов на 80 % зависит от правильного подбора, расстановки и воспитания кадров. И эта работа должна начинаться со дня приема человека на работу.

Вторым по важности мероприятием должно быть ограничение доступа к конфиденциальной информации. Работа должна быть организована таким образом, чтобы каждый сотрудник имел доступ только к той информации, которая необходима ему в процессе выполнения прямых служебных обязанностей. Эта мера не сможет сама по себе полностью защитить от возможной ее утечки, но возводит свести возможный ущерб к минимуму.

Третьим направлением в работе с кадрами является проведение воспитательной работы. Специалисты в области противодействия промышленному шпионажу дают следующие рекомендации:

- использовать любую возможность для пропаганды программ обеспечения режима секретности;
- всемерно стимулировать заинтересованность сотрудников в выполнении режима секретности;
- не забывать периодически вознаграждать сотрудников за успехи в защите секретной информации.

Следует иметь в виду, что голые призывы не дают положительных результатов, поэтому значительное место в воспитательной работе необходимо отводить обучению, целями которого являются:

- четкое знание сотрудником объемом охраняемой информации, за безопасность которой он несет личную ответственность;
- понимание исполнителем секретных работ характера и ценности данных, с которыми он работает;
- обучение правилам хранения и защиты секретных данных.

При этом ни одно правило или процедура не должны вводиться без разъяснения их сути, их разумности и необходимости. Каждый руководитель, доводя такие правила до сведения своих подчиненных, обязан подчеркнуть, что они являются неотъемлемой частью их работы.

Вместе с тем не следует ограничиваться только воспитательной работой и обучением. Сотрудник, нарушивший правила работы с секретной информацией, должен знать, что у него будут серьезные неприятности и он будет строго наказан руководством.

Такие подходы к работе с кадрами дают неплохие результаты и могут применяться на предприятиях разного профиля деятельности.

Важным направлением в организации работы по защите конфиденциальной информации является установление порядка обращения с ее носителями, такими как документы, чертежи, дискеты, компьютерные программы и т. п.

При этом следует учитывать, что:

- специалисты ставят обязательным условием наличие на носителях конфиденциальной информации отличительных пометок, различающихся в зависимости от уровня секретности, но они должны отличаться от применяемых в сфере защиты государственных секретов;
- в условиях фирмы обеспечить каждому исполнителю работу в специально выделенном помещении бывает практически невозможно, поэтому следует соблюдать «политику чистых столов». Суть ее заключается в том, что в отсутствие работника на его рабочем месте не должно быть никаких документов.

У нас существует миф о том, что в западных фирмах на каждом шагу стоят ксероксы и сделать копию с любого документа не составляет труда любому желающему. Это абсолютно не соответствует действительности: в любой фирме, имеющей дело с конфиденциальной информацией, существует строго установленный порядок размножения документов. С целью затруднить или даже сделать не-

возможным копирование закрытых материалов принимаются дополнительные меры защиты. Так, американская фирма «Ксерокс» разработала специальный краситель, который наносится на текст документа, что исключает возможность несанкционированного копирования — копия получается нечитабельной.

Как показывает практика, значительная утечка коммерческой информации происходит в ходе ведения переговоров. Это объясняется разными причинами: неверно понимаемый престиж, неумение правильно отрекламировать свою продукцию и т. д. Большую роль играет умение ведения переговоров. Сотрудник должен четко знать, какую информацию он имеет право сообщить партнеру по переговорам, а какую — нет. Необходимо учить проведению рекламы по методу «черного ящика», т. е. можно сообщить параметры изделия, полученный результат, а как он получен — секрет фирмы. Сотрудник должен понимать, что от успешно проведенных переговоров зависит не только процветание фирмы, но и его личное благополучие.

Ключевая роль в структуре подразделения, занимающегося защитой коммерческой тайны, должна отводиться аналитической службе. Современное предприятие, функционирующее в условиях рыночной экономики, разумеется, не может позволить себе засекречивать всю информацию. Это слишком дорого и невыгодно: определенная часть сведений должна использоваться в рекламе, к тому же большое количество засекреченных материалов создает помехи в работе.

В то же время специалисты в области стратегического планирования и управления производством относят сбор информации о конкурентных фирмах и компаниях к обычному маркетингу, также как и информацию о потенциальных потребителях, репутации фирмы, государственном регулировании на рынке и т. п.

Существуют три основных направления сбора информации.

I. Информация о рынке:
- цена, условия договоров, спецификация продукта, скидки;
- объем, тенденция и прогноз сбыта конкретного продукта;
- доля на рынке и тенденция ее изменения;
- рыночная политика и планы;
- отношение с потребителями и репутация;
- численность и расстановка торговых агентов;
- каналы, политика и методы сбыта;
- постановка рекламы.

II. Информация о производстве продукции:
- оценка качества и эффективности;
- номенклатура изделий;
- технология и оборудование;
- уровень издержек;
- производственные мощности;
- способ упаковки;
- доставка;
- размещение и размер производственных подразделений и складов;
- возможности проведения научно-исследовательских работ.

III. Информация об организационных особенностях и финансах:
- выявление лиц, принимающих ключевые решения;
- философия лиц, принимающих ключевые решения;
- программы расширения и приобретений;
- главные проблемы и возможности их решения;
- программа проведения научно-исследовательских работ.

Приведенные направления охватывают практически все аспекты деятельности предприятия, фирмы или компании. И пытаться защитить коммерческую тайну, накладывая ограничения на доступ

к информации по перечисленным направлениям, вряд ли возможно, но оказывать противодействие соперникам по конкурентной борьбе на рынке просто необходимо. Вот здесь-то аналитические подразделения и должны сыграть свою роль в определении ключевой информации, выявлении возможных каналов утечки, поиске путей ее защиты.

С формированием в России рыночных отношений руководители частных фирм явнее других работодателей осознали значение квалифицированного персонала для развития и процветания своих компаний. Важную роль в оценке пригодности кандидата на вакантную должность стал играть уже не только уровень профессиональной подготовки, но и моральные качества работника.

На какие вопросы работодатель обычно желает получить ответ:

- не имеет ли кандидат на вакантную должность вредных наклонностей (алкоголизм, наркомания);
- но скрывает ли сведения о совершенных в прошлом уголовно наказуемых деяниях;
- верно ли сообщил данные о прежних местах работы;
- лоялен ли по отношению к руководству фирмы;
- не имеет ли каких-либо связей с конкурирующими фирмами;
- не вынашивает ли криминальные замыслы.

Наша экономика находится лишь на этапе становления рыночных отношений, поэтому для коммерческих структур, не связанных с выполнением оборонных заказов, состояние защиты от промышленного шпионажа выглядит удручающим.

Что можно рекомендовать руководителю, начинающему создавать систему безопасности па своей фирме? Прежде всего, знать, что это обойдется недешево. Поручить создание системы безопасности профессионалам, только им, и никому более. Сразу же следует подумать о безопасности наиболее важных секретов, утечка которых способна нанести ущерб, значительно превышающий затраты на их защиту. При этом надо установить:

- какая информация нуждается в защите;
- кого она может заинтересовать;
- каков «срок жизни» этих секретов;
- во что обойдется их защита.

Затем следует подготовить план по охране коммерческой тайны. Основываясь на зарубежном опыте, он должен состоять из двух разделов:

- предотвращение похищения секретной информации;
- предотвращение утечки секретной информации. Для этого требуется:
- определить, какая коммерческая информация является секретом фирмы;
- установить места ее накопления;
- выявить потенциальные каналы утечки информации;
- получить консультацию по перекрытию этих каналов у специалистов;
- проанализировать соотношение затрат по использованию различных систем, обеспечивающих защиту секретной информации, и выбрать наиболее приемлемую;
- назначить людей, ответственных за каждый участок этой системы;
- составить график проверки состояния дел на участках. Система обеспечения безопасности фирмы включает в себя следующие организационные мероприятия:
- контроль помещений и оборудования (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль за посетителями);
- работа с персоналом (беседы при приеме на работу, ознакомление вновь принятых с правилами защиты информации, обучение сохранению коммерческой тайны, стимулирование соблюдения коммерческой тайны, работа с сотрудниками, подозреваемыми в хищении секретной информации, беседы с увольняющимися);
- организация работы с конфиденциальными документами (установление порядка делопроизводства, контроль за прохождением секретных документов, контроль за публикациями, рассекречивание и уничтожение конфиденциальных документов, охрана секретов других фирм);
- работа с конфиденциальной информацией, накопленной в компьютерах фирмы (создание систе-

мы защиты электронной информации от несанкционированного доступа, обеспечение контроля за пользованием ЭВМ);
- защита коммерческих тайн фирмы в процессе заключения контрактов (здесь важно четко определить круг лиц, имеющих отношение к этой работе).

Вышеизложенный план является примерным. Однако во всех случаях защиты коммерческой тайны необходимо обратить особое внимание на документы, поскольку в нашей стране основные объемы коммерческой информации хранят в документах.

Руководитель должен упорядочить процессы фиксации секретной информации в деловых бумагах и организовать их движение таким образом, чтобы похищение конфиденциальных документов было бы затруднено настолько, чтобы оно становилось экономически невыгодным для похитителя.

При работе с документами, содержащими коммерческую тайну, следует соблюдать определенные правила, которые сводятся к нижеследующим:
- строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;
- назначение ответственных лиц за контролем секретного делопроизводства и наделение их соответствующими полномочиями;
- разработка инструкции (памятка) по работе с секретными документами, ознакомление с ней соответствующих сотрудников фирмы;
- контроль за принятием служащими письменных обязательств о сохранении коммерческой тайны фирмы;
- введение системы материального и морального поощрения сотрудников, имеющих доступ к секретной информации;
- внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны фирмы;
- личный контроль со стороны руководителя фирмы за службами внутренней безопасности и секретного делопроизводства.

Существуют различные способы ведения секретного делопроизводства, которые направлены на предотвращение утечки содержащихся в документах коммерческих секретов. Как уже было указано выше, документы, содержащие коммерческую тайну, подразделяются по степени, секретности имеющейся в них информации и снабжаются соответствующим грифом секретности.

С коммерческой тайной связано такое понятие, как интеллектуальная собственность, которое в широком смысле слова может быть определено как коммерчески ценные идеи. Не обязательно, чтобы это было что-то новое или запатентованное. Главное, чтобы информация не относилась к числу общеизвестной.

Впервые понятие «интеллектуальная собственность» прозвучало у нас в 1990 году в тексте Закона о собственности в РСФСР. А вообще оно существует с 1967 года, когда на Стокгольмской конференции была создана Всемирная организация интеллектуальной собственности, к которой недавно присоединилось и наше государство. До этого собственностью считалось только то, что можно взять в руки, потрогать или на что можно посмотреть. Наше руководство не задумывалось над тем, какой поистине бесценной интеллектуальной собственностью располагает страна, и что беречь ее надо не меньше, чем золотой запас. Этому свидетельствует целый ряд горьких уроков. Притчей во языцех стал метод непрерывной разливки стали, изобретенный у нас и успешно используемый во всем мире, для возвращения которого на Родину пришлось заплатить немалые деньги. В стране создано большое число лекарственных препаратов, секреты которых уплыли за рубеж, и сейчас мы вынуждены покупать патенты на их производство. Японский бизнесмен тепло поблагодарил журнал «Юный техник» за его приложение «Сделай сам». Используя чертежи, помещенные в этом издании, он заработал миллионы долларов.

Новые идеи — специфический товар, имеющий коммерческую стоимость. В отличие от материальных вещей, которые постоянно обладают стоимостью, сколько бы раз их ни производили, стоимость идей одноразовая (никто не будет платить за уже известные сведения).

Интеллектуальная собственность имеет не только реальную стоимость, в которую входят затраты на получение информации и ее защиту, но и потенциальную стоимость (возможная прибыль при ее

реализации). В качестве несколько неожиданного примера информации, имеющей потенциальную стоимость, можно привести «негативную информацию» (о том, что не надо делать), которая позволяет не расходовать средства на тупиковые разработки.

Сегодня уровень конкурентоспособности в немалой степени зависит от умения защитить свою деловую и техническую информацию от хищений, несанкционированного использования, изменения или уничтожения.

В промышленно развитых странах основой защиты коммерческой тайны являются законодательные акты и контракты найма-увольнения, заключаемые служащими с фирмой. Даже при наличии соответствующих законов многие фирмы идут на то, чтобы подписывать контракты со своими служащими о неразглашении доверенных им секретов либо с момента установления трудовых отношений, либо когда сотрудник получает доступ к коммерческим секретам.

В условиях, когда правового регулирования охраны коммерческой тайны еще не существует, хотя кое-какие проекты уже разработаны, следует обусловить принятие на себя служащим фирмы, работающим по контракту, обязательства о неразглашении коммерческих секретов, при этом данный документ должен прямо предусматривать право работодателя расторгнуть трудовое соглашение (контракт) с сотрудником, нарушившим названное обязательство, а также принимать иные меры, предусмотренные законом.

В странах, где нормы права довольно детально регламентируют охрану коммерческой тайны, тем не менее, общеприняты типовые формы соглашений (контрактов) о ее неразглашении. Рассмотрим форму документа, рекомендованную по защите деловой информации.

Соглашение о неразглашении коммерческой тайны

Приступая к выполнению своих обязанностей в качестве служащего Компании, я понимаю, что получу доступ к информации, касающейся ее бизнеса. Я также понимаю, что во время работы будут заниматься анализом, составлением схем, таблиц, чертежей, докладов и других конфиденциальных документов, относящихся к делам Компании.

В связи с этим даю обязательство, что ни во время моей работы, ни после увольнения не буду обсуждать с кем-либо или раскрывать (за исключением случаев выполнения своих обязанностей в качестве служащего Компании) какую-либо информацию или коммерческие секреты, полученные или разработанные мною. Я также согласен с тем, что все аналитические разработки, схемы, чертежи, доклады и другие документы, подготовленные лично мною либо в сотрудничестве с другими служащими, являются собственностью Компании. Обязуюсь, что не буду сам и не позволю никому другому снимать копии или делать аннотации с вышеупомянутых документов.

Я подтверждаю, что не имею перед кем-либо никаких обязательств, которые входят в противоречие с настоящим Соглашением или ограничивают мою деятельность в Компании.

Дата
Подпись служащего *Подпись свидетеля*

Конечно, служащий фирмы, подписывая подобного рода документ, должен четко представлять, что конкретно из деловой информации и технологических разработок является тайной фирмы. Как раз по этой причине и считается обязательным требование о том, чтобы вся секретная информация была обособлена от остальных сведений, а документы, ее содержащие, носили соответствующий гриф.

Приведенный выше текст соглашения о сохранности коммерческой тайны, по мнению юристов, оставляет многие вопросы без ответа. На практике для охраны коммерческой тайны фирмы ее служащими как во время работы в ней, так и после увольнения, используются более детально проработанные соглашения. Важно, чтобы условия сохранения коммерческой тайны бывшим сотрудником фирмы были реальными по времени, оставляя ему возможность подыскать достойно оплачиваемую работу.

Использование контрактов о сохранении коммерческой тайны позволяет обеспечить формальную юридическую защиту коммерческой информации, к которой имеет или имел доступ персонал фирмы.

Однако коммерческие тайны полностью или частично могут стать известными деловым партнерам вашей фирмы в процессе обмена с ними необходимой для совместной работы информацией. Следовательно, они должны принять на себя обязательства по защите ваших коммерческих тайн, равно как и вы должны поступить таким же образом в отношении их. Это традиционная для делового мира практика, но и она должна подкрепляться письменными обязательствами.

Соглашение о сохранности коммерческой информации

Здесь и далее «Доверяющий» или Ваше имя, здесь и далее «Доверенный» желают рассмотреть возможность для чего необходимо, чтобы Доверенный имел доступ к информации о _____.

Эта информация составляет коммерческую тайну Доверяющего и раскрывается только в заранее оговоренных целях. Доверенный обязуется сохранять в секрете эту информацию и не использовать ее в других целях. Доверенный обязуется ознакомить под роспись с этим Соглашением всех своих сотрудников, которые получат доступ к данной информации. По окончании переговоров (или сотрудничества) Доверенный сразу же вернет все материалы, содержащие данную информацию, Доверяющему.

Это соглашение не относится к информации, законным владельцем которой является Доверенный, или информации, полученной им у третьих лиц.

Дата
Подписи

Готовя документы на приобретение каких-либо товаров или услуг, размещая заказы на них, следует в соответствующих соглашениях или договорах обязательно указать, что продавец (поставщик) обязуется содержать в секрете всю предоставленную ему в связи с данным заказом вашу информацию. По исполнении заказа все документы фирмы, содержащие секретную информацию, он обязуется возвратить во взаимообусловленные сроки.

Рекомендуется на документах с конфиденциальной информацией, адресуемой поставщикам фирмы, ставить штамп, который свидетельствовал бы о том, что изложенные в документе сведения являются частной собственностью фирмы и требуют соответствующей защиты и своевременного возвращения владельцу.

Соглашение о сохранении коммерческой информации следует подписать и с теми партнерами, которые предоставляют фирме разного рода сервисные услуги (ремонт оборудования, уборка помещений и т. п.).

Если фирма прибегает к услугам торговых посредников или нанимает торговый персонал, то и в этом случае единственной возможностью сохранения коммерческих секретов будет подписание с ними соответствующего контракта.

Нет иных путей для сохранения коммерческих секретов производимой (реализуемой) фирмой продукции (товаров) в общении с контрагентом, кроме как заключение соответствующего соглашения о сохранении коммерческой тайны. Такие сведения могут быть нужны ему, например, для того, чтобы оценить ваши возможности по наращиванию производства данного вида продукции (товара), и краткое соглашение о сохранении тайны заставит его беречь полученную информацию.

Таким же образом охраняются коммерческие тайны третьей стороны, в частности вашего поставщика.

Деловые партнеры могут высказать пожелание о предоставлении им всей коммерческой информации для оценки реального состояния ваших дел. На предварительной стадии обсуждения сделки следует воздерживаться от детального обсуждения вашей охраняемой информации. Это возможно лишь после подписания соглашения о сохранении тайны.

В целом же защита коммерческих тайн фирмы в общении с дружественными, лояльными лицами, или же занимающими по отношению к вашему бизнесу нейтральную позицию, осуществляется на ос-

нове заключения соответствующих соглашений, прямо предписанных в нормах права, либо так или иначе основанных на них.

Даже тщательно охраняемые тайны фирмы могут стать известны вашим конкурентам из обычных публикаций для широкой публики, если пустить это дело на самотек. Поэтому один из сотрудников должен предварительно просматривать готовящиеся к печати брошюры, рекламные объявления, пресс-релизы и иные материалы, предназначенные для симпозиумов, конгрессов, выставок, а также выступления, научные и иные публикации сотрудников вашей фирмы. Он должен руководствоваться простым, но достаточно эффективным правилом, суть которого состоит в том, чтобы в максимально возможной степени раздробить, разобщить по времени и по авторам ту строго охраняемую коммерческую- информацию, без которой невозможно опубликование упомянутых выше работ. Все это существенно препятствует сбору секретной информации о фирме конкурентами или недоброжелателями. Конечно, этот барьер преодолим, но лишь посредством очень больших затрат.

Трудно найти золотую середину между стремлением сохранить коммерческую тайну и желанием использовать в рекламных целях наиболее впечатляющие данные из строго охраняемой информации, особенно те из них, которые, несомненно, помогли бы расширить сбыт производимых товаров и услуг.

Рассмотрим теперь вопрос о том, где и как предприниматель может получить необходимые ему сведения о клиентах и конкурентах, дающие ему возможность нормально работать в условиях рыночной экономики. Известно, что обладание такими сведениями по суки своей есть один из элементов системы превентивных мер по борьбе с промышленным шпионажем.

В капиталистических странах сведения о клиентах принято считать не коммерческой тайной фирмы, а, скорее, ее капиталом. Поэтому список клиентов фирмы и иные сведения о них составляются, в первую очередь, усилиями руководителя и эта информация не доверяется даже его ближайшему окружению.

На каждого клиента фирмы накапливается информация, где отражаются его привычки, характерные черты поведения, его интересы в личной жизни, о предоставляемых ему фирмой привилегиях. Отражаются сведения о его требованиях к качеству и количеству товаров и услуг, какие режимы доставки товаров применялись, какова периодичность поставок, сведения об особенностях платы и иных специфических чертах контрактов с данным клиентом. Здесь отражаются те сведения, которые определяют прибыльность всей операции с ним, какие предполагаются объемы сделок, частота поставок.

Сведения о деятельности фирмы и ее руководителях собирают в различных экономических газетах и журналах, справочниках, выпытывают у биржевиков, покупают у частных детективов.

Осведомленность о наиболее выгодных клиентах конкурента дает шанс победить в состязании с ним, если вам удастся «переманить» его клиентуру. Здесь на первый план выступает персонифицированная информация о клиентах, сведения о симпатиях и антипатиях, об их привязанностях, дружеских связях в среде предпринимателей и их конкурентах, которые влияют на принятие ими решений о поддержке деловых отношений с вашей фирмой или об их прекращении.

Сбор информации о клиентах и конкурентах должен быть упорядочен самым тщательным образом, и эта информация должна находиться только у руководства фирмы.

Сотрудники фирмы, продвигающие на рынок ее продукцию, должны представить письменные отчеты о конкретных клиентах по каждому факту продаж. В этих отчетах должны быть отражены перспективы будущих сделок.

Если вашей фирме по силам затраты на содержащие аналитического отдела, изучающего конъюнктуру рынка, клиентов, конкурентов, то и в этом случае следует распределять такого рода конфиденциальную информацию среди сотрудников.

Документация об этом должна быть строго секретной, а персонал, работающий с ней, должно соблюдать правила обращения с секретными документами. Все служащие, работающие непосредственно с клиентами, должны дать письменные обязательства сохранять коммерческие тайны фирмы.

Аналитический отдел или отдел маркетинга, изучая клиентов, должен одновременно собирать и анализировать сведения о конкурентах. Для этого должна быть разработана программа действий каждого сотрудника отдела. Следует четко знать, какие сведения надо получить и где они концентрируются. Кто и каким образом может добыть эти сведения с наименьшими затратами. Какие трудности могут возникнуть при этом, и как их следует преодолевать. Обязательно следует фиксировать: где, когда и как получена данная информация, кем конкретно и что по ней сделано.

В наших условиях добывание достоверной информации о клиентах и конкурентах — предмет постоянной головной боли. Рынок, его информационные структуры — еще в стадии формирования, притом на самых первых ступенях. По этой причине решение проблемы, вероятнее всего, может осуществляться:

- собственными силами (создание отделов маркетинга, изучения спроса и т. п.);
- получением за плату нужной информации у тех коммерческих структур, которые ею располагают (банки, страховые компании, биржи-, частные детективные агентства и т. п.);
- обращением за помощью, разумеется, платной, к службам промышленной контрразведки, к частным сыскным агентствам и т. п.

Предприниматель осуществляет выбор сам, но в любом случае выбор этот потребуется сделать, потому что система превентивных мер, обеспечивающая безопасность фирмы, без исчерпывающей информации о ее клиентах и конкурентах существовать не может, а сама фирма в таких условиях обречена на проигрыш в конкурентной борьбе.

Добывая жизненно важную коммерческую информацию, не следует забывать, что ваши конкуренты озабочены тем же. Во Франции, например, за промышленными секретами охотятся десятки тысяч промышленных шпионов и на оплату их труда французские бизнесмены ежегодно тратят свыше одного миллиарда долларов .

Следует не забывать о работе с представителями средств массовой информации, тем более что наше законодательство никак не защищает предпринимателей от журналистов.

Исходя из Закона РФ от «О средствах массовой информации» от 27 декабря 1991 года, не допускается использование средств массовой информации «… для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну». Но! До настоящего времени наше законодательством не имеет толкового определения коммерческой тайны и поэтому не предписывает охранять ее кому бы то ни было, не говоря уже о журналистах, которых Закон о средствах массовой информации наделяет правом «искать, запрашивать получать и распространять информацию». (Ст. 47 Закона)

Кроме того, Закон о печати не предусматривает ответственности за возможность нанесения публикацией даже существенного имущественного вреда посредством разглашения коммерческих тайн предпринимателей.

На многих предприятиях промышленно развитых стран посетителям выдаются разовые карточки (пропуска) гостя, размещаемые на груди или на лацкане пиджака. Карточки окрашены в яркие цвета. Доступ в те или иные помещения фирмы определяются цветом гостевой карточки. Передвижение гостя, таким образом, контролируется не только сопровождающими его лицами, но и остальным персоналом фирмы.

Некоторые помещения в любом случае должны оставаться недоступными для посещения всеми без исключения посторонними лицами, а также сотрудниками фирмы, не допущенными к работе с ее секретами. Эти помещения — святая святых. К ним относятся хранилища секретных документов, комнаты для работы с ними, зал совещаний, определенные подразделения фирмы, такие как: отдел маркетинга, служба внутренней безопасности, аналитический отдел. Все эти помещения находятся в зоне безопасности, которая запретна для доступа посторонним лицам, строго охраняется и периодически проверяется на возможное наличие в ней технических средств промышленного шпионажа. Эта зона — объект особых забот для службы внутренней безопасности. Ее стерильность от электронных средств, предназначенных для промышленного шпионажа, во многом обеспечивает экономическую безопасность и конкурентноспособность фирмы, ее выживание в условиях рыночной экономики.

1.3. Специальные технические средства негласного получения информации

Нормативно-правовая база определяет рамки рынка специальных технических средств негласного получения информации, используемых для оперативно-розыскной деятельности (ОРД) уполномоченными государственными структурами. Между тем, существует необходимость упорядочения законодательства для легитимного удовлетворения потребностей в подобной технике в других разрешенных по закону видах деятельности, требующих проведения расследования и дознания методами негласного наблюдения.

Оперативно-розыскная деятельность, как специфическая, социально полезная и необходимая форма осуществления в обществе функций расследования и дознания уполномоченными на эту де-

ятельность законом структурами или учреждениями, существует с незапамятных времен. Как правило, она бывает закреплена той или иной совокупностью законодательных положений. В настоящее время мы переживаем обновление государственного регламентирования ОРД. В последнее десятилетие в России принят ряд законодательных актов, регулирующих эту деятельность применительно к новым общественным условиям. Наиболее существенным из них является Федеральный Закон Российской Федерации от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности». В ст.6 (Глава II) данного Закона содержится перечень оперативно-розыскных мероприятий, которые в совокупности определяют три основных метода сбора необходимой информации, а именно:

1. Гласные формы получения информации (опрос, привлечение экспертов, обследования и т. д.);

2. Проведение активных побуждающих действий (контролируемые поставки, оперативный эксперимент и т. д.);

3. Негласное наблюдение.

Проблема классификации техники, подпадающей под определение «специальное техническое средство, предназначенное (разработанное, приспособленное, запрограммированное) для негласного получения информации», смыкается с еще двумя незавершенными аспектами формирования нормативно-правовой базы в этой области. Во-первых, речь идет о необходимости разработки и утверждения межведомственного документа, согласованного Государственным Таможенным Комитетом и ФСБ России, и регулирующего порядок экспорта и импорта специальной техники данного назначения. Для таможенных органов это означает введение в определенные разделы Товарной Номенклатуры Внешней Экономической Деятельности (ТН ВЭД) дополнительных позиций и субпозиций, наличие экспертных органов и структур, проводящих оценку конкретных изделий, разработку формализованной разрешительной и сопроводительной документации и т. д. Во-вторых, необходим легитимный механизм создания, реализации и применения технических средств двойного назначения. Этот механизм, с одной стороны, мог бы сделать подконтрольным и прозрачным оборот данной продукции и существенно подорвать позиции черного рынка по удовлетворению спроса субъектов Закона о ЧДОД. С другой стороны, признание легитимности применения технических средств двойного назначения и соответствующего рынка их реализации послужило бы стимулирующим фактором для укрепления инфраструктуры производителей СТС НПИ, что, в конечном счете, создает более благоприятные условия и для технического оснащения правоохранительных органов, применяющих СТС.

При всех перечисленных выше недостатках действующая в настоящее время нормативно-правовая база, в основном, определила рамки, в которых может функционировать рынок специальных технических средств, предназначенных для применения в оперативно-розыскных мероприятиях с целью получения негласной информации. По имеющимся сведениям, Федеральной Службой Безопасности РФ разработаны проекты документов, направленных на совершенствование этих нормативных актов с учетом накопленного в 1997-98 г. г. опыта, и их следует ожидать в ближайшее время.

Практика толкования и применения понятий «специальная техника» и «специальные технические средства» в разных источниках информации и различных сферах деятельности чрезвычайно многообразна. Отнесение тех или иных средств к СТС негласного получения информации или к «технике двойного назначения» для негласного наблюдения должно осуществляться на основе четких принципов и целого ряда критериев.

Следует иметь в виду, что применение радиомикрофонов, лазерных и направленных микрофонов, траверсов, электронных стетоскопов и минивидеокамер организациями и частными лицами, не имеющими на это специальных полномочий, категорически запрещено и карается законом. (ст. 137 УК РФ).

Также запрещено применение для защиты информации скремблирующих устройств (шифраторов), шумогенераторов и разрядников без соответствующего разрешения компетентных органов.

Итак, что же относится к коммерческой тайне и требует защиты от утечки информации и ее похищения?

I. Деловая информация:

- финансовые сведения;
- данные о цене (стоимости) продукции и услуг, технологии;
- деловые планы и планы производства новой продукции;

- списки клиентов и продавцов, контракты, преференции и планы;
- информация о маркетинге;
- соглашения, предложения, квоты;
- списки персонала, организационные схемы и информация о сотрудниках (их характеристики).

II. Техническая информация:

- научно-исследовательские проекты;
- конструкторские разработки по производству какой-либо продукции и ее технические параметры;
- заявки на патенты;
- дизайн, эффективность и возможности производственных методов, оборудования и систем;
- информационный процесс;
- программное обеспечение ЭВМ;
- химическая формула.

Анализируя зарубежный опыт по созданию механизма защиты коммерческой тайны, можно выделить основные блоки, из которых он состоит:

- нормы права, направленные на защиту интересов ее владельцев;
- нормы, устанавливаемые руководством предприятия, фирмы и т. п. (приказы, распоряжения, инструкции);
- специальные структурные подразделения, обеспечивающие соблюдение этих норм (подразделение режима, службы безопасности и т. п.).

Все вышеперечисленное должно быть тесно связано между собой. Так, например, фирма может иметь самые совершенные правила и инструкции, касающиеся внутреннего порядка обращения с конфиденциальными материалами, но при отсутствии государственно-правового регулирования вряд ли сможет защитить свои секреты. Точно также вряд ли удастся сохранить секреты при наличии правого регулирования, но в отсутствие профессионалов, которые будут претворять нормы права и инструкции на практике. Ну, а не зная основных направлений защиты секретов, не удастся сохранить свою конфиденциальную информацию даже при наличии государственной поддержки и наличия специального структурного подразделения в штатном расписании.

Сегодня, когда полным ходом идет процесс становления новых хозяйственных форм и отношений, у предприятий возникают проблемы, связанные с необходимостью защиты собственной секретной информации.

2. Законодательство в области технической защиты информации

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации на конкретном объекте информатизации.

2.1. Нормативная база анализа защищенности

Наиболее значимыми нормативными документами в области информационной безопасности, определяющими критерии для оценки защищенности АС и требования, предъявляемые к механизмам защиты, являются:

1. Общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408)
2. Практические правила управления информационной безопасностью (Code of practice for Information security management/ISO 17799)

Кроме этого, в нашей стране первостепенное значение имеют Руководящие документы (РД) Гостехкомиссии России. В других странах их место занимают соответствующие национальные стандарты (там, где они есть).

ISO 15408: Common Criteria for Information Technology Security Evaluation

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее «Общие критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности АС, а также средств вычислительной техники (СВТ) «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость «Общих критериев» ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во второй части «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.

Третья часть «Общих критериев» содержит класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment.

Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

- Наличие побочных каналов утечки информации;
- Ошибки в конфигурации, либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние;
- Недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;

- Наличие уязвимостей («дыр») в средствах защиты информации, позволяющих пользователям получать НСД к информации в обход существующих механизмов защиты.

Соответствующие требования гарантированности оценки, содержатся в следующих четырех семействах требований:

- Семейство AVA_CCA: Covert Channel Analysis (Анализ каналов утечки информации)
- Семейство AVA_MSU: Misuse (Ошибки в конфигурации, либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние)
- Семейство AVA_SOF: Strength of TOE Security Functions (Стойкость функций безопасности, обеспечиваемая их реализацией)
- Семейство AVA_VLA: Vulnerability Analysis (Анализ уязвимостей)

При проведении работ по аудиту безопасности, перечисленные семейства требований могут использоваться в качестве руководства и критериев для анализа уязвимостей АС (СВТ).

ISO 17799: Code of Practice for Information Security Management

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. ISO 17799 является ни чем иным, как международной версией британского стандарта BS 7799.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

1. Практические правила разбиты на следующие 10 разделов:
1. Политика безопасности
2. Организация защиты
3. Классификация ресурсов и их контроль
4. Безопасность персонала
5. Физическая безопасность
6. Администрирование компьютерных систем и вычислительных сетей
7. Управление доступом
8. Разработка и сопровождение информационных систем
9. Планирование бесперебойной работы организации
10. Контроль выполнения требований политики безопасности

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.

При использовании некоторых из средств контроля, например, шифрования данных, могут потребоваться советы специалистов по безопасности и оценка рисков, чтобы определить, нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности, в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля, перечисленные ниже, представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например, обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью. Они служат в качестве основы для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

- документ о политике информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты;
- средства защиты от вирусов;
- планирование бесперебойной работы организации;
- контроль над копированием программного обеспечения, защищенного законом об авторском праве;
- защита документации организации;
- защита данных;
- контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

РД Гостехкомиссии России

В общем случае, в нашей стране, при решении задач защиты информации, должно обеспечиваться соблюдение следующих указов Президента, федеральных законов, постановлений Правительства Российской Федерации, РД Гостехкомиссии России и других нормативных документов:

- Доктрина информационной безопасности Российской Федерации;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ;
- Закон Российской Федерации «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ
- Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.
- Закон Российской Федерации «О связи» от 16.02.95 N 15-ФЗ;
- Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 N 3523-1;
- Закон Российской Федерации «Об участии в международном информационном обмене» от 04.07.96 N 85-ФЗ;
- Постановление Правительства РФ «О лицензировании отдельных видов деятельности» от 16.09.98г;
- Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г;
- ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении».
- Руководящий документ. «Положение по аттестации объектов информатизации по требованиям безопасности информации» (Утверждено Председателем Гостехкомиссии России 25.11.1994 г.);
- Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования к защите информации» (Гостехкомиссия России, 1997);
- «Положение о сертификации средств защиты информации по требованиям безопасности информации» (Постановление Правительства РФ № 608, 1995 г.);
- Руководящий документ. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.);
- Руководящий документ. «Концепция защиты средств вычислительной техники от НСД к информации» (Гостехкомиссия России, 1992 г.);
- Руководящий документ. «Защита от НСД к информации. Термины и определения» (Гостехкомиссия России, 1992 г.);
- Руководящий документ. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» (Гостехкомиссия России, 1992 г.);

- Руководящий документ. «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997 г.);
- Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» (Гостехкомиссия России, 1999 г.);
- Руководящий документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (Гостехкомиссия России, 2001г.)

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Наиболее значимые из них, определяющие критерии для оценки защищенности АС (СВТ) рассматриваются ниже.

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации.» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. (Основным «источником вдохновения» при разработке этого документа послужила знаменитая американская «Оранжевая книга»). Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий первый.

Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- первая группа содержит только один седьмой класс, к которому относят все СВТ не удовлетворяющие требованиям более высоких классов;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой содержит только первый класс.

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС — коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

РД «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации»

При анализе системы защиты внешнего периметра корпоративной сети, в качестве основных критериев целесообразно использовать РД «»СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ.

Всего выделяется пять показателей защищенности:
1. Управление доступом
2. Идентификация и аутентификация
3. Регистрация событий и оповещение
4. Контроль целостности
5. Восстановление работоспособности

На основании показателей защищенности определяется следующие пять классов защищенности МЭ:
1. Простейшие фильтрующие маршрутизаторы — 5 класс
2. Пакетные фильтры сетевого уровня — 4 класс
3. Простейшие МЭ прикладного уровня — 3 класс
4. МЭ базового уровня — 2 класс
5. Продвинутые МЭ — 1 класс

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию «Особой важности». Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки «совершенно секретной» информации и т. п.

2.2. Развитие отечественной нормативной базы в области технической защиты информации

В настоящее время описанные РД уже устарели и содержащаяся в них классификация АС, СВТ и МЭ не может признаваться состоятельной. Достаточно заметить, что классификация АС и СВТ, разрабатывалась без учета распределенной (сетевой) природы современных АС, а все современные коммерческие МЭ по своим возможностям существенно превосходят требования 1-го класса защищенности (за исключением требования по использованию сертифицированных криптографических алгоритмов).

Развитием нормативной базы в этом направлении является разработка «Профилей защиты» для различных классов СВТ, АС и МЭ на базе «Общих критериев». В настоящее время создано уже значительное количество англоязычных профилей защиты. Значительные усилия в этом направлении предпринимаются и в России под эгидой Гостехкомиссии России.

РД Гостехкомиссии России «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К), содержит достаточно полный набор требований и рекомендаций организационного уровня по защите речевой информации, информации, обрабатываемой средствами вычислительной техники, а также по защите информации при подключении к сетям общего пользования.

В документе рассматриваются, в том числе следующие вопросы:
- Защита информации на рабочих местах на базе автономных ПЭВМ;
- Защита информации при использовании съемных накопителей большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ;
- Защита информации в локальных вычислительных сетях;
- Защита информации при межсетевом взаимодействии;
- Защита информации при работе с системами управления базами данных.

СТР-К может использоваться при проведении аудита и аттестации безопасности АС для оценки полноты и правильности реализации организационных мер защиты информации в АС.

Аттестации АС и сертификация СВТ по требованиям безопасности информации, аудит и обследование безопасности, в отдельных случаях, предполагают использование помимо перечисленных, и других нормативных документов. Полный набор этих документов можно найти на официальном сайте ФСТЭК (см. Ссылки).

Одним из важнейших документов в области защиты информации с помощью технических средств является Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», извлечение из которого в силу важности приводимых положений приводим ниже.

Утверждено постановлением Совета Министров —
Правительства Российской Федерации
от 15 сентября 1993 г. № 912-51

Государственная Техническая комиссия при Президенте РФ

ПОЛОЖЕНИЕ

«О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения)

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее положение является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, в органах (аппаратах, администрациях) представительной, исполнительной и судебной властей Российской Федерации, республик в составе Российской Федерации, автономной области, автономных округов, краев, областей, городов Москвы и Санкт-Петербурга и в органах местного самоуправления (далее именуются — органы государственной власти), на предприятиях и в их объединениях, учреждениях и организациях независимо от их организационно-правовой формы и формы собственности (далее именуются — предприятия).

2. Положение определяет структуру государственной системы защиты информации в Российской Федерации, ее задачи и функции, основы организации защиты сведений, отнесенных в установленном порядке к государственной или служебной тайне, от иностранных технических разведок и от утечки по техническим каналам (далее именуется — защита информации).

3. Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации.

4. Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранными техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров — Правительством Российской Федерации.

5. Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности и осуществляется во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

6. Главными направлениями работ по защите информации являются:

- обеспечение эффективного управления системой защиты информации;
- определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;
- анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки информации, подлежащих защите;
- разработка организационно-технических мероприятий по защите информации и их реализация;
- организация и проведение контроля состояния защиты информации.

7. Основными организационно-техническими мероприятиями по защите информации являются:

- лицензирование деятельности предприятий в области защиты информации;
- аттестование объектов по выполнению требований обеспечения защиты информации при прове-

дении работ со сведениями соответствующей степени секретности;
- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;
- категорирование вооружений и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности государства;
- обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;
- оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории Российской Федерации;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;
- разработка средств защиты информации и контроля за ее эффективностью (специального и общего применения) и их использование;
- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

8. Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случае ее утечки, разрушения (уничтожения).

9. Проведение любых мероприятий и работ с использованием сведений, отнесенных к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

II. ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

10.Основные задачи государственной системы защиты информации:
- проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;
- исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения;
- принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации;
- анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;
- организация сил, создание средств защиты информации и контроля за ее эффективностью;
- контроль состояния защиты информации в органах государственной власти и на предприятиях.

18. Организация работ по защите информации на предприятиях осуществляется их руководителями.

В зависимости от объема работ по защите информации руководителем предприятия создается структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.

Подразделения по защите информации (штатные специалисты) на предприятиях осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной или служебной тайне, определяют совместно с заказчиком работ основные направления комплексной защиты информации, участвуют в согласовании технических (тактико-технических) заданий на проведение работ, дают заключение о возможности проведения работ с информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю предприятия или его заместителю. Работники этих подразделений (штатные специалисты) приравниваются по оплате труда к соответствующим категориям работников основных структурных подразделений.

Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации.

19. Предприятия, имеющие намерения заниматься деятельностью в области защиты информации, должны получить соответствующую лицензию на определенный вид этой деятельности. Лицензии выдаются Гостехкомиссией России и Федеральным агентством правительственной связи и информации в соответствии со своей компетенцией по представлению органа государственной власти.

20. Высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации осуществляют:

- первичную подготовку специалистов по комплексной защите информации;
- переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;
- усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

Подготовка кадров для государственной системы защиты информации осуществляется при методическом руководстве Гостехкомиссии России.

III.ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ И СРЕДСТВАХ ИНФОРМАТИЗАЦИИ И СВЯЗИ

21. Защита информации в системах и средствах информатизации и связи является составной частью работ по их созданию, эксплуатации и осуществляется во всех органах государственной власти и на предприятиях, располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

22. Требования по защите информации в системах и средствах информатизации и связи определяются заказчиками совместно с разработчиками на стадии подготовки и согласования решений Совета Министров-Правительства РФ, приказов и директив, планов и программ работ, технических и тактико-технических заданий на проведение исследований, разработку (модернизацию),испытания, производство и эксплуатацию (применение) на основе стандартов, нормативно-технических и методических документов, утверждаемых Комитетом РФ по стандартизации, метрологии и сертификации, Государственной технической комиссией при президенте РФ и другими органами государственной власти в соответствии с их компетенцией. Указанные требования согласовываются с подразделениями по защите информации.

23. Организация защиты информации в системах и средствах информатизации и связи возлагается на руководителей органов государственной власти и предприятий, заказчиков и разработчиков систем и средств информатизации и связи, руководителей подразделений, эксплуатирующих эти системы и средства, а ответственность за обеспечение защиты информации — непосредственно на пользователя (потребителя) информации.

24. В интересах обеспечения защиты информации в системах и средствах информатизации и связи ЗАЩИТЕ ПОДЛЕЖАТ:

- информационные ресурсы, содержащие сведения, отнесенные к государственной или служебной тайне, представленные в виде носителей на магнитной и оптической основе, информативных физических полей, информационных массивов и баз данных;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы),программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации, содержащей сведения, отнесенные к государственной или служебной тайне;
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для ведения секретных переговоров.

25. Целями защиты информации являются:

- предотвращение утечки информации по техническим каналам;
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах ее обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

26. Защита информации осуществляется путем:

- предотвращения перехвата техническими средствами информации, передаваемой по каналам связи;
- предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;
- исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);
- предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата техническими средствами информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранирования зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации достигается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы),организацией системы контроля безопасности программного обеспечения.

Выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращения перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

27. Информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности, по результатам сертификационных испытаний, или предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

Для оценки готовности систем и средств информатизации и связи к обработке (передаче) информации, содержащей сведения, отнесенные к государственной или служебной тайне, проводится аттестование указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

VI. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

47. Контроль состояния защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки защиты ее от иностранных технических разведок.

Контроль заключается в проверке выполнения актов законодательства РФ по вопросам защиты информации, решений Государственной технической комиссии при Президенте РФ, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

48. Контроль организуется Гостехкомиссией России, Министерством безопасности Российской Федерации, Министерством внутренних дел РФ, Министерством обороны РФ, Службой внешней разведки РФ, Федеральным агентством правительственной связи и информации при Президенте РФ, структурными и межотраслевыми подразделениями органов государственной власти, входящими в государственную систему защиты информации, и предприятиями в соответствии с их компетенцией.

Акты проверок предприятий рассылаются в орган, проводивший проверку, и в орган государственной власти по подчиненности предприятия.

49. Гостехкомиссия России организует контроль силами центрального аппарата и подчиненных ей в специальном отношении специальных центров. Она может привлекать для этих целей подразделения по защите информации органов государственной власти.

Центральный аппарат Гостехкомиссии России осуществляет в пределах своей компетенции контроль в органах государственной власти и на предприятиях, обеспечивает методическое руководство работами по контролю (за исключением объектов и технических средств, защита которых входит в компетенцию МО РФ, МВД РФ, ФСК РФ, СВР РФ, ФАПСИ, Главного управления охраны Российской Федерации).

Специальные центры, подчиненные в специальном отношении Государственной технической комиссии при Президенте РФ, в пределах своей компетенции осуществляют контроль в органах государственной власти и на предприятиях, расположенных в зонах ответственности этих центров.

Контроль в органах государственной власти силами центрального аппарата Государственной технической комиссии при Президенте РФ и специальных центров, подчиненных в специальном отношении Государственной технической комиссии при Президенте РФ, осуществляется по согласованию с соответствующими органами государственной власти.

50. Органы государственной власти организуют и осуществляют контроль на подчиненных им предприятиях через свои подразделения по защите информации. Повседневный контроль за состоянием защиты информации на предприятиях проводится силами их подразделений по защите информации.

51. Контроль на предприятиях негосударственного сектора при выполнении работ с использованием сведений, отнесенных к государственной или служебной тайне, осуществляется органами государственной власти, Гостехкомиссией России, ФСК РФ, ФАПСИ и заказчиком работ в соответствии с их компетенцией.

52. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

НАРУШЕНИЯ по степени важности делятся на ТРИ КАТЕГОРИИ:

- ПЕРВАЯ — невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;
- ВТОРАЯ — невыполнение требований по защите информации, в результате чего создаются предпосылки для ее утечки по техническим каналам;
- ТРЕТЬЯ — невыполнение других требований по защите информации.

53. При обнаружении нарушений первой категории руководители органов государственной власти и предприятий обязаны:

- немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения и принять меры по их устранению;
- организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;
- сообщить в Государственную техническую комиссию при Президенте РФ, руководству органа государственной власти, федеральному органу государственной безопасности и заказчику о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер, проводимой Государственной технической комиссией при Президенте РФ или по ее поручению подразделениями по защите информации органов государственной власти.

При обнаружении нарушений второй и третьей категорий руководители проверяемых органов государственной власти и предприятий должны принять меры по их устранению в сроки, согласованные с органом, проводившим проверку, или заказчиком (представителем заказчика). Контроль за устранением этих нарушений осуществляется подразделениями по защите информации этих органов государственной власти и предприятий.

54....

Допуск представителей центрального аппарата Государственной технической комиссии при Президенте Российской Федерации, специальных центров, подчиненных ей в специальном отношении, на объекты для проведения контроля состояния защиты информации, доступ их к работам и документам, необходимым для проведения контроля, осуществляется в установленном порядке по предъяв-

лении специального удостоверения представителя Государственной технической комиссии при Президенте РФ и предписания на право проведения проверки данного объекта. Допуск на военные объекты осуществляется по разрешению начальника Генерального штаба Вооруженных Сил Российской Федерации.

Предписания на право проверки состояния защиты информации выдаются:

- для объектов органов государственной власти — председателем Государственной технической комиссии при Президенте РФ (заместителем председателя);
- для предприятий по всей территории РФ — начальником инспекции Государственной технической комиссии при Президенте РФ;
- для предприятий в пределах установленных зон ответственности — начальниками специальных центров, подчиненных в специальном отношении Государственной технической комиссии при Президенте РФ;
- для подведомственных предприятий — руководителями органов государственной власти.

VII. ФИНАНСИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

55. Финансирование мероприятий по защите информации, содержащей сведения, отнесенные к государственной или служебной тайне, а также подразделений по защите информации в органах государственной власти и на бюджетных предприятиях предусматривается в сметах расходов на их содержание.

56.Создание технических средств защиты информации, не требующие капитальные вложения, осуществляется в пределах средств, выделяемых заказчиками на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции. Расходы по разработке технических средств защиты включается стоимость разработки образца продукции.

Создание технических средств защиты информации, требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчикам на строительство сооружения или объектов.

оглавление
1
2
3
4
5
6
7
8

3. Особенности несанкционированного получения информации техническими средствами

3.1. Понятие уязвимости информации

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения. Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть:

1. [A] объективными
2. [B] субъективными
3. [C] случайными.

1. Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами защиты информации. К ним можно отнести:

[A.I] сопутствующие техническим средствам излучения

- [A.I.a] электромагнитные (побочные излучения элементов технических средств [1], кабельных линий технических средств [2], излучения на частотах работы генераторов [3], на частотах самовозбуждения усилителей [4])
- [A.I.b] электрические (наводки электромагнитных излучений на линии и проводники [1], просачивание сигналов в цепи электропитания, в цепи заземления [2], неравномерность потребления тока электропитания [3])

  * [A.I.c] звуковые (акустические [1], виброакустические [2])

  [A.II] активизируемые
- [A.II.a] аппаратные закладки (устанавливаемые в телефонные линии [1], в сети электропитания [2], в помещениях [3], в технических средствах [4])
- [A.II.b] программные закладки (вредоносные программы [1], технологические выходы из программ [2], нелегальные копии ПО [3])

[A.III] определяемые особенностями элементов

- [A.III.a] элементы, обладающие электроакустическими преобразованиями (телефонные аппараты [1], громкоговорители и микрофоны [2], катушки индуктивности [3], дроссели [4], трансформаторы и пр. [5])
- [A.III.b] элементы, подверженные воздействию электромагнитного поля (магнитные носители [1], микросхемы [2], нелинейные элементы, поверженные ВЧ навязыванию [3])

  [A.IV] определяемые особенностями защищаемого объекта
- [A.IV.a] местоположением объекта (отсутствие контролируемой зоны [1], наличие прямой видимости объектов [2], удаленных и мобильных элементов объекта [3], вибрирующих отражающих поверхностей [4])

- [A.IV.b] организацией каналов обмена информацией (использование радиоканалов [1], глобальных информационных сетей [2], арендуемых каналов [3])

2. Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами:

[B.I] ошибки
- [B.I.a] при подготовке и использовании программного обеспечения (при разработке алгоритмов и программного обеспечения [1], инсталляции и загрузке программного обеспечения [2], эксплуатации программного обеспечения [3], вводе данных [4])
- [B.I.b] при управлении сложными системами (при использовании возможностей самообучения систем [1], настройке сервисов универсальных систем [2], организации управления потоками обмена информации [3])
- [B.I.c] при эксплуатации технических средств (при включении/выключении технических средств [1], использовании технических средств охраны [2], использовании средств обмена информацией [3])

[B.II] нарушения
- [B.II.a] режима охраны и защиты (доступа на объект [1], доступа к техническим средствам [2])
- [B.II.b] режима эксплуатации технических средств (энергообеспечения [1], жизнеобеспечения [2])
- [B.II.c] режима использования информации (обработки и обмена информацией [1], хранения и уничтожения носителей информации [2], уничтожения производственных отходов и брака [3])
- [B.II.d] режима конфиденциальности (сотрудниками в нерабочее время [1], уволенными сотрудниками [2]).

3. Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности:

[C.I] сбои и отказы
- [C.I.a] отказы и неисправности технических средств (обрабатывающих информацию [1], обеспечивающих работоспособность средств обработки информации [2], обеспечивающих охрану и контроль доступа [3])
- [C.I.b] старение и размагничивание носителей информации (дискет и съемных носителей [1], жестких дисков [2], элементов микросхем [3], кабелей и соединительных линий [4])
- [C.I.c] сбои программного обеспечения (операционных систем и СУБД [1], прикладных программ [2], сервисных программ [3], антивирусных программ [4])
- [C.I.d] сбои электроснабжения (оборудования, обрабатывающего информацию [1], обеспечивающего и вспомогательного оборудования [2])

[C.II] повреждения
- [C.II.a] жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации [1], кондиционирования и вентиляции)
- [C.II.b] ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий [1], корпусов технологического оборудования [2])

Угрозы безопасности ИПО, от которых необходимо обеспечить защиту объектов, включают ***утечку*** информации, составляющую тайну вследствие использования нарушителем имеющихся уязвимостей (каналов утечки) и ***нежелательные воздействия*** на информацию и/или ее носитель исходящие из ИУ.

Возникновение и реализация угроз безопасности информации происходят при:
- возникновении условий, порождающих источники угроз безопасности информации;
- появлении потенциальных источников угроз;

- появлении реальных источников угроз (трансформация потенциальных источников угроз в реальные угрозы);
- возникновении факторов, способствующих реализации угрозы утечки информации, несанкционированных и/или непреднамеренных воздействий на информацию;
- реализации угрозы, т. е. наступлении события, заключающегося в утечке информации, несанкционированном и/или непреднамеренном воздействии на информацию;
- нанесении ущерба объекту защиты и/или другим объектам вследствие утечки информации, несанкционированных и/или непреднамеренных воздействий на информацию.

Таким образом, ***угроза*** реализуется в виде цепочки или сети условий и факторов (частных угроз) и их последствий. Возникшие последствия реализации частной угрозы, в свою очередь, также могут становиться угрозой, содержащей условия и факторы для возникновения более отдаленных негативных последствий.

Утечка информации может происходить по различным каналам в результате ее разглашения, добывания информации агентурной и технической разведками, несанкционированного доступа к информации.

Нежелательные воздействия на информацию и/или ее носитель подразделяются на воздействия несанкционированные (преднамеренные) и непреднамеренные, которые могут приводить к уничтожению, искажению, блокированию, подделке информации, хищению или утрате ее носителя. Защите от этих воздействий подлежит как информация, составляющая тайну, так и открытая информация. Угрозы утечки информации могут реализовываться субъектами, имеющими право на доступ к информации и не обладающими таким правом.

Нарушение безопасности данных в АС возможно как вследствие использования нарушителем каналов утечки данных, так и вследствие различных воздействий, в результате которых происходит уничтожение (модификация) данных или создаются каналы утечки данных (рис. 3.1).

Под ***каналом утечки данных*** в рассматриваемом случае будем понимать потенциальную возможность такого доступа к данным, которая обусловлена архитектурой и технологической схемой функционирования АС, а также существующей организацией работы с данными.

Каналы утечки данных в АС можно разделить на *косвенные* и *прямые*.

Косвенными называется такие каналы утечки данных, использование которых для НСД не требует непосредственного доступа к данным и техническим устройствам АС. Косвенные каналы утечки данных возникают вследствие:

- недостаточной звукоизоляции и светозащищенности помещений;
- недостаточной защищенности ТС АС от электромагнитных излучений;
- просчетов в организации применения морально-этических, законодательных и организационных методов и средств защиты информации.

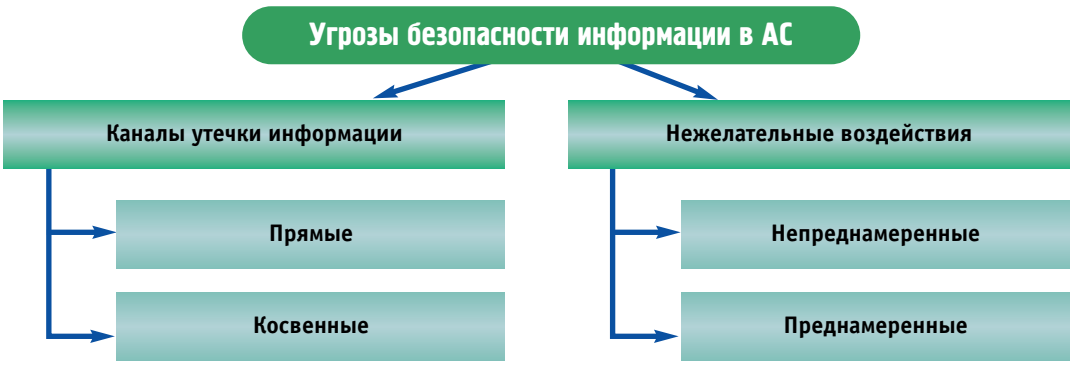


Рис. 3.1. Угрозы безопасности в АС

Прямые каналы утечки данных требуют непосредственного доступа к данным и техническим средствам АС и, в свою очередь, подразделяются на каналы утечки с модификацией данных и без модификации данных.

Наличие прямых каналов утечки данных обусловлено недостаточной защищенностью технических и программных средств АС, недостатками ОС, СУБД, языков программирования и другого математического обеспечения, а также просчетами в организации процесса работы с данными, недостатками законодательства и др.

Косвенные каналы утечки данных могут быть использованы нарушителем, если имеют место следующие стратегии:

- применение подслушивающих устройств;
- применение дистанционного фотографирования;
- перехват электромагнитных излучений;
- хищение носителей данных;
- хищение производственных отходов (перфолент, перфокарт, распечаток программ и т.д.).

Прямые каналы утечки данных позволяют нарушителю несанкционированно подключиться к аппаратуре и выполнить действия по анализу и модификации хранимых, обрабатываемых и передаваемых данных. Для воздействия на данные, а также в целях организации нормальной работы сети нарушитель может осуществить следующие действия:

- получить доступ к терминалу;
- работать за пользователя АС;
- подменить пользователя;
- подобрать пароль.

Нежелательные воздействия на АС можно подразделить на *преднамеренные* (несанкционированные) и *непреднамеренные*. Анализ опыта проектирования, изготовления и эксплуатации АС показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования АС. Причинами ***непреднамеренных*** воздействий при эксплуатации АС могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены следующими мотивами:

- недовольством служащего своей карьерой;
- сугубо материальным интересом;
- любопытством;
- конкурентной борьбой;
- шпионажем;
- стремлением самоутвердиться любой ценой и т.п.

По ***цели воздействия*** различают три основных типа угроз безопасности АС:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации.

- хищение (копирование) информации и средств её обработки;
- утрата (неумышленная потеря, утечка) информации.

При реализации этих угроз информация становится известной лицам, которые не должны иметь

к ней доступ. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе |ли передаваемой от одной системы к другой.

Угрозы нарушения целостности информации, хранящейся компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.

- модификация (искажение) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации — компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция некоторой базы данных).

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АС, либо блокируют доступ к некоторым ее ресурсам.

- блокирование информации;
- уничтожение информации и средств её обработки.

Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Нарушения конфиденциальности и целостности информации, а также доступности и целостности определенных компонентов и ресурсов АС могут быть вызваны различными опасными воздействиями на АС.

3.2. Особенности ведения компьютерной разведки и разведки ПЭМИН

Важно отметить, что технические средства не только сами излучают в пространство сигналы, содержащие обрабатываемую ими информацию, но и улавливают за счет микрофонов либо антенных свойств другие излучения (акустические, электромагнитные), существующие в непосредственной близости от них. Уловив, они преобразовывают принятые излучения в электрические сигналы и бесконтрольно передают их по своим линиям связи на значительные расстояния. Это еще больше повышает опасность утечки информации, К числу технических устройств, способных образовывать электрические каналы утечки относятся телефоны, датчики охранной и пожарной сигнализации, их линии, сеть электропроводки.

Если, работая на компьютере, вы одновременно включали телевизор, то, наверное, заметили, что при включенном компьютере на некоторых телевизионных каналах начинаются помехи. Этому есть простое объяснение. Все составляющие части компьютера — провода, усилители, даже печатные платы, — работают как антенны, проводящие электромагнитное излучение. Компьютер не только принимает излучение, но и передает, иногда перенося его на некоторое расстояние от источника, а близлежащая электропроводка и металлические трубки могут впоследствии работать как антенны.

Все компьютеры работают на излучение в широком радиочастотном диапазоне и представляют собой радиопередатчики. Когда телевидение принимает сигналы от компьютера, это происходит случайно; а теперь представьте себе, что кто-то решил целенаправленно принимать такую излучаемую информацию. Конечно же это возможно, и такие случаи бывали. Недаром компьютеры с наиболее засекреченной информацией устанавливают в комнатах с непроницаемыми для излучения стенами.

Рассмотрим это явление более подробно. Работа любой вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные проводные линии, цепи «питание» и «земля», возникающие вследствие электромагнитных воздействий в ближней зоне излучения. Считалось достаточно трудным делом расшифровать информацию, содержащуюся в излучении, и что

поэтому восстановление информации под силу только профессионалам, располагающим очень сложной и дорогой аппаратурой обнаружения и декодирования. Однако это оказалось не так.

Применение в компьютерах импульсных сигналов прямоугольной формы и высокочастотной коммутации приводит к тому, что в спектре излучений будут компоненты с частотами вплоть до СВЧ. Импульсы — вот ключевое слово. Всем известно, что компьютеры способны преобразовывать длинные строки нулей и единиц во что угодно (например, в наши любимые компьютерные игры). На самом деле, разумеется, по проводам не бегают крошечные нули и единички. По ним просто течет электрический ток различного напряжения, который наше воображение представляет как нули и единички. Любой электрический прибор является источником излучения. Но только цифровой прибор, такой, как компьютер, испускает импульсы высокого и низкого уровня напряжения. Энергетический спектр таких сигналов убывает с ростом частоты, но эффективность их излучения при этом увеличивается, и уровень излучений может оставаться постоянным до частот в несколько гигагерц. Усиление излучения на некоторых частотах спектра (резонансы) могут вызвать различные паразитные связи. Цепи, не предназначенные для передачи цифровых сигналов, могут излучать их вследствие наводок, например, провода источников питания.

Изображение на экране монитора компьютера формируется в основном так же, как и в телевизионном приемнике. Оно состоит из множества крошечных точек, называемых пикселями. Каждый пиксель представляет собой капельку определенного вещества, которая зажигается (флуоресцирует) под воздействием энергии, и покрыта защитным слоем. Контролирующая схема управляет позицией электронной пушки, которая периодически простреливает электронами весь экран, на короткое время зажигая те пиксели, которые должны засветиться. Каждый раз, когда это происходит, мы получаем импульс электромагнитного излучения с высоким напряжением. Поскольку видеосигнал является цифровым, то логическая единица создает светящуюся точку, а логический нуль препятствует ее появлению. Однако видеосигнал содержит еще и тактовые синхроимпульсы. Так как последние повторяются, то энергетический спектр видеосигнала содержит гармоники, интенсивность которых убывает с ростом частоты. Источниками излучения видеосигнала дисплея могут быть элементы обработки сигнала изображения и электронный луч кинескопа. Эти сигналы усиливаются до нескольких десятков вольт для подачи на электроннолучевую трубку.

Уровень широкополосного излучения дисплея зависит от числа букв на экране. Уровень узкополосных составляющих не зависит от заполнения экрана, а определяется системой синхронизации и частотой повторения светящихся точек. Поэтому бывает очень трудно, а подчас и невозможно отделить различные сигналы друг от друга и расшифровать их.

Информация, отображаемая на экране дисплея, может быть восстановлена с помощью телевизионного приемника, который обрабатывает лишь небольшую часть спектра сигнала шириной около 8 МГц (обычно ТВ-приемник имеет полосу пропускания 4,5 МГц и демодулятор сигнала с частично подавленной боковой полосой, эквивалентной АМ-детектору с полосой пропускания 8 МГц) на частотах в диапазонах метровых и дециметровых волн.

Пусть ТВ-приемник обрабатывает один «лепесток» энергетического спектра излучения, то есть частота его настройки совпадает с серединой одного из «лепестков», а полоса пропускания равна его ширине. Усиление НЧ-сигнала над порогом, определяющим уровень яркости, задается уровнем контрастности. В первом приближении уровень контрастности определяет крутизну фронтов видеосигнала в приемнике. В отличие от дисплея максимум видеосигнала в ТВ-приемнике определяет уровень черного, а минимум определяет уровень белого. Таким образом, изображение на экране ТВ-приемника будет представлять собой копию изображения на экране дисплея, и состоять из черных букв на белом (или сером) фоне.

Если видеосигнал представляет собой длинный импульс, то лучше всего будут излучены в пространство его фронты, которые и дадут при приеме точки. Излучение дисплея, принимаемое ТВ-приемником, не содержит информации о синхросигнале, поэтому изображение на экране телевизора будет перемещаться в горизонтальном и в вертикальном направлениях. Качество приема может быть улучшено при использовании внешнего генератора синхросигналов. С такой приставкой к обычному телевизору можно восстановить информацию с дисплея почти любого типа при условии достаточно высокого уровня его излучения.

4. Выявление технических каналов утечки информации

4.1. Классификация каналов утечки информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Каналы утечки информации по физическим принципам можно классифицировать на следующие группы:

- акустические (включая и акустопреобразовательные);
- визуально-оптические (наблюдение, фотографирование);
- электромагнитные (в том числе магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, отходы и т.п.).

4.2. Физические принципы возникновения каналов утечки информации

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные излучения, которые в той или иной степени связаны с обрабатываемой информацией.

Физические явления, лежащие в основе появления этих излучений, имеют различный характер, но тем не менее они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторой «побочной системе связи», образованной источником опасного излучения, средой и, возможно, приемной стороной (злоумышленником). При этом в отличие от традиционных систем связи, в которых передающая и приемная стороны преследуют одну цель — передать и принять информацию с наибольшей достоверностью, в случае побочной системы связи, «передающая сторона» заинтересована в максимально возможном ухудшении (ослаблении, ликвидации) передачи информации.

Побочную систему связи принято называть техническим каналом утечки информации.

Правомерно предполагать, что образованию каналов утечки информации способствуют определенные обстоятельства и причины технического характера. К последним можно отнести несовершенство схемных решений (конструктивных и технологических), принятых для данной категории технических средств, и эксплуатационный износ элементов изделия (изменение параметров элементов, аварийный выход/вывод из строя).

В любых технических средствах существуют те или иные физические преобразователи, выполняющие соответствующие им функции, основанные на определенном физическом принципе действия. Хорошие знания всех типов физических преобразователей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих каналы утечки информации.

Преобразователем вообще является прибор, который преобразует изменения одной физической величины в изменения другой. Преобразователь обычно определяется как прибор, преобразующий неэлектрическую величину в электрический сигнал, и наоборот.

Примером конкретной реализации преобразователей является звукоусилительная система, в которой микрофон (входной преобразователь) превращает звук (воздействующую физическую величину) в электрический сигнал. Последний передается и усиливается усилителем низкой (звуковой) частоты (преобразователь по мощности), а затем поступает на громкоговоритель (выходной преобразователь), воспроизводящий звук существенно более громкий, нежели тот, который воспринимается микрофоном.

Каждый преобразователь действует на определенных физических принципах и образует присущий этим принципам побочный канал передачи информации — канал утечки.

Функции приборов и устройств электросвязи можно разделить на два основных вида: обработку электрических сигналов и преобразование какого-либо внешнего физического воздействия в электрические сигналы. Во втором случае основную роль выполняют датчики и преобразователи.

Многообразные эффекты внешнего мира не ограничиваются в своих проявлениях лишь электрическими сигналами. Многочисленны различные физические явления (например звук, свет, давление и т.д.), их можно насчитать десятки. Для преобразования информации о физических явлениях в форму электрического сигнала в электронных системах используются чувствительные устройства — датчики. Датчики являются началом любой электронной системы. Датчики — это источники электрического сигнала.

Существуют два вида датчиков:

- специально разработанные для целей создания необходимого электрического сигнала;
- случайные, являющиеся результатом несовершенства схемы или устройства.

По форме преобразования датчики могут быть разделены на датчики — преобразователи сигнала и датчики — преобразователи энергии. Например, если рассматриваются фотодатчики, то фотодиод преобразует энергию света в электрический сигнал, тогда как солнечный элемент преобразует энергию света в электроэнергию.

Итак, на преобразователь воздействуют определенные силы, в ответ на которые порождается определенная реакция.

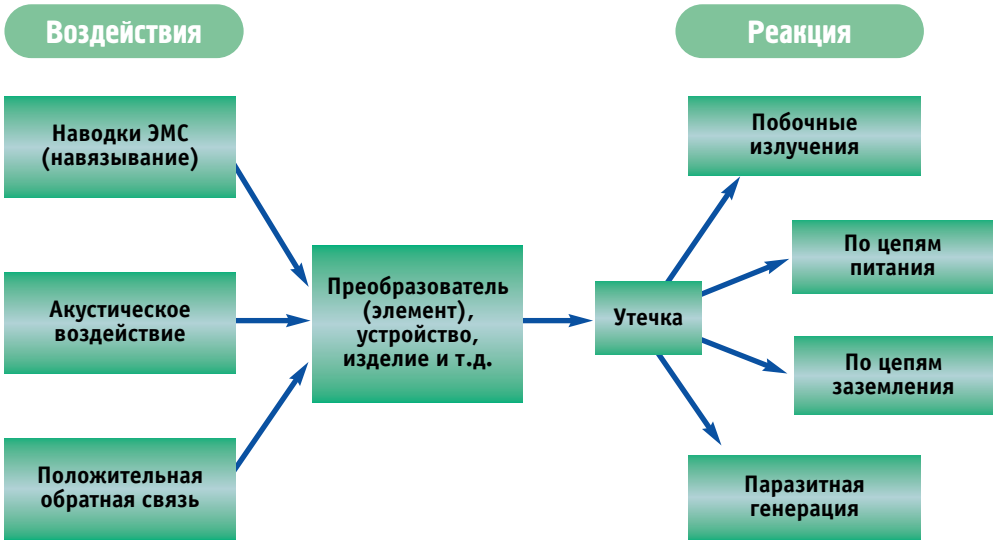


Рис. 4.1. Схема образования опасных сигналов

Любой преобразователь характеризуется определенными параметрами. Наиболее важными из них являются:

- ***чувствительность*** — отношение изменения выходного сигнала к изменению сигнала на его входе;
- ***разрешающая способность*** (характеризует наибольшую точность, с которой осуществляется преобразование);
- ***линейность*** (характеризует равномерность изменения выходного сигнала в зависимости от входного);
- ***инертность*** или время отклика, которое равно времени установления выходного сигнала в ответ на изменение входного сигнала;
- ***полоса частот*** (эта характеристика показывает, на каких частотах воздействия на входе еще воспринимаются преобразователем, создавая на выходе допустимый уровень сигнала).

По физической природе имеется значительное количество различных первичных преобразователей, среди которых выделяются такие группы как фотоэлектрические, термоэлектрические, пьезоэлектрические, электромагнитные и акустоэлектрические преобразователи, широко использующиеся в современных системах связи, управления и обработки информации.

Помимо преобразователей источниками каналов утечки информации могут быть различного рода излучатели электромагнитных колебаний, а также паразитные связи и наводки по электрическим и электромагнитным полям.

Таким образом, основными источниками образования технических каналов утечки любой, в том числе конфиденциальной, информации являются:

- преобразователи физических величин;
- излучатели электромагнитных колебаний;
- паразитные связи и наводки на провода и элементы электронных устройств.

Каждую из этих групп в свою очередь можно декомпозировать по принципам преобразования или иным параметрам. Например, излучатели электромагнитных колебаний декомпозируются по диапазону частот на низкочастотные, высокочастотные и оптические.

Преобразователи могут быть классифицированы по принципам на индуктивные, емкостные, пьезоэлектрические и оптические. При этом по виду преобразования они могут быть и акустическими и электромагнитными.

Каналами утечки информации за счет побочных электромагнитных излучений и наводок могут быть:

- электромагнитные поля рассеивания технических средств;
- наличие связей между информационными цепями и различными токопроводящими средами (система заземления и сеть электропитания, цепи связи, находящиеся в том же кабеле, что и информационные сети, вспомогательные технические средства и системы, имеющие линии связи, расположенные в тех же помещениях, различные металлические трубопроводы, воздуховоды, металлоконструкции зданий и другие протяженные токопроводящие объекты).

Паразитные связи и наводки проявляются в виде обратной связи (наиболее характерна положительная обратная связь), утечки по цепям питания и заземления.

4.2.1. Акустический канал утечки информации

Акустический контроль помещения, автомобиля, непосредственно человека

При разговоре человек может и не догадываться, что все, что он произносит, может услышать и зафиксировать постороннее лицо:

- С помощью *закладных передающих устройств* («жучков»), назначением которых является передача акустической (разговорной речи и другой) информации по радиоканалу, оптическому каналу, сети электропитания, телефонной линии, строительным коммуникациям. Понятие «жучок» или закладное передающее устройство у многих на слуху. О том, какие разновидности этих устройств существуют, и как они применяются, смотрите дальше на этом сайте;
- С помощью *направленных микрофонов* — специальных устройств, позволяющих на расстоянии нескольких десятков метров прослушивать разговорную речь. Например, ведущие разговор люди могут и не догадываться, что стоящий около них человек с кейсом за 20 метров прослушивает и записывает все, что они произносят;
- С помощью *стетоскопов* — специальных электронных устройств, преобразующих вибрации строительных коммуникаций (стен, окон, батарей отопления и др.), возникающих от речевой информации, в электрические сигналы звука этой речевой информации, которые потом прослушиваются и записываются. Наглядный пример работы стетоскопа можно увидеть, приставив обычную кружку к стене верхней частью, а противоположную сторону — дно кружки к уху. При этом можно услышать произносимую речь за стеной, хотя качество будет неважным, ведь все таки это кружка, а не электронный стетоскоп;
- С помощью *лазерного или инфракрасного зондирования оконных стекол*. Этот способ не требует нахождения рядом с разведываемым объектом, и может вестись с больших расстояний. Например,

при ведении разговора в помещении, акустическая воздушная волна вызывает совершенно незначительную вибрацию стекол окон, промодулированную этим разговором. Если, с противоположного здания, либо какого другого сооружения, направить на эти стекла лазерный луч и принять его переотражение от этих стекол, то весь разговор можно прослушать и зафиксировать;

- С помощью перехвата акустических колебаний речевой информации через технические средства, обладающие свойствами *электроакустических преобразований*:
  - возможность использования «*микрофонного эффекта*» некоторых элементов технических средств, находящихся в месте обсуждения конфиденциальной информации: трансформаторы, катушки индуктивности вторичных электрочасов, звонки телефонных аппаратов, реле, громкоговорители и т.д., путем подключения спецаппаратуры к их соединительным линиям за пределами местонахождения этих средств;
  - возможность применения «*высокочастотного навязывания*», примером которого может служить тот факт, что если даже телефонный аппарат не используется (трубка на телефоне), вся произносимая информация около телефонного аппарата становиться известной за пределами того места, где стоит этот аппарат;
  - с помощью перехвата акустических сигналов путем приема и детектирования побочных электромагнитных излучений (ЭМИ) на частотах *высокочастотных генераторов* технических средств приема, обработки, хранения и передачи информации, модулированных информационным сигналом;
  - с помощью перехвата акустических сигналов путем «*высокочастотного облучения*» специальных полуактивных закладных устройств.

Акустические закладки

Для перехвата акустической (речевой) информации наряду с портативными диктофонами используются специальные миниатюрные электронные устройства перехвата акустической (речевой) информации, несанкционированно и скрытно устанавливаемые в помещениях или автомашинах и часто называемые акустическими закладками. Акустические закладки можно классифицировать по виду исполнения, месту установки, источнику питания, способу передачи информации и ее кодирования, способу управления и т.д.

Перехватываемая акустическими закладками информация может передаваться по радио или оптическому каналу, по электросети переменного тока, по соединительным линиям ВТСС (например, телефонной линии), а также по металлоконструкциям зданий, трубам систем отопления и водоснабжения и т.д.

Наиболее широко используются акустические закладки, передающие информацию по радиоканалу. Такие устройства часто называют радиозакладками.

Закладки могут быть выполнены в виде отдельного модуля обычно в форме параллелепипеда или закамуфлированы под предметы повседневного обихода: пепельницу, электронный калькулятор, электролампочку, зажигалку, наручные часы, авторучку, вазу, поясной ремень и т.п.

Современные технологии позволяют выполнить акустические закладки размером с рисовое зернышко и весом в несколько граммов. Однако дальность передачи информации с таких закладок составляет несколько десятков метров, а время работы несколько часов.

Акустические закладки могут быть установлены в интерьерах помещения, предметах повседневного обихода, радиоаппаратуре, розетках электросети и электрических приборах, технических средствах связи и их соединительных линиях и т.п. Они также могут быть скрыты в одежде и личных вещах агента, находящегося в помещении.

В зависимости от среды распространения акустических колебаний перехватываемых радиозакладками, последние можно подразделить на акустические радиозакладки и радиостетоскопы.

Акустические радиозакладки предназначены для перехвата акустических сигналов по воздушному каналу утечки информации. Чувствительным элементом в них является, как правило, электретный микрофон. Поэтому акустические радиозакладки иногда называют радиомикрофонами, но среди специалистов по разведке этот термин используется редко. Подобные средства позволяют улавливать негромкую речь на дальности 5…10 метров.

Радиостетоскопы (контактные микрофоны, конструкционно объединенные с микропередатчиками) перехватывают акустические сигналы по вибрационному каналу утечки информации. В качестве чувствительных элементов в них обычно используются пьезомикрофоны, электретные микрофоны или датчики акселерометрического типа.

Радиостетоскопы способны улавливать звуковые колебания через бетонные стены толщиной 0,3…0,5 м, а также через двери и оконные рамы.

Питание акустических закладок осуществляется от автономных источников питания (аккумуляторов, батарей), электросети переменного тока, телефонной сети, а также от источников питания радиоэлектронной аппаратуры, в которой они устанавливаются.

В зависимости от мощности излучения и типа источника питания время работы акустической закладки составляет от нескольких часов до нескольких суток и даже месяцев. Например, время работы серийно выпускаемой акустической закладки РК 260 при мощности излучения 7 мВт составляет при питании от двух батарей АА — 10 суток, а при использовании литиевой батареи — 70 суток. При электропитании от сети переменного тока или телефонной линии время работы не ограничено.

Большинство радиозакладок с автономными источниками питания имеют мощность излучения до 10 мВт и дальность передачи информации до100…200м.

Однако встречаются закладки с мощностью излучения в несколько десятков милливатт и дальностью передачи информации до 500…1000 м. Например, радиозакладка HKG-1173 при мощности излучения 20 мВт обеспечивает дальность передачи информации до 400 … 1000 м.

При использовании внешних источников питания (например, электросети или автомобильных аккумуляторов) мощность излучения может составлять более 100 мВт, что обеспечивает дальность передачи информации в несколько километров. Например, радиозакладка HKG-1452 при мощности излучения 200 мВт имеет дальность действия до 2…8 км.

В случае необходимости передачи информации на большие расстояния используются специальные ретрансляторы.

Технически можно выполнить закладку, передающую информацию практически в любом диапазоне радиоволн. Однако широкое распространение нашли закладки, работающие в УКВ диапазоне.

Для передачи информации в основном используются следующие диапазоны длин волн: VHF (метровый), UHF (дециметровый) и GHz (ГГц). Наиболее часто используются частоты: 88 … 108 МГц; 108 … 174 МГц; 400 … 512 МГц; 1100 … 1300 МГц. Однако не исключено использование и других поддиапазонов. Например, радиозакладка SIM-A-31T работает в диапазоне 10.5 ГГц. Выбор рабочей частоты закладки во многом определяет скрытность ее работы.

По способу стабилизации несущей частоты передатчика радиозакладки можно разделить на: нестабилизиованные, со схемотехнической и с кварцевой стабилизацией частоты.

Нестабилизированные радиозакладки используются в основном в метровом (VFM) диапазоне длин волн. Их можно изготовить в сверхминиатюрном виде, однако они имеют ряд существенных недостатков. К основному из них относится значительная нестабильность несущей частоты и в ряде случаев зависимость ее от внешних факторов. Например, частота излучения может изменяться при приближении к антенне закладки человека или металлического предмета.

Невысокая стабильность частоты приводит к необходимости использовать для приема информации приемники с автоматической подстройкой частоты или приемники со сравнительно большой полосой пропускания, что, конечно, приводит к уменьшению дальности передачи информации. К недостатку нестабилизированных радиозакладок можно также отнести сравнительно высокий уровень внеполосных электромагнитных излучений.

Наибольшей стабильностью частоты обладают радиозакладки с кварцевой стабилизацией, их часто называют кварцованные. Они практически не подвержены влиянию внешних факторов. Именно их используют в качестве носимых на теле. Радио-закладки с кварцевой стабилизацией частоты используются практически во всех диапазонах длин волн и обладают низким уровнем внеполосных излучений. В современных радиозакладках ослабление излучений на гармониках составляет 40…50 дБ.

Радиозакладки с кварцевой стабилизацией частоты по сравнению с нестабилизированными имеют большую дальность действия (при использовании специальных приемников), но конечно и большие размеры.

В передатчиках радиозакладок, как правило, осуществляется модуляция несущей частоты. Редко используются закладки с модуляцией сигнала промежуточной частоты или двойной модуляцией как, например, радиозакладка РК-1970-SS. Прием информации, передаваемой подобной закладкой, должен осуществляться на специальный приемник, что также увеличивает скрытность передачи информации. Попытка прослушать сигнал обычным приемником ни к чему не приведет — после детектирования будет слышен лишь шумоподобный сигнал.

В радиозакладках в основном используются простые сигналы с частотной широкополосной (WFM) и узкополосной (NFM) модуляцией частоты. При использовании широкополосной частотной модуляции ширина спектра излучаемого сигнала составляет 50… 120 кГц. Для использования узкополосной частотной модуляции необходима кварцевая стабилизация частоты передатчика, но при этом можно существенно сузить спектр передаваемого сигнала (до 6.. 12 кГц), а, следовательно, значительно увеличить дальность передачи информации при условии, что для приема будет использоваться специальный приемник. Например, радиозакладка РН-417 при использовании широкополосной частотной модуляции обеспечивает передачу информации на расстояние до 1000 м, а радиозакладка РН-417У при тех же параметрах, но при использовании узкополосной частотной модуляции — на расстояние до 1500 м.

Для повышения скрытности используются сложные сигналы (например, шумоподобные или с псевдослучайной перестройкой несущей частоты и т.п.) и различные способы кодирования информации.

Из способов кодирования наиболее часто применяется аналоговое скремблирование речевого сигнала, при котором изменяются характеристики речевого сигнала таким образом, что он становиться неразборчивым. Например, в радиозакладке РК-2010 S используется простая инверсия спектра с точкой инверсии 1.862 кГц, а в радиозакладках «Брусок-Л3Б ДУ», РК-1380-SS и РК-540-SS — сложная инверсия спектра сигнала.

Наиболее сложный способ кодирования речевой информации заключается в преобразовании ее в цифровой вид. К таким радиозакладкам относится, например, закладки РК-1195-SS, РК-2050 и РК-2080. В радиозакладках SIM-PR-9000T и РК-1970 осуществляется преобразование речевой информации в цифровой вид с последующим ее шифрованием по одному из алгоритмов.

Наиболее простые радиозакладки выпускаются без системы управления включением передатчика, т.е. работа на излучение (передача информации) начинается при подключении источника питания.

Для увеличения времени работы закладки оборудуются системой управления включением передатчика от голоса (система VAS или VOX). Иногда такую систему называют акустоматом. То есть закладка в обычном режиме (режиме дежурного приема) работает как приемник акустического сигнала, при этом потребляемый ток незначителен. При появлении в помещении источника акустического сигнала, например, при начале разговора, подается напряжение на передатчик, и он начинает работать на излучение, т.е. передавать информацию. При прекращении разговора, через определенное время (обычно несколько секунд), передатчик выключается (излучение исчезает) и закладка переходит в режим дежурного приема.

Использование системы VAS позволяет значительно (в несколько раз) увеличить время работы закладки.

Для повышения скрытности, а также увеличения времени работы современные радиозакладки оборудуются системой дистанционного управления.

Недостатком радиозакладок является возможность обнаружения их излучений специальным приемником контроля. С целью устранения этого недостатка разработаны закладные устройства, передающие информацию по оптическому каналу в инфракрасном, невидимом глазу диапазоне. Такие закладки иногда называют «инфракрасными». Инфракрасный передатчик преобразует акустические колебания в световые, используя при этом широтно-импульсную модуляцию. Для приема информации, передаваемой такими закладками, используются приемники оптического излучения. Дальность передачи информации для них составляет несколько сот метров. Например, инфракрасный передатчик STG-4403 обеспечивает передачу информации на расстояние до 500 м.

Направленные микрофоны

Если требуется организовать прослушивание разговоров в помещении, доступ в которое так же, как и доступ в соседние помещения, невозможен, то используются направленные микрофоны и лазерные акустические локационные системы.

Направленные микрофоны имеют коэффициент усиления более 70…90 дБ и позволяют прослушивать разговоры на расстоянии до 300…500 м (в условиях города — до 50…70 м).

В основном используются три вида направленных микрофонов: ***параболические*** (рефлекторные), ***трубчатые*** («микрофон-труба») и ***плоские*** (микрофонные решетки) микрофоны.

Параболический микрофон имеет параболический отражатель, в фокусе которого находится обычный высокочувствительный микрофон.

Наиболее простым по конструкции является направленный микрофон «Большое ухо», выпускаемый в ФРГ. Основой устройства является параболоид вращения диаметром 43 см, в фокусе которого помещен электретный микрофон, подключенный ко входу малошумящего усилителя низкой частоты, собранного на четырех операционных усилителях, конструктивно оформленных в одном корпусе интегральной микросхемы.

«Микрофон-труба» представляет собой трубчатую фазированную приемную акустическую антенну, нагруженную на высокочувствительный микрофон или решетку микрофонов, включенных последовательно.

Характерным представителем такого типа микрофонов является микрофон «Акустическое ружье». Микрофон имеет несколько десятков тонких трубок с длинами от нескольких сантиметров до метра и более. Эти трубы собирают в пучок: длинные в центре, короткие по наружной поверхности пучка. Концы трубок с одной стороны образуют плоский срез, входящий в предкапсюльный объем микрофона. Звуковые волны, приходящие к приемнику по осевому направлению, проходят в трубки и поступают в предкапсюльный объем в одинаковой фазе, и их амплитуды складываются арифметически. Звуковые волны, приходящие под углом к оси, оказываются сдвинутыми по фазе, так как трубки имеют разную длину. Следовательно, их суммарная амплитуда будет значительно меньше.

Дальность приемов сигналов подобных микрофонов может быть увеличена за счет использования большего числа трубчатых элементов.

«Микрофон-труба» может быть закамуфлирован под зонт или трость или выполнен в обычном исполнении.

Так называемые «плоские» направленные микрофоны появились сравнительно недавно и представляют собой акустическую антенную решетку, включающую несколько десятков микрофонов. Они могут встраиваться в стенку атташе-кейса или вообще носиться в виде жилета под рубашкой или пиджаком. Дальность их действия сравнительно ниже по отношению к первым двум типам направленных микрофонов и составляет 30…50 м.

Лазерные акустические системы

В том случае, когда требуется прослушать разговоры в закрытом помещении на значительном расстоянии, используются лазерные акустические локационные системы (ЛАЛС). На практике такие системы часто называют лазерными микрофонами.

ЛАЛС состоит из источника когерентного излучения (лазера) и приемника оптического излучения, оснащенного фокусирующей оптикой. Для обеспечения высокой механической устойчивости передатчика и приемника, что крайне необходимо для нормальной работы системы, последние устанавливаются на тревожных штативах. Передатчик и приемник переносятся в обычном портфеле-дипломате. Как правило, в таких системах используются лазеры, работающие в ближнем ИК (0,9…1,1 мкм), невидимом глазу диапазоне длин волн.

Принцип действия системы заключается в следующем. Передатчик осуществляет облучение наружного оконного стекла узким лазерным лучом. Приемник принимает рассеянное отраженное излучение, модулированное по амплитуде и фазе по закону изменения акустического (речевого) сигнала,

возникающего при ведении разговоров в контролируемом помещении. Принятый сигнал демодулируется, усиливается и прослушивается на головных телефонах или записывается на магнитофон.

Для улучшения разборчивости речи в приемнике используется специальное шумоподавляющее устройство.

Для наведения лазерного луча на цель совместно с передатчиком и приемником используются специальные устройства — визиры.

Данные системы наиболее эффективны для прослушивания разговоров в помещениях небольшого размера, которые по своим акустическим характеристикам близки к объемному резонатору Гельмгольца, когда все двери и окна помещения достаточно хорошо герметизированы. Эффективны они и для подслушивания разговоров, ведущихся в салонах автомашин.

Современные ЛАЛС позволяют снимать информацию не только с наружных, но и внутренних оконных стекол, зеркал, стеклянных дверей и других предметов. В ряде случаев оконные стекла скрытно обрабатывают специальным составом, увеличивающим коэффициент отражения лазерного излучения, а следовательно, и дальность разведки.

Лазерные акустические системы разведки имеют дальность действия при диффузном отражении до 100…300 м без специальной обработки стекол, до 500 м — при обработке (покрытии) стекол специальным материалом, значительно увеличивающим мощность диффузно отраженного от них лазерного излучения, и более километра — при установке на оконных стеклах специальных направленных отражателей (триппель-призм).

Средства акустической разведки могут использоваться не только для прослушивания и записи ведущихся разговоров, но и для перехвата акустических колебаний, возникающих при выводе на печать текста, например на принтере. Современные специальные комплексы обработки акустической информации позволяют восстановить текст, выводимый на печать по перехваченным акустическим излучениям.

Электроакустические технические каналы утечки информации

Такие каналы возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих «микрофонным эффектом», а также путем «высокочастотного навязывания». Наиболее чувствительными элементами радиоэлектронной аппаратуры к акустическим воздействиям являются катушки индуктивности и конденсаторы переменной емкости.

Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающих «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Физические преобразователи аудиоинформации

Индуктивные преобразователи

Если в поле постоянного магнита поместить катушку индуктивности (рамку) и вращать ее хотя бы под воздействием воздушного потока, то на ее выходе появится ЭДС индукции.

Воздушный поток переменной плотности возникает и при разговоре человека. Раз так, то можно ожидать, что в соответствии с разговором (под воздействием его воздушного потока) будет вращаться и катушка (рамка), что вызовет пропорционально изменяющуюся ЭДС индукции на ее концах. Так можно связать акустическое воздействие на провод в магнитном поле с возникающей ЭДС индукции на его концах. Это типичный пример из группы индукционных акустических преобразователей. Представителем этой группы является, например, электродинамический преобразователь (рис. 4.2).

Рассмотрим акустическое воздействие на катушку индуктивности с сердечником. Механизм и условия возникновения ЭДС индукции в такой катушке сводятся к следующему.

Под воздействием акустического давления появляется вибрация корпуса и обмотки катушки. Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению ЭДС

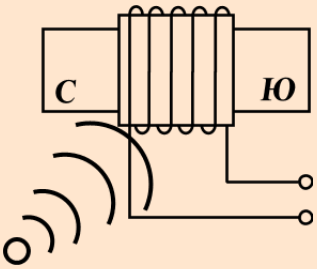


Рис. 4.2. Устройство электродинамического преобразователя

индукций на концах катушки

$$E = \frac{d}{dt}(\Phi_C + \Phi_B),$$

где Φ_C — магнитный поток, замыкающийся через сердечник; Φ_B — магнитный поток, замыкающийся через обмотки по воздуху. Она зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки.

Индуктивные преобразователи подразделяются на электромагнитные, электродинамические и магнитострикционные.

К электромагнитным преобразователям относятся такие устройства как громкоговорители, электрические звонки (в том числе и вызывные звонки телефонных аппаратов), электрорадиоизмерительные приборы.

Примером непосредственного использования этого эффекта для целей акустического преобразования является электродинамический микрофон (рис. 4.3).

ЭДС на выходе катушки определяется по формуле $E = -L\frac{di}{dt}$,

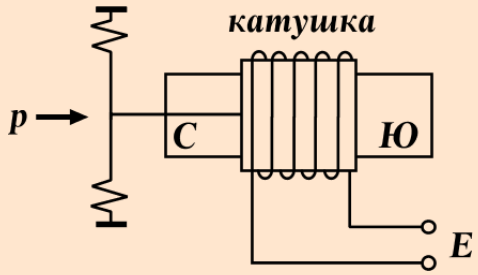


Рис. 4.3. Электродинамический микрофон

где $L = 4k\pi\mu_0\omega^2 S/l$ — индуктивность; k — коэффициент, зависящий от соотношения параметров; l — длина намотки катушки; (μ_0 — магнитная проницаемость; S — площадь поперечного сечения катушки; ω — число витков катушки.

Возникновение ЭДС на выходе такого преобразователя принято называть микрофонным эффектом. Можно утверждать, что микрофонный эффект может проявляться как в электродинамической, так и в электромагнитной, конденсаторной и других конструкциях, широко используемых в микрофонах самого различного назначения и исполнения.

Микрофонный эффект электромеханического звонка телефонного аппарата.

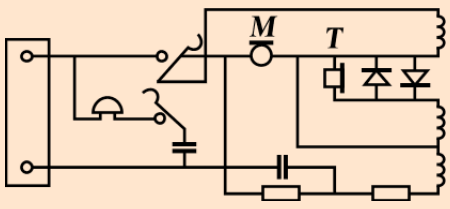


Рис. 4.4. Схема телефонного аппарата

Электромеханический вызывной звонок телефонного аппарата — типичный представитель индуктивного акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микротелефонной трубке. На рис. 4.4 приведена схема телефонного аппарата, а на рис. 4.5 — схема вызывного звонка.

ЭДС микрофонного эффекта звонка может быть определена по формуле

$$E_{M.Э} = \eta p,$$

где p — акустическое давление;

$\eta = FS\mu_0\omega S_M/d^2 Z_M$ — акустическая чувствительность звонка; здесь F — магнитодвижущая сила постоянного магнита; S — площадь якоря (пластины); μ_0 — магнитная проницаемость сердечника; ω — число витков катушки; S_M — площадь плоского наконечника; d — назначение зазора; Z_M — механическое сопротивление.

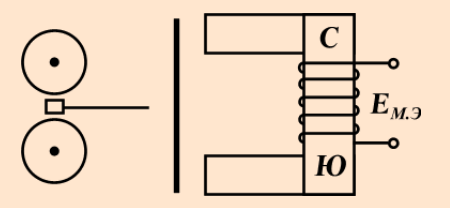


Рис. 4.5. Схема вызывного звонка

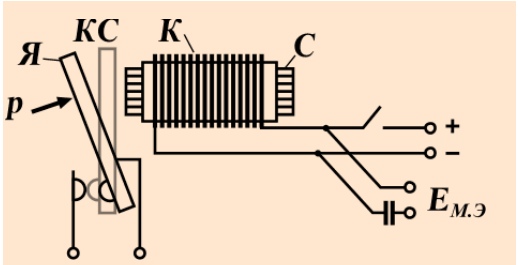


Рис. 4.6. Схема работы реле:
КС — контактная схема;
К — катушка; С — сердечник

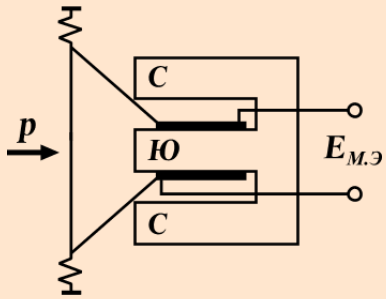


Рис. 4.7. Схема громкоговорителя

На таком же принципе (электромеханического вызывного звонка) образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения (рис. 4.6). Акустические колебания воздействуют на якорь реле. Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

Микрофонный эффект громкоговорителей.

Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию (2. . .3 мВ/Па) и довольно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов. Схема динамической головки представлена на рис. 4.7. ЭДС микрофонного эффекта динамической головки

$$E_{М.Э}=\eta p,$$

где $\eta=BLS/Z_M$ — акустическая чувствительность; здесь L — длина проводника, движущегося в магнитном поле с индукцией B; S — площадь поверхности, подверженной влиянию давления акустического поля; Z_M — механическое сопротивление.

Известно, что абонентские громкоговорители бывают однопрограммные и многопрограммные. В частности, у нас в стране находят достаточно широкое распространение трехпрограммные абонентские громкоговорители.

Трехпрограммные абонентские громкоговорители в соответствии с ГОСТ 18.286-88 (приемники трехпрограммные проводного вещания) имеют основной канал (НЧ) и каналы радиочастоты (ВЧ), включенные через усилитель-преобразователь. Усилитель-преобразователь обеспечивает преобразование ВЧ сигнала в НЧ сигнал с полосой 100…6400 Гц за счет использования встроенных гетеродинов. Так, например, в трехпрограммном громкоговорителе «Маяк-202» используются два гетеродина для второй и третьей программ ВЧ. Один вырабатывает частоту 78 кГц, другой 120 кГц.

Наличие сложной электронной схемы построения трехпрограммных громкоговорителей (обратные связи, взаимные переходы, гетеродины) способствует прямому проникновению сигнала, наведенного динамической головкой, на выход устройства (в линию). Не исключается и излучение наведенного сигнала на частотах гетеродинов (78 и 120 кГц).

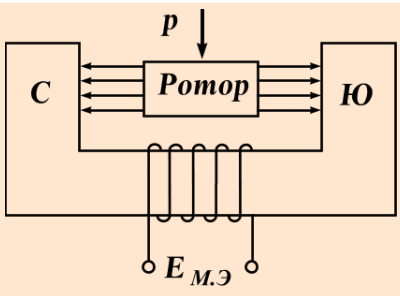


Рис. 4.8. Устройство шагового двигателя

Микрофонный эффект вторичных электрочасов.

Исполнительное устройство вторичных электрочасов представляет собой шаговый электродвигатель, управляемый трехсекундными разнополярными импульсами напряжением ±24 В, поступающими с интервалом 57 с от первичных электрочасов.

Микрофонный эффект вторичных часов, обусловленный акустическим эффектом шагового элек-

тродвигателя, проявляется в основном в интервалах ожидания импульсов управления. Схематически устройство шагового двигателя представлено на рис. 4.8.

Степень проявления микрофонного эффекта вторичных электрочасов существенно зависит от их конструкции: в пластмассовом, деревянном или металлическом корпусе; с открытым или закрытым механизмом; с жестким или «мягким» креплением.

Микрофонный эффект электроизмерительных приборов.

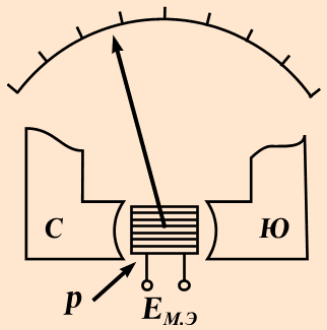


Рис. 4.9. Устройство магнитоэлектрического измерительного прибора

В магнитоэлектрическом измерительном приборе имеются неподвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита. Рамка соединена со стрелкой, конец которой перемещается по шкале измерения (рис. 4.9).

Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции.

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор. Различие между магнитоэлектрическим и электромагнитным приборами сводится к тому, что в электромагнитном приборе вместо постоянного магнита используется электромагнит.

Следует отметить, что ЭДС микрофонного эффекта возникает и может использоваться в состоянии покоя прибора, когда он не используется для конкретных измерений.

Микрофонный эффект трансформаторов.

Представителем индукционных акустоэлектрических преобразователей являются различные трансформаторы (повышающие, понижающие, входные, выходные, питания и др.).

Трансформатор состоит из замкнутого сердечника из мягкой стали или феррита, на котором имеются как минимум две изолированные друг от друга катушки (обмотки) с разными числами витков.

Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается в коэффициент трансформации раз.

Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается в коэффициент трансформации раз.

Магнитострикционные преобразователи.

Магнитострикция — изменение размеров и формы кристаллического тела при намагничивании — вызывается изменением энергетического состояния кристаллической решетки в магнитном поле, и, как следствие, расстояний между узлами решетки. Наибольших значений магнитострикция достигает в ферро- и ферритомагнетиках, в которых магнитное взаимодействие частиц особенно велико.

Обратное по отношению к магнитострикции явление — Виллари эффект — изменение намагничиваемости тела при его деформации. Виллари эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика, определяющей его намагниченность. В усилителях с очень большим коэффициентом усиления входной трансформатор на ферритах при определенных условиях вследствие магнитострикционного эффекта способен преобразовывать механические колебания в электрические.

Емкостные преобразователи.

Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения.

Для простейшего конденсатора, состоящего из двух пластин, разделенных слоем диэлектрика (воздух, парафин и др.), емкость определяется по формуле

$$C = \varepsilon S/d,$$

где ε — диэлектрическая проницаемость диэлектрика; S — площадь поверхности каждой пластины; d — расстояние между пластинами.

Из этого соотношения следует, что емкость конденсатора зависит от расстояния между пластинами. При наличии в цепи емкости постоянного источника тока и нагрузки воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости. Изменение емкости приводит к изменению сопротивления цепи и, соответственно, к изменению сопротивления и падению напряжения на сопротивлении нагрузки пропорционально акустическому давлению. Эти зависимости используются в конструкции конденсаторных микрофонов. Принципиальная схема конденсаторного микрофона приведена на рис. 4.10.

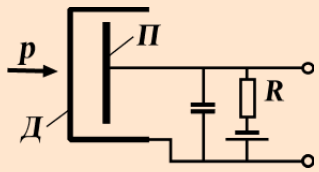


Рис. 4.10. Устройство конденсаторного микрофона

Когда на микрофон действует волна звукового давления p, диафрагма $Д$ движется относительно неподвижного электрода — жесткой пластины $П$. Это движение вызывает переменное изменение электрической емкости между диафрагмой и задней пластиной, а, следовательно, производит соответствующий электрический сигнал на выходе.

Конденсаторы переменной емкости с воздушным диэлектриком являются одним из основных элементов перестраиваемых колебательных контуров генераторных систем. Они устроены так, что система пластин вдвигается в другую систему пластин, образующих конденсатор переменной емкости. На такой конденсатор акустическое давление оказывается довольно просто, изменяя его емкость, а, следовательно, и характеристики устройства, в котором он установлен, приводя к появлению неконтролируемого канала утечки информации.

Пьезоэлектрический эффект

Изучение свойств твердых диэлектриков показало, что некоторые из них поляризуются не только с помощью электрического поля, но и в процессе деформации при механических воздействиях на них. Поляризация диэлектрика при механическом воздействии на него называется прямым пьезоэлектрическим эффектом. Этот эффект имеется у кристаллов кварца и у всех сегнетоэлектриков. Чтобы его наблюдать, из кристалла вырезают прямоугольный параллелепипед, грани которого должны быть ориентированы строго определенным образом относительно кристалла. При сдавливании параллелепипеда одна его грань заряжается положительно, а другая — отрицательно. Оказывается, что в этом случае плотность поляризованного заряда грани прямо пропорциональна давлению и не зависит от размеров параллелепипеда. Если сжатие заменить растяжением параллелепипеда, то заряды на его гранях изменяют знаки на обратные.

У ***пьезокристаллов*** наблюдается и обратное явление. Если пластину, вырезанную из пьезокристалла, поместить в электрическое поле, зарядив металлические обкладки, то она поляризуется и деформируется, например, сжимается. При перемене направления внешнего электрического поля сжатие пластинки сменяется ее растяжением (расширением). Такое явление называется обратным пьезоэлектрическим эффектом.

Чтобы воспринять изменение заряда или напряжения, к пьезоэлектрическому материалу подсоединяют две металлические пластины, которые фактически образуют пластины конденсатора, емкость которого определяется соотношением $C = Q/U$, где Q — заряд; U — напряжение.

На практике в качестве пьезоэлектрического материала применяются кристаллы кварца, рочелиевая соль, синтетические кристаллы (сульфат лития) и поляризованная керамика (титанат бария).

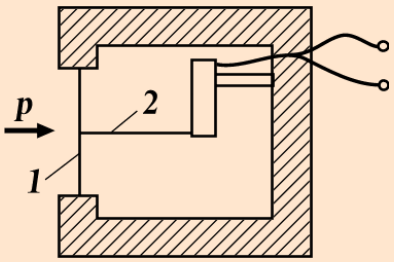


Рис. 4.11. Устройство пьезоэлектрического микрофона

Кварцевые пластины широко используются в пьезоэлектрических микрофонах, охранных датчиках, стабилизаторах генераторов незатухающих колебаний. На рис. 4.11 показано устройство пьезоэлектрического микрофона.

Когда звуковое давление *p* отклоняет диафрагму *1*, ее движение вызывает деформацию пьезоэлектрической пластины *2*, которая, в свою очередь, вырабатывает электрический сигнал на выходных контактах.

Оптические преобразователи

Здесь необходимо рассмотреть технический канал утечки информации, возникающий за счет того, что при ведении разговора, воздушная акустическая волна вызывает деформирование волоконных световодов, внутри которых происходит изменение интенсивности света, модулированное речью. За пределами помещения или здания эти изменения с помощью спецаппаратуры можно зафиксировать и преобразовать в акустические сигналы.

К оптическим преобразователям относятся приборы, преобразующие световую энергию в электрическую и обратно. Простейшим прибором этого типа является светодиод — прибор, излучающий свет при пропускании через *p-n* переход тока в прямом направлении. Обратный светодиоду прибор именуется фотодиодом. Фотодиод — это приемник оптического излучения, преобразующий его в электрические сигналы. Кроме того, фотодиод, преобразующий свет в электрическую энергию, выступает и как источник электрической энергии — солнечный элемент.

Более сложными оптическими преобразователями являются электронно-оптические преобразователи (ЭОП) и передающие телевизионные трубки различного исполнения (ПЗС, видиконы и пр.).

В плане технических каналов утечки информации в оптических системах опасным является акустооптический эффект. Акустооптический эффект — это явление преломления, отражения или рассеяния света, вызванный упругими деформациями стеклянных отражающих поверхностей или волоконно-оптических кабелей под воздействием звуковых колебаний.

Основным элементом оптического кабеля волоконно-оптических систем является волоконный световод в виде тонкого стеклянного волокна цилиндрической формы. Волоконный световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с различными оптическими характеристиками (показателями преломления n_1 и n_2). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки — создание лучших условий отражения на границе сердцевина-оболочка и защита от излучения в окружающее пространство.

Передача волны по световоду осуществляется за счет отражений ее от границы сердечника и оболочки, имеющих разные показатели преломления (n_1 и n_2). В отличие от обычных электрических проводов, в световодах нет двух проводников, и передача происходит волноводным методом в одном волноводе, за счет многократного отражения волны от границы раздела сред. Наибольшее распространение получили волоконные световоды двух типов: ступенчатые и градиентные.

В современных волоконно-оптических системах в процессе передачи информации используется модуляция источника света по амплитуде, интенсивности и поляризации.

Внешнее акустическое воздействие на волоконно-оптический кабель приводит к изменению его геометрических размеров (толщины), что вызывает изменение пути движения света, т.е. к изменению интенсивности, причем пропорционально значению этого давления.

Волоконные световоды как преобразователи механического давления в изменение интенсивности света являются источником утечки акустической информации за счет акустооптического (или акустоэлектрического) преобразования — микрофонного эффекта в волоконно-оптических системах передачи информации (используется также в охранных системах).

При слабом закреплении волокон в разъемном соединителе световодов проявляется акустический эффект модуляции света акустическими полями. Акустические волны вызывают смещение соединяемых концов световода относительно друг друга. Таким образом осуществляется амплитудная модуляция излучения, проходящего по волокну. Это свойство находит практическое применение в гидрофо-

нах с колеблющимися волоконными световодами. Глубина модуляции зависит от двух параметров, один из которых определяется конструкцией и свойствами волокна, а другой зависит от давления.

Чувствительность световода к давлению определяется значением соотношения

$Ч = \Delta\Phi/\Phi\Delta p$, где $\Delta\Phi$ — сдвиг фазы, вызываемый изменением давления Δp.

Параметрические каналы утечки информации

Параметрический канал утечки информации может образовываться за счет того, что проводимый в помещении разговор, а точнее воздушная акустическая волна этого разговора будет вызывать незначительное колебание элементов электромагнитных генераторов Вашей различной бытовой аппаратуры (приемники, музыкальные центры и т.д.). За счет этого будет изменяться и электромагнитное поле этих генераторов, по которому, если принять это электромагнитное поле на спецприемник, можно восстановить речевую информацию.

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого частотного спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Известно, что характер поля изменяется в зависимости от расстояния до передающего устройства. Оно делится на две зоны: ближнюю и дальнюю. Для ближней зоны расстояние r значительно меньше длины волны электромагнитного сигнала и поле имеет ярко выраженный магнитный (или электрический) характер, а в дальней поле носит явный электромагнитный характер и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами.

Коль скоро длина волны определяет расстояние, и, тем более назначение, устройство, принцип работы и другие характеристики, правомерно классифицировать излучатели электромагнитных сигналов на низкочастотные, высокочастотные и оптические.

Низкочастотные излучатели. Низкочастотными излучателями электромагнитных колебаний в основном являются звукоусилительные устройства различного функционального назначения и конструктивного исполнения. В ближней зоне таких устройств наиболее мощным выступает магнитное поле опасного сигнала. Такое поле усилительных систем достаточно просто обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот.

Высокочастотные излучатели. К группе высокочастотных (ВЧ) излучателей относятся ВЧ автогенераторы, модуляторы ВЧ колебаний и устройства, генерирующие паразитные ВЧ колебания по различным причинам и условиям. Источниками опасного сигнала выступают ВЧ генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы ЭВМ.

Модуляторы ВЧ колебаний как и элементы, обладающие нелинейными характеристиками (диоды, транзисторы, микросхемы), порождают нежелательные составляющие высокочастотного характера.

Довольно опасным источником высокочастотных колебаний могут быть усилители и другие активные элементы технических средств в режиме паразитной генерации за счет нежелательной положительной обратной связи.

Источниками излучения высокочастотных колебаний в различной радиотехнической аппаратуре являются встроенные в них генераторы, частота которых может быть промодулирована речевым сигналом. В результате воздействия акустического поля меняется давление на все элементы этих высокочастотных генераторов. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т. п., что может привести к изменениям параметров высокочастотного сигнала, в том числе и к модуляции его информационным сигналом. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а, следовательно, к изменению частоты излучения генератора, т.е. к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Поэтому этот канал утечки информации называется параметрическим. Встроенные генераторы (гетеродины) обязательно имеются в радиоприемниках, телевизорах, магнитофонах, трехпрограммных громкоговорителях и ряде электроизмерительных

приборов. К ним примыкает различные усилительные системы — усилители низкой частоты, системы звукоусиления, способные по тем или иным причинам войти в режим самовозбуждения (т.е. по существу стать неконтролируемым гетеродином).

Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки.

В качестве примера модуляции речью частоты автогенераторов можно рассмотреть микрофонный эффект гетеродинов радиоприемников бытового назначения. Основным элементом гетеродина радиоприемника является колебательный контур с конденсатором переменной емкости.

Период собственных колебаний гетеродина определяется условием равенства реактивных сопротивлений катушки индуктивности и конденсатора $X_L = X_C$. Частоту ω_0, при которой выполняется это равенство, называют собственной частотой колебательного контура. Ее значение определяется из выражения $\omega_0 = 1\sqrt{LC}$. Под воздействием акустического давления будет меняться расстояние между пластинами переменного воздушного конденсатора гетеродина. Изменение расстояния приведет к изменению емкости, последнее — к изменению частоты гетеродина по закону акустического давления (произойдет частотная модуляция частоты гетеродина акустическим сигналом).

Кроме конденсаторов, акустическому воздействию подвержены катушки индуктивности с поперечными сердечниками, монтажные провода значительной длины, в результате чего они также создают микрофонный эффект.

Практика показала, что акустическая реакция гетеродина возможна на расстоянии до нескольких метров, особенно в помещениях с хорошей акустикой. В зависимости от типа приемника прием такого сигнала возможен на значительном расстоянии, иногда достигающем 1...2 км.

Источником излучения высокочастотных колебаний в аппаратуре звукозаписи является генератор стирания-подмагничивания (ГСП), частота которого F может быть промодулирована речевым сигналом за счет нелинейных элементов в усилителе записи, а также из-за наличия общих цепей электропитания.

Параметрический канал утечки информации может быть реализован и путем «*высокочастотного облучения*» помещения, где установлены полуактивные закладные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического (речевого) сигнала.

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. А специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала. Подобного вида закладки иногда называют полуактивными.

Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленным излучением и приемник.

Канал утечки информации за счет «высокочастотного навязывания»

Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр.

Технический канал утечки информации путем «высокочастотного навязывания» может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии (цепи), имеющие функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несо-

гласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используется специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы.

4.2.2. Визуально-оптический канал утечки информации

Получение видовых характеристик объекта постоянно совершенствуется благодаря новой аппаратуре наблюдения (телевизионной, инфракрасной видовой, визуально-оптоэлектрической, фотографической) и ее расположения на различных носителях (корабль, автомобиль, самолет, спутник). Глаз человека является конечным прибором восприятия визуальной информации. Его возможности существенно повышаются за счет использования различных приборов наблюдения как в видимом диапазоне (бинокли, монокуляры, перископы, телескопы), так и приборов визуализации изображений объекта в ИК диапазоне, радиолокационных изображений, тепловых и рентгеновских изображений (приборов ночного видения, тепловизоров, рентгеновских аппаратов, РЛС бокового обзора и т. п.)

Объекты получения визуальной информации — самые разные, определяемые заказчиком информации, — от сцен неверности супругов, изображений новой техники и ее составных частей до глобального наблюдения за всей поверхностью Земли например, с целью получения данных по возможному урожаю этого года.

Для собственника информации (частное лицо, фирма, государство) ее потери могут иметь самые плачевные последствия. Так, например, проведенная на показе мод в Париже съемка новых моделей с целью определения реакции публики на «революционное изменение линии талии» привела к тому, что к моменту, когда французские модельеры повезли свою продукцию за океан, то они увидели там тысячи платьев, пошитых по их новым фасонам. И вместо планировавшихся барышей понесли огромные убытки.

Видовые характеристики объекта дают возможность описания и классификации обнаруживаемых объектов по форме и контурам, определение его деталей по снимку или наблюдаемым характеристикам.

Получение видовых характеристик объекта является результатом решения трех задач:

- обнаружение — это стадия зрительного восприятия, когда наблюдатель выделяет из окружающего фона объект, характер которого остается для него неясным;
- различение — когда наблюдатель способен определить крупные детали объекта, раздельно воспринимать два объекта, расположенные рядом;
- опознавание (идентификация) — когда наблюдатель, различая отдельные мелкие детали, выделяет существенные признаки объекта и может отличить этот объект от других, имеющихся в его поле зрения.

Видовые характеристики объектов наблюдения могут быть получены либо непосредственно в световом диапазоне, либо путем визуализации изображений в ИК диапазоне, радиолокационном диапазоне, за счет теплового излучения объектов.

Возможность образования визуального канала утечки информации зависит от определенных психофизиологических особенностей восприятия наблюдателем объекта, таких, как:

- угловые размеры объекта;
- уровни адаптационной яркости;
- контраст объект/фон;
- время восприятия;
- зашумленность изображения.

Любое изображение характеризуется яркостным контрастом K — прямым или обратным.

При прямом — яркость фона $B_ф$ больше яркости объекта B_o:

$K = (B_ф - B_o)/B_ф$ и при обратном:

$K = (B_o - B_ф)/B_o$

Контраст может выражаться в относительных единицах или процентах. Контраст до 20% рассматривается как малый, до 50 % — как средний и более 50 % — как высокий.

Оптимальным при длительном наблюдении является контраст изображения 85–90%. Минимальное значение K, при котором глаз различает объект (порог контрастной чувствительности), равен 2—3 % в случае, когда точно известно направление на объект, и 7–9 % при нефиксированном наблюдении.

Существенные ограничения могут быть наложены условиями временных характеристик восприятия, что связано с инерциальными свойствами зрения и имеет большое значение при наблюдении за движущимися объектами или объектами кратковременного попадания в поле зрения оператора. При таком наблюдении эффект кратковременности усиливается эффективной яркостью объекта, которая при коротких раздражениях может быть существенно меньше действительной яркости. В этом случае яркостный контраст движущегося объекта может быть существенно меньше неподвижного.

Определяющими при визуальных характеристиках являются также угловые размеры объекта наблюдения

$a = 2arctg\,(L/2I)$,

где L — линейный размер изображения объекта, а I — расстояние от глаза наблюдателя до плоскости наблюдения. Эти характеристики связаны с физиологическими данными наблюдателя.

Абсолютный порог обнаружения апор у большинства людей составляет 0,5" (тонкая черная линия на светлом фоне).

С этим показателем связан другой параметр наблюдения — острота зрения (разрешающая способность глаза), равная $1/a_{пор}$. Острота зрения зависит от расстояния между соседними светочувствительными элементами сетчатки глаза. Она максимальна в центральной части сетчатки (в углу зрения ~7°).

Диапазон яркостей фона и объекта, воспринимаемый глазом, весьма широк и лежит в пределах 10^{-7}– 10^{5} кд/м^2.

Однако следует учитывать, что этот диапазон в реальных условиях существенно зависит от средней яркости поля зрения — уровня адаптации. Так для высокого уровня адаптации (дневной свет) он равен 1000:1, а для низкого — 10:1. Переход от одного уровня адаптации к другому требует определенного времени, что необходимо учитывать, например, при перемещении наблюдателя из темного в освещенное (или наоборот) помещение.

Существенное влияние на получение визуальной информации оказывает состояние трассы наблюдения — от чистого воздуха до очень сильного тумана, соответствующее по метеорологическому коду от 10 до 0, что определяет метеорологическую дальность возможного обнаружения и наблюдения объектов.

Несмотря на эти ограничения возможности несанкционированного получения информации по визуально-оптическому каналу исключительно важны. Так, например, длиннофокусные фотоаппараты позволяют осуществлять съемку документов, расположенных на стене офиса или столе, на расстоянии до 5 км.

Телескоп РК 6500, выполненный по схеме Шмидта, позволяет опознать автомобиль на расстоянии 10 км. Приборы с электронной стабилизацией изображения позволяют вести наблюдение с рук из движущихся автомобилей и вертолетов.

На рынке технических средств разведки появились в большом количестве миниатюрные фотоаппараты в обычном исполнении и закамуфлированные под различные бытовые предметы — наручные часы, зажигалки и т. п., в т. ч. фотоаппараты с дистанционным управлением. Эти аппараты позволяют снимать копии с документов формата А4–А6 и позволяют переснимать до 800 документов.

Такое значительное количество технических средств получения визуальных характеристик объектов и носителей информации, располагаемых на различных носителях, начиная от пуговицы пиджака и заканчивая многотонными спутниками-шпионами, требует от специалистов применения комплекса защитных мероприятий по исключению возможности утечки видовой информации.

Появление и широкое практическое использование световодов позволило получить принципиально новые приборы визуального наблюдения. При их использовании приборы наблюдения отходят от традиционной схемы «линии зрения», то есть наблюдения только за теми объектами, которые находятся на линии зрения глаза или оптической оси прибора. Появилась возможность получения

информации из замкнутых помещений — зонд пропускается в замочную скважину или отверстие в стене, и его поворот обеспечивает визуальный обзор внутри помещения.

4.2.3. Электромагнитный канал утечки информации

Телефонный канал утечки информации

Использование телефонного канала утечки информации возможно по следующим направлениям:

- прослушивание телефонных переговоров;
- использование телефонного аппарата для подслушивания переговоров в помещении.

Подслушивание телефонных переговоров возможно:

- через гальванический съем телефонных переговоров (путем контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети). Определяется путем ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры.
- телефонно-локационный способом (путем высокочастотного навязывания). По телефонной линии подается высокочастотный тональный сигнал, который воздействует на нелинейные элементы телефонного аппарата (диоды, транзисторы, микросхемы), на которые также воздействует акустический сигнал. В результате в телефонной линии формируется высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала в телефонной линии. Возможное противодействие: подавление в телефонной линии высокочастотного сигнала.
- индуктивный и емкостной способ негласного съема телефонных переговоров (бесконтактное подключение).

Подслушивание разговоров в помещении с использованием телефонных аппаратов возможно в следующих случаях:

- низкочастотный и высокочастотный способ съема акустических сигналов и телефонных переговоров. Данный способ основан на подключении к телефонной линии подслушивающих устройств, которые преобразованные микрофоном звуковые сигналы передают по телефонной линии на высокой или низкой частоте. Позволяют прослушивать разговор как при поднятой, так и при опущенной телефонной трубке. Защита осуществляется путем отсекания в телефонной линии высокочастотной и низкочастотной составляющей
- использование телефонных дистанционных подслушивающих устройств. Данный способ основывается на установке дистанционного подслушивающего устройства в элементы абонентской телефонной сети путем параллельного подключения его к телефонной линии и дистанционным включением. Дистанционное телефонное подслушивающее устройство имеет два деконспирирующих свойства: в момент подслушивания телефонный аппарат абонента отключен от телефонной линии, а также при положенной телефонной трубке и включенном подслушивающем устройстве напряжение питания телефонной линии составляет менее 20 В, в то время как оно должно составлять 60.

Радиотелефонный канал утечки информации

В настоящее время системы защиты информации, которыми оснащены радиотелефоны (сотовые телефоны) ненадежны и не гарантированы от подслушивания, в связи с чем не рекомендуется вести конфиденциальные переговоры по сотовой связи. В стадии разработки подсистемы конфиденциальной сотовой связи с гарантированной стойкостью от прослушивания. Также рекомендуется отключать сотовые телефоны у себя и у клиентов при ведении конфиденциальных переговоров. Также необходимо учитывать, что при включенном радиотелефоне Вас всегда можно запеленговать и вычислить, так как радиотелефон всегда привязан к нескольким «сотам» и возможно осуществить пеленг местонахождения. В настоящее время наиболее защищенным является сотовая сеть «Сонет» (в ней применен цифровой стандарт SDMA)

Необходимо помнить, что в Уголовном кодексе предусмотрена ответственность за незаконное прослушивание телефонных переговоров, ограничивающаяся только штрафами.

Каналами утечки информации за счет побочных электромагнитных излучений и наводок могут быть:

- электромагнитные поля рассеивания технических средств;
- наличие связей между информационными цепями и различными токопроводящими средами (система заземления и сеть электропитания, цепи связи, находящиеся в том же кабеле, что и информационные сети, вспомогательные технические средства и системы, имеющие линии связи, расположенные в тех же помещениях, различные металлические трубопроводы, воздуховоды, металлоконструкции зданий и другие протяженные токопроводящие объекты).

Перехват компьютерной информации

Работая с информацией на компьютере, даже если он не подключен к Интернету, локальной вычислительной сети и к пр., Вы должны знать, что Ваша информация может быть полностью восстановлена и записана специальными приемными средствами, находясь как рядом от Вас, так и на определенном расстоянии за счет излучений от ПЭВМ (об излучениях мониторов наверное говорить не надо), наводок на посторонние проводники, выходящие из Вашей комнаты в неизвестное направление, а также на цепи электропитания и заземления (такая возможность есть у злоумышленников, подключившись спецаппаратурой к одной и той же сети электропитания 220В до общей трансформаторной подстанции, обеспечивающей электроэнергией Ваш дом).

Подытожив выше сказанное, необходимо сказать, что для того чтобы дистанционно считывать информацию с Вашего компьютера (ПЭВМ) у злоумышленников есть следующие способы:

- Прием побочных (паразитных) радиоизлучений компьютера:
  - излучений элементов ПЭВМ;
  - излучений на частотах работы высокочастотных (ВЧ) генераторов ПЭВМ;
- Прием наводок побочных радиоизлучений на посторонние проводники;
- Прием просочившихся информационных сигналов в цепи электропитания и заземления;
- Съем информации с использованием закладных устройств.

4.2.4. Материально-вещественный канал утечки информации

Во всех случаях защиты коммерческой тайны необходимо обратить особое внимание на документы, поскольку в нашей стране основные объемы коммерческой информации хранят в документах.

Руководитель должен упорядочить процессы фиксации конфиденциальной информации в деловых бумагах и организовать их движение таким образом, чтобы похищение конфиденциальных документов было бы затруднено настолько, чтобы оно становилось экономически невыгодным для похитителя.

При работе с документами, содержащими коммерческую тайну, следует соблюдать определенные правила, которые сводятся к нижеследующим:

- строгий контроль (лично или через службу безопасности) за допуском персонала к конфиденциальным документам;
- назначение ответственных лиц за контролем конфиденциального делопроизводства и наделение их соответствующими полномочиями;
- разработка инструкции (памятка) по работе с конфиденциальными документами, ознакомление с ней соответствующих сотрудников фирмы;
- контроль за принятием служащими письменных обязательств о сохранении коммерческой тайны фирмы;
- введение системы материального и морального поощрения сотрудников, имеющих доступ к конфиденциальной информации;
- внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны фирмы;
- личный контроль со стороны руководителя фирмы за службами внутренней безопасности и конфиденциального делопроизводства.

Существуют различные способы ведения конфиденциального делопроизводства, которые направлены на предотвращение утечки содержащихся в документах коммерческих секретов. Как уже

было указано выше, документы, содержащие коммерческую тайну, подразделяются по степени конфиденциальности имеющейся в них информации и снабжаются соответствующим грифом конфиденциальности.

Грамотно поставленная работа с документами поможет защитить их от постороннего глаза. Не следует держать на столе сразу несколько документов, до к тому же различных по степени значимости.

При работе с документами не отлучайтесь из комнаты, а если приходится выходить, то не забудьте закрыть дверь.

Посторонних к документам допускать не следует. Документы, которые правомерно могут потребовать сотрудники налоговой инспекции или правоохранительных служб, следует держать отдельно от остальных конфиденциальных бумаг. По окончании работы наиболее важные документы убираются в сейф, менее важные — в специальные контейнеры. Те и другие следует опечатать и сдать на хранение сотрудникам службы безопасности фирмы.

При пересылке документов следует иметь в виду, что использование телемониторов-игл позволяет через не проклеенные уголки конвертов прочитать содержимое делового письма, не вскрывая его. Поэтому конверты с документами целесообразно дополнительно проклеить скотчем.

Доверяя свои бумаги почте, отправляйте их заказными письмами и письмами с уведомлением о вручении их адресату.

Перемещение документов внутри фирмы также следует держать под контролем.

Организация защиты документов — обязанность руководителей фирмы и ее службы безопасности. Следует быть уверенным, что с момента появления и до уничтожения документ к посторонним не попадал. Если документ утерян (украден), специалисты по службе безопасности должны провести расследование.

Подготовку документов, содержащих важные сведения, следует доверять проверенным людям. Количество экземпляров должно быть строго ограниченным. Для разделения документов по степени важности можно использовать яркие цветные наклейки. При необходимости следует определять степень конфиденциальности документа, а также срок действия ограничительных грифов. При этом необходимо помнить: чем больше секретной информации в нем отражено, тем больше потребуется затрат для его защиты.

Копирование документов — один из способов получения сведений, составляющих тайну фирмы. Множительная техника должна находиться под надежным контролем. Количество копий должно строго учитываться, а их уничтожение — контролироваться. Придерживайтесь правила: наиболее ценные «документы руководители фирм копируют сами».

Если документы размножаются на принтерах ЭВМ, то следует позаботиться о защите информации на магнитных носителях. Если это пишущая машинка нового поколения, то следует принять меры по хранению перфоленты, позволяющей повторно печатать один и тот же текст в автоматическом режиме. По стуку клавишей пишущей машинки специалист с помощью электроники получит текст, аналогичный оригиналу, находясь вне помещения вашего офиса.

Для работы с конфиденциальными документами должны отводиться специальные помещения с хорошей звукоизоляцией. В эти помещения не должны допускаться не только посторонние лица, но и сотрудники, не имеющие разрешения (допуска) на работу с секретами фирмы. Эти помещения должны иметь капитальные стены, надежные перекрытия, прочные двери с замками и запорами, защиту на окнах от проникновения посторонних лиц. Эти помещения должны надежно охраняться, в том числе системой охранной сигнализации, электронно-механическими приспособлениями, системами кабельного телевидения и т. п.

Черновики конфиденциальных документов должны готовиться в тетрадях с пронумерованными листами. После подготовки документов «набело» черновики должны уничтожаться уполномоченными на то сотрудниками. Число копий конфиденциальных документов должно строго учитываться, а копировальные машины снабжаться счетчиком копий и ключом, запускающим машины в действие.

Копировальная бумага и красящая лента пишущих машин — предмет особых забот, так как с них можно снять конфиденциальную информацию. Поэтому использованная копировальная бумага и лента уничтожаются под контролем ответственных лиц.

Вероятность утечки конфиденциальной информации из документов особенно велика в процессе их пересылки. Доставку конфиденциальных документов и ценностей следует организовать своими силами с привлечением сотрудников собственной службы безопасности или же обратиться в специализированные фирмы, которые такие услуги оказывают за плату.

Служащие фирмы, отвечающие за сохранность, использование и своевременное уничтожение конфиденциальных документов, должны быть защищены от соблазна торговли секретами фирмы простым, но весьма надежным способом — хорошей зарплатой.

В процессе хранения и пересылки секретных документов могут быть применены средства защиты и сигнализации при несанкционированном доступе к ним. Одна из новинок — светочувствительное покрытие, наносимой на документы, которое может проявиться под воздействием света, указывая тем самым на факт ознакомления с документами или их фотографированием посторонними лицами.

Используют в этих целях и электронику. Электронное устройство величиной со спичечный коробок реагирует на свет. Стоит его включить и поместить в сейфе, под бумагами на рабочем столе — и в вашем распоряжении надежный сторож. Электронное устройство срабатывает при попадании на него света и подает пронзительный звуковой сигнал. Это устройство называется «Home Detective» (домашний детектив) и стоит 10 долларов США. По желанию заказчика фирма снабжает «Home Detective» радиопередатчиком, включающим на значительном расстоянии иные защитные системы и внешнюю сигнализацию.

Специалистам по вопросам защиты коммерческой информации известны и иные технологии и системы охраны конфиденциальных документов от несанкционированного доступа или возможной утечки из них охраняемых сведений.

4.3. Способы выявления каналов утечки информации

4.3.1. Приборы обнаружения технических средств промышленного шпионажа

Все приборы, предназначенные для поиска технических разведсредств по принципу их действия, можно разделить на два больших класса: устройства поиска ***активного типа***, то есть такие, которые сами воздействуют на объект и исследуют сигнал отклика. К приборам этого типа обычно относят:

- нелинейные локаторы;
- рентгенометры;
- магнитно-резонансные локаторы;
- акустические корректоры.

И устройства поиска ***пассивного типа***. К ним относятся:

- металлоискатели;
- тепловизоры;
- устройства поиска по электромагнитному излучению;
- устройства поиска аномальных параметров телефонной линии;
- устройства поиска аномалий магнитного поля.

Нелинейные локаторы

Среди устройств первого типа наибольшее распространение на отечественном рынке получили нелинейные локаторы, действие которых основано на том факте, что при облучении устройств, содержащих любые полупроводниковые элементы, происходит отражение сигнала на высших кратных гармониках. Причем регистрируется этот сигнал локатором независимо от того, работает или не работает закладка в момент облучения. То есть, если где-то в комнате спрятан радиомикрофон, то он обязательно отзовется на зондирующий сигнал локатора. Ведь это устройство как минимум должно включать в себя собственно микрофон, источник питания, радиопередатчик и антенну; более сложные радиомикрофоны дополнительно могут быть оснащены устройством управления, позволяющим включать и выключать подслушивание по сигналу извне или по кодовому слову, а также устройством записи; и совсем уж изощренные «подслушки» дополнительно могут иметь устройство кодирования информации, например, для того, чтобы все записанное за несколько часов выбросить в эфир в виде короткого импульса. Причем «отзыв» будет прослушиваться на частотах, превышающих основную ча-

оглавление
1 2 3 4 5 6 7 8

стоту зондирующего сигнала в два, три, четыре — и так далее — раз.

Нелинейные локаторы обычно включают в себя:

- генератор;
- направленный излучатель зондирующего сигнала;
- высокочувствительный и также направленный приемник, чтобы определить источник ответного сигнала;
- системы индикации и настройки всего устройства.

Есть и разновидности нелинейных локаторов, основанных на нелинейности отклика среды, применяемые для локации телефонных линий. Но хотя такие приборы на российском рынке представлены достаточно широко, особого распространения они не получили в силу затрудненности анализа и неоднозначности результатов. Во всяком случае, с ними успешно соперничают так называемые «кабельные радары», также посылающие в линию зондирующие импульсы, но отклик исследуется не на присутствие в нем высших гармоник, а на изменение полярности, длительности и амплитуды, происходящее при отражениях от какой-либо неоднородности линии, контактной ли, диэлектрической или механической. Выводимый на экран электронно-лучевой трубки сигнал позволяет достаточно точно судить о том, на каком расстоянии от прибора находится; изменение сечения проводов или неоднородность в диэлектрических характеристиках кабеля — а это параметры, говорящие о возможном подключении именно в этих местах прослушивающих устройств.

Ренгенометры

Рентгенметры используют облучение обследуемых поверхностей рентгеновскими лучами. Данные приборы очень надежные, но на российском рынке широкого признания не получили как в силу громоздкости, так и из-за дороговизны. Эти устройства предлагаются на рынке, но используют их в основном государственные структуры.

Магнито-резонансные локаторы

Магнито-резонансные локаторы фиксируют резонансную ориентацию молекул в ответ на зондирующий импульс. Данные устройства очень дороги и сложны.

Металлоискатели

Металлоискатели основаны на принципе обнаружения металлических предметов, определяемых на основе отклика металлических предметов в магнитном поле. Они недороги и удобны в работе, но большого распространения не получили в силу достаточно ограниченного спектра своих возможностей.

Тепловизоры

Тепловизоры предназначены для фиксирования очень малого перепада температур (буквально в сотые доли градуса). Являются очень перспективными устройствами (особенно дооснащенные компьютерами). Так как любая работающая электронная схема, пусть незначительно, но излучает тепло в пространство, именно тепловой контроль является достаточно недорогим, но очень эффективным и универсальным средством их обнаружения. К сожалению, в настоящее время на рынке представлено не очень большое количество данных приборов.

Устройства, фиксирующие электромагнитное излучение технических средств разведки

Устройства, фиксирующие электромагнитное излучение технических средств разведки. Принцип действия основан на выделении сигнала работающего радиопередатчика. Причем задача, многократно усложненная тем, что заранее никогда не известно, в каком диапазоне частот активен разыскиваемый передатчик. Радиозакладка может излучать в очень узком частотном спектре, как в диапазоне, скажем, нескольких десятков герц, маскируясь под электромагнитное поле обычной электрической сети, так и в свехвысокочастотном диапазоне, оставаясь совершенно неслышной в любых других. Представлены на рынке очень широко и так же широко применяются на практике.

К устройствам, фиксирующим электромагнитное излучение технических средств разведки, относят:

- различные приемники;
- сканеры;
- частотомеры;

- шумомеры;
- анализаторы спектра;
- детекторы излучения в инфракрасном диапазоне;
- селективные микровольтметры и т. д.

Сканеры

Сканеры — специальные очень чувствительные приемники, способные контролировать широкий частотный диапазон от нескольких десятков герц до полутора-двух гигагерц. Сканеры могут пошагово, к примеру, через каждые 50 Гц, прослушивать весь частотный диапазон, причем делают это очень быстро (за одну секунду и даже менее того), автоматически фиксируя в электронной памяти те шаги, при прохождении которых в эфире было замечено активное радиоизлучение. Могут они работать и в режиме автопоиска.

Сегодня на рынке представлены самые разнообразные сканеры. Есть достаточно простые и малогабаритные, выполненные в виде переносной рации, снабжаемые автономным питанием и потому очень удобные в полевых условиях. Есть профессиональные, очень сложные многофункциональные комплексы, способные принимать информацию сразу по нескольким сотням каналов с шагом всего в 10 Гц. Причем предусмотрены возможные режимы работы с подключением к ним компьютера и магнитофона для фиксации и анализа принимаемых сигналов.

Частотомеры

Частотомеры — это приемники, которые не просто прослушивают эфир, выделяя излучение в некоем частотном диапазоне, но и точно фиксируют саму частоту. Российские производители, как правило, не совмещают возможности сканера и частотомера, поэтому наиболее эффективной является японская техника, реализующая иную схему, предполагающую совместную работу сканера, частотомера и компьютера. Сканер просматривает частотный диапазон и, обнаружив сигнал, останавливается. Частотомер точно фиксирует несущую частоту этого сигнала, и это фиксируется компьютером, который тут же может приступить и к анализу; впрочем, по имеющимся на сканере амплитудным индикаторам зачастую сразу можно определить, что же за сигнал «пойман». Далее приемник возобновляет сканирование эфира до получения следующего сигнала.

Анализаторы спектра

Анализаторы спектра отличаются от сканеров заметно меньшей чувствительностью (и, как следствие, меньшей ценой), но зато с их помощью значительно облегчается просмотр радиодиапазонов. Эти приборы дополнительно оснащаются встроенным осциллографом, что позволяет кроме получения числовых характеристик принятого сигнала, высвечиваемых на дисплее, сразу же увидеть и оценить его спектр.

К совершенно отдельному классу относятся выполненные на основе высокочувствительных сканеров комплексы, реализующие сразу несколько поисковых функций. Они в состоянии проводить круглосуточный автоматический мониторинг эфира, анализировать основные характеристики и направления пойманных сигналов, умея засечь не только излучение радиозакладки, но и работу ретрансляционных передатчиков.

Устройства, контролирующее изменение магнитного поля

Устройства, позволяющие контролировать изменения магнитного поля, применяются для поиска звукозаписывающей аппаратуры. Отслеживают они, как правило, то изменение магнитного поля, которое образуется при стирании информации с пленки (в случае, когда запись идет на пленку, а не на микросхему), двигателя магнитофона или иного электромагнитного излучения. В частности, существуют действующие по этому принципу детекторы отечественного производства, которые позволяют даже на фоне внешних помех, в десятки тысяч раз превосходящих уровень сигнала, исходящего от работающего магнитофона, засечь его примерно на полуметровом расстоянии.

Устройства обнаружения несанкционированного подключения к телефонной линии

Задача обнаружения несанкционированного подключения к телефонным линиям достаточна сложна в силу изношенности телефонных соединений, большой протяженности, а также возможнос-

тью бесконтактного способа съема телефонной информации. В настоящее время нет устройств на 100 % гарантирующих защиту от несанкционированного подключения к телефонной линии.

На российском рынке представлены простые и недорогие модели так называемых телефонных стражей, которые, будучи установленными в телефонной розетке, контролируют линию на предмет возможного подключения к ней подслушивающих устройств с низким входным сопротивлением. При снятии трубки это устройство светодиодным индикатором сигнализирует, что линия не прослушивается. В случае же несанкционированного подключения к линии индикатор немедленно гаснет, а охраняемый телефон автоматически отключается. Существуют и более усложненные варианты таких приборов, которые дополнительно, не определяя факта прослушивания, могут производить при снятой трубке автоматическую отсечку всех возможно подключенных гальваническим способом слушающих устройств по постоянному току и даже подавлять их, засылая в линию высокочастотные импульсы, вызывающие резкое повышение напряжения в сети, что приводит к поломке или к автоматическому отключению многих записывающих и слушающих устройств.

4.3.2. Демаскирующие признаки электронных устройств перехвата информации

Обнаружение электронных устройств перехвата информации (закладных устройств), так же как и любых других объектов, производится по их демаскирующим признакам.

Каждый вид электронных устройств перехвата информации имеет свои демаскирующие признаки, позволяющие обнаружить закладку.

Наиболее ***информативными признаками*** проводной микрофонной системы являются:

- тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;
- наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

Демаскирующие признаки автономных *некамуфлированных* акустических закладок включают:

- признаки внешнего вида — малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;
- одно или несколько отверстий малого диаметра в корпусе;
- наличие автономных источников питания (например, аккумуляторных батарей);
- наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;
- наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

Камуфлированные акустические закладки по внешнему виду, на первый взгляд, не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета.

Закладки, устанавливаемые в малогабаритные предметы, ограничивают возможности последних. Эти ограничения могут служить косвенными признаками закладных устройств. Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают.

Некоторые камуфлированные закладные устройства не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

В ряде случаев закамуфлированное закладное устройство обнаруживается по наличию в обследуемом предмете не свойственных ему полупроводниковых элементов (выявляемых при облучении его нелинейным радиолокатором). Например, обнаружение полупроводниковых элементов в пепельнице или в папке для бумаг может указать на наличие в них закладных устройств.

Наличие портативных звукозаписывающих и видеозаписывающих устройств в момент записи можно обнаружить по наличию их побочных электромагнитных излучений (излучений генераторов подмагничивания и электродвигателей).

Дополнительные демаскирующие признаки акустических радиозакладок:

- радиоизлучения (как правило, источник излучения находится в ближней зоне) с модуляцией радиосигнала информационным сигналом;
- наличие (как правило) небольшого отрезка провода (антенны), выходящего из корпуса закладки.

Вследствие того, что при поиске радиозакладок последние находятся в ближней зоне излучения и уровень сигналов о них, как правило, превышает уровень сигналов от других РЭС, у большинства радиозакладок обнаруживаются побочные излучения и, в частности, излучения на второй и третьей гармониках, субгармониках и т.д.

Дополнительные демаскирующие признаки сетевых акустических закладок:

- наличие в линии электропитания высокочастотного сигнала (как правило, несущая частота от 40 до 600 кГц, но возможно наличие сигнала на частотах до 7 МГц), модулированного информационным низкочастотным сигналом;
- наличие тока утечки (от единиц до нескольких десятков мА) в линии электропитания при всех отключенных потребителях;
- отличие емкости линии электропитания от типовых значений при отключении линии от источника питания (на распределительном щитке электропитания) и отключении всех потребителей.

Дополнительные демаскирующие признаки акустических и телефонных закладок с передачей информации по телефонной линии на высокой частоте:

- наличие в линии высокочастотного сигнала (как правило, несущая частота до 7 МГц) с модуляцией его информационным сигналом.

Дополнительные демаскирующие признаки телефонных радиозакладок:

- радиоизлучения с модуляцией радиосигнала информационным сигналом, передаваемым по телефонной линии;
- отличие сопротивления телефонной линии от « оо « при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);
- отличие сопротивления телефонной линии от типового значения (для данной линии) при отключении телефонного аппарата, отключении и закорачивании линии на распределительной коробке (щитке);
- падение напряжения (от нескольких десятых до 1,5…2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной и поднятой телефонной трубке;
- наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне.

Дополнительные демаскирующие признаки акустических закладок типа «телефонного уха»:

- отличие сопротивления телефонной линии от « ? « при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);
- падение напряжения (от нескольких десятых до 1,5…2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной телефонной трубке;
- наличие тока утечки (от единиц до нескольких десятков мА) в телефонной линии при отключенном телефоне;
- подавление (не прохождение) одного-двух вызывных звонков при наборе номера телефонного аппарата.

Дополнительные демаскирующие признаки полуактивных акустических радиозакладок:

- облучение помещения направленным (зондирующим) мощным излучением (как правило, гармоническим);
- наличие в помещении переизлученного зондирующего излучения с амплитудной или частотной модуляцией информационным акустическим сигналом.

4.3.3. Классификация методов и средств поиска электронных устройств перехвата информации

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры: детекторов диктофонов и видеокамер, индикаторов поля, радиочастотомеров и интерсепторов, сканерных приемников и анализаторов спектра, программно-аппаратных комплексов контроля, нелинейных локаторов, рентгеновских комплексов, обычных тестеров, а также специальной аппаратуры для проверки проводных линий и т.д.

Метод поиска закладных устройств во многом определяется использованием той или иной аппаратуры контроля.

К основным методам поиска закладных устройств можно отнести:

- специальное обследование выделенных помещений;
- поиск радиозакладок с использованием индикаторов поля, радиочастотомеров и интерсепторов;
- поиск радиозакладок с использованием сканерных приемников и анализаторов спектра;
- поиск радиозакладок с использованием программно-аппаратных комплексов контроля;
- поиск портативных звукозаписывающих устройств с использованием детекторов диктофонов (по наличию их побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);
- поиск портативных видеозаписывающих устройств с использованием детекторов видеокамер (по наличию побочных электромагнитных излучений генераторов подмагничивания и электродвигателей видеокамер);
- поиск закладок с использованием нелинейных локаторов;
- поиск закладок с использованием рентгеновских комплексов;
- проверка с использованием ВЧ-пробника (зонда) линий электропитания, радиотрансляции и телефонной связи;
- измерение параметров линий электропитания, телефонных линий связи и т.д.;
- проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Простейшими и наиболее дешевыми обнаружителями радиоизлучений закладных устройств являются индикаторы электромагнитного поля, которые световым или звуковым сигналом сигнализируют о наличии в точке расположения антенны электромагнитного поля с напряженностью выше пороговой (фоновой). Более сложные из них — частотомеры обеспечивают, кроме того, измерение несущей частоты наиболее «сильного» в точке приема сигнала.

Для обнаружения излучений закладных устройств в ближней зоне могут использоваться и специальные приборы, называемые интерсепторами. Интерсептор автоматически настраивается на частоту наиболее мощного сигнала и осуществляет его детектирование. Некоторые интерсепторы позволяют не только производить автоматический или ручной захват радиосигнала, осуществлять его детектирование и прослушивание через динамик, но и определять частоту обнаруженного сигнала и вид модуляции.

Чувствительность обнаружителей поля мала, поэтому они позволяют обнаруживать излучения радиозакладок в непосредственной близости от них.

Существенно лучшую чувствительность имеют специальные (профессиональные) радиоприемники с автоматизированным сканированием радиодиапазона (сканерные приемники или сканеры). Они обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладок — от десятков кГц до единиц ГГц. Лучшими возможностями по поиску радиозакладок обладают анализаторы спектра. Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики, что немаловажно при обнаружении радиозакладок, использующих для передачи информации сложные виды сигналов.

Возможность сопряжения сканирующих приемников с переносными компьютерами послужило основой для создания автоматизированных комплексов для поиска радиозакладок (так называемых программно-аппаратных комплексов контроля). Кроме программно-аппаратных комплексов, построенных на базе сканирующих приемников и переносных компьютеров, для поиска закладных уст-

ройств используются и специально разработанные многофункциональные комплексы, такие, например, как «OSCOR-5000».

Специальные комплексы и аппаратура для контроля проводных линий позволяют проводить измерение параметров (напряжений, токов, сопротивлений и т.п.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

Обнаружители пустот позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, которые применяются в любых закладных устройствах, электропроводящие металлические детали конструкции и т.д. Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам — нелинейные радиолокаторы.

Принципы работы ***нелинейных радиолокаторов*** близки к принципам работы радиолокационных станций, широко применяемых для радиолокационной разведки объектов. Существенное отличие заключается в том, что если приемник радиолокационной станции принимает отраженный от объекта зондирующий сигнал (эхо-сигнал) на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик полупроводников.

Металлоискатели (металлодетекторы) реагируют на наличие в зоне поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные рентгеновские установки применяются для просвечивания предметов, назначения которых не удается выявить без их разборки прежде всего тогда, когда она невозможна без разрушения найденного предмета.

4.3.4. Методы обнаружения диктофонов и акустических закладок

Диктофоны и акустические закладки в своем составе содержат большое количество полупроводниковых приборов, поэтому наиболее эффективным средством их обнаружения является нелинейный локатор, устанавливаемый на входе в выделенное помещение и работающий в составе системы контроля доступа.

К типовым представителям устройств этого класса относится, например, нелинейный локатор «Циклон — Рамка». Локатор имеет два датчика, выносной пульт управления и может скрытно устанавливаться в дверной проем выделенного помещения, что позволяет контролировать наличие у посетителей (как в ручной клади, так и под одеждой) любых радиоэлектронных устройств, в том числе диктофонов и подслушивающих устройств, как во включенном, так и в выключенном состояниях. Зона контроля локатора составляет: по высоте — 2,2 м, по длине — 1,5 м, по ширине -1,5 м.

Для обнаружения работающих в режиме записи диктофонов применяются так называемые ***детекторы диктофонов***. Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи. Электродвижущая сила (ЭДС), наводимая этим полем в датчике сигналов (магнитной антенне), усиливается и выделяется из шума специальным блоком обработки сигналов. При превышении уровня принятого сигнала некоторого установленного порогового значения срабатывает световая или звуковая сигнализация. Во избежание ложных срабатываний порог обнаружения необходимо корректировать практически перед каждым сеансом работы, что является недостатком подобных приборов.

Детекторы диктофонов выпускаются в переносном и стационарном вариантах. К переносным относятся детекторы «Сова», RM-100, TRD-800, а к стационарным — PTRD-14, PTRD-16, PTRD-18 и т.д.

В переносном (носимом) варианте блок анализа детектора размещается в кармане оператора, поисковая антенна в рукаве (обычно крепится на предплечье), а датчик сигнализации вибраторного типа — на поясе или в кармане. В ходе переговоров оператор приближает антенну (руку) к возможным

местам установки диктофона (портфель, одежда собеседника и т.д.). При обнаружении излучений (превышении магнитного поля установленного оператором порогового значения) включенного на запись диктофона скрытый сигнализатор-вибратор начинает вибрировать, сигнализируя оператору о возможной записи разговора.

Для защиты выделенных помещений в основном используются детекторы диктофонов, выполненные в стационарных вариантах. В отличие от переносных детекторов, имеющих один датчик сигналов, стационарные детекторы диктофонов оборудованы несколькими датчиками (например, детектор PTRD-18 имеет возможность подключения до 16 датчиков одновременно), что позволяет существенно повысить вероятность обнаружения диктофонов.

Стационарный вариант предполагает установку (заделку) антенн в стол для переговоров и в кресла (подлокотники). Блок анализа и индикатор наличия диктофонов размещается в столе руководителя или у дежурного (в этом случае создается дополнительный канал управления). При наличии у беседующего диктофона в одежде или в вещах (папка, портфель и т.д.) у руководителя скрытным образом будет срабатывать индикация этого факта.

Ввиду слабого уровня магнитного поля, создаваемого работающими диктофонами (особенно в экранированных корпусах), дальность их обнаружения детекторами незначительна. Например, дальность обнаружения диктофона L- 400 в режиме записи в условиях офиса даже при использовании стационарного детектора PTRD-018 не превышает 45 … 65 см. Дальность обнаружения диктофонов в неэкранированных корпусах может составлять 1 … 1,5 м. Основные характеристики детекторов диктофонов представлены в каталоге.

Наряду со средствами обнаружения портативных диктофонов на практике эффективно используются и средства их подавления. Для этих целей используются устройства электромагнитного подавления типа «Рубеж», «Шумотрон», «Буран», «УПД» и др. (таблица 4.8) и устройства ультразвукового подавления типа «Завеса». Основные характеристики устройств подавления диктофонов представлены в каталоге.

Принцип действия устройств электромагнитного подавления основан на генерации в дециметровом диапазоне частот (обычно в районе 900 МГц) мощных шумовых сигналов. В основном для подавления используются импульсные сигналы. Излучаемые направленными антеннами помеховые сигналы, воздействуя на элементы электронной схемы диктофона (в частности, усилитель низкой частоты и усилитель записи), вызывают в них наводки шумовых сигналов. Вследствие этого одновременно с информационным сигналом (речью) осуществляется запись и детектированного шумового сигнала, что приводит к значительному искажению первого.

Зона подавления диктофонов зависит от мощности излучения, его вида, а также от типа используемой антенны. Обычно зона подавления представляет собой сектор с углом от 30 до 80 градусов и радиусом до 1,5 м (для диктофонов в экранированном корпусе).

Устройства подавления диктофонов используют как непрерывные, так и импульсные сигналы. Например, подавитель диктофонов «Шумотрон-2» работает в импульсном режиме на частоте 915 МГц. Длительность излучаемого импульса не более 300 мкс, а импульсная мощность -не менее 150 Вт. При средней мощности излучения 20 Вт обеспечивается дальность подавления диктофонов в экранированном корпусе (типа «Olimpus-400») до 1,5 м в секторе около 30 градусов. Дальность подавления диктофонов в неэкранированном корпусе составляет несколько метров.

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения около 20 кГц), воздействующие непосредственно на микрофоны диктофонов или акустических закладок, что является их преимуществом. Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона или акустической закладки (усилитель начинает работать в нелинейном режиме) и тем самым — к значительным искажениям записываемых (передаваемых) сигналов.

В отличие от систем электромагнитного подавления подобные системы обеспечивают подавление в гораздо большем секторе. Например, комплекс «Завеса» при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 м3. Однако системы ультразвукового подавления имеют и один важный недостаток: эффективность их резко снижается, если микрофон диктофона или закладки прикрыть фильтром из

специального материала или в усилителе низкой частоты установить фильтр низких частот с граничной частотой 3,4 … 4 кГц.

Для обнаружения радиозакладок в выделенных помещениях могут использоваться индикаторы поля, интерсепторы, радиочастотомеры, сканерные приемники, программно-аппаратные комплексы контроля и другие технические средства.

Наиболее эффективным методом выявления радиозакладок в выделенных помещениях является постоянный (круглосуточный) ***радиоконтроль*** с использованием программно-аппаратных комплексов контроля. Для его организации в специально оборудованном помещении на объекте разворачивается стационарный пункт радиоконтроля, в состав которого, как правило, включаются один или несколько программно-аппаратных комплексов, позволяющих контролировать все выделенные помещения. На пункте радиоконтроля устанавливается опорная антенна, а в выделенных (контролируемых) помещениях — малогабаритные широкополосные антенны и звуковые колонки или выносные микрофоны, которые при установке камуфлируются. Антенны и звуковые колонки (или микрофоны) специально проложенными кабелями соединяются соответственно с блоками высокочастотного (антенного) или низкочастотного коммутаторов, установленных в помещении стационарного пункта контроля.

Если при проведении радиоконтроля обнаружена передача информации радиозакладкой, то до ее выявления может быть организована ***постановка прицельных помех*** на частоте передачи закладки. Для этих целей может использоваться, например, устройство постановки помех АРК-СП.

В состав аппаратуры АРК-СП входят широкополосная антенна, перестраиваемый передатчик помех и программное обеспечение. Управляющая программа позволяет с высокой скоростью настраивать передатчик на предварительно заданные частоты в диапазоне от 65 до 1000 МГц. Передатчик создает прицельную по частоте помеху с узкополосной и широкополосной модуляцией несущей частоты специальными сигналами: речевая фраза или тональный сигнал. Мощность помехи — 150 … 200 мВт. Аппаратура функционирует под управлением ПЭВМ автономно или в составе программно-аппаратных комплексов контроля типа АРК и позволяет осуществлять постановку помех одновременно (попеременно) на четырех частотах (время излучения на одной не менее 50 мс).

Аппаратура питается от сети 220 В и имеет размеры 300×300×55 мм.

Для подавления радиозакладок также могут использоваться системы пространственного электромагнитного зашумления, применяемые для маскировки побочных электромагнитных излучений ТСПИ. Однако при этом необходимо помнить, что ввиду сравнительно низкой спектральной мощности излучаемой помехи, эти системы эффективны только для подавления маломощных (как правило, с мощностью излучения менее 10 мВт) радиозакладок. Поэтому для подавления радиозакладок необходимо использовать генераторы шума с повышенной мощностью.

Для защиты речевой информации от сетевых акустических закладок используются помехоподавляющие фильтры низких частот и системы линейного зашумления.

Помехоподавляющие фильтры устанавливаются в линии питания розеточной и осветительной сетей в местах их выхода из выделенных помещений. Учитывая, что сетевые закладки используют для передачи информации частоты свыше 40 … 50 кГц, для защиты информации необходимо использовать фильтры низких частот с граничной частотой не более 40 кГц. К таким фильтрам относятся, например, фильтры типа ФСПК, граничная частота которых составляет 20 кГц.

В системах зашумления линий электропитания используются генераторы шума типа «Гром-ЗИ-4», «Гром-ЗИ-6Ц», «Гном-2С» и др. Основные характеристики генераторов шума представлены в каталоге.

При выборе генераторов шума особое внимание необходимо уделять полосе частот и спектральной мощности помехового сигнала. Например, генераторы шума «Гром-ЗИ-4», «Гром-ЗИ-6Ц» создают помеховый сигнал в диапазоне частот от 0,1 до 1 МГц и от 0,1 до 5 МГц соответственно. Поэтому они не эффективны для подавления сетевых закладок, использующих для передачи информации частоты ниже 100 кГц.

4.4. Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам

1. Общие положения

1.1. Настоящая методика предназначена для проведения инструментально-расчетной оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам при аттестации помещений на соответствие требованиям защищенности, при плановом периодическом контроле защищенности, а также после осуществления их ремонта или реконструкции.

Методика устанавливает нормативные значения октавных коэффициентов звукоизоляции (виброизоляции) ЗП, обеспечивающие защищенность их от утечки речевой конфиденциальной информации, порядок проведения оценки защищенности помещений, состав контрольно-измерительной аппаратуры и порядок проведении измерений.

1.2. При оценке защищенности помещений от утечки речевой конфиденциальной информации по акустическому каналу метод оценки заключается в определении *коэффициентов звукоизоляции* его ограждающих конструкций (ОК) в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц и последующем сопоставлении полученных коэффициентов с их нормативными значениями. *Коэффициент звукоизоляции* в каждой октавной полосе определяется как разность между измеренными уровнями тестового акустического сигнала (далее тест-сигнала) перед ОК L_{c1} и за ее пределами в выбранных контрольных точках (КТ) L_{c2}, дБ .

1.3. При оценке защищенности помещений от утечки речевой конфиденциальной информации по виброакустическому каналу метод оценки заключается в определении коэффициентов виброизоляции ограждающих их конструкций (ОК), а также различных элементов инженерно-технических систем (ИТС), включая их коммуникации, в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц и последующем сопоставлении полученных коэффициентов с их нормативными значениями. *Коэффициент звукоизоляции* в каждой октавной полосе определяется как разность между измеренными уровнями тестового вибрационного сигнала перед ОК и элементами ИТС V_{c1} и на их поверхностях за пределами ЗП в выбранных КТ V_{c2}.

1.4. В качестве тест-сигнала могут быть использованы гармонические (тональные) частоты, соответствующие среднегеометрическим частотам октавных полос, либо шумовой сигнал с нормальным распределением плотности вероятности мгновенных значений в пределах соответствующей октавной полосы.

Октавные уровни излучаемого тест-сигнала в ЗП и уровни акустического (вибрационного) в КТ определяются с использованием измерителя шума и вибраций (шумомера), на вход которого подключается либо приемник звука (микрофон), либо приемник вибраций (вибродатчик).

1.5. При оценке защищенности помещений от утечки речевой конфиденциальной информации по акустическому каналу для каждой ОК выбирается не менее трех КТ в местах наиболее опасных с точки зрения перехвата речевой информации. При оценке защищенности помещений по виброакустическому каналу КТ выбираются на элементах (коммуникациях) ИТС, выходящих за пределы ЗП.

1.6. Нормативные значения октавных коэффициентов звукоизоляции (виброизоляции), обеспечивающих защищенность помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам, приведены в разделе 2 (таблица 1).

2. Нормативные значения октавных коэффициентов звукоизоляции (виброизоляции) ЗП, обеспечивающие его защищенность от утечки речевой конфиденциальной информации

Таблица 1.

Место возможного перехвата речевой конфиденциальной информации из помещения		Нормативное значение октавного коэффициента звукоизоляции (виброизоляции), дБ	
		Помещения, не оборудованные системами звукоусиления	Помещения, оборудованные системами звукоусиления
Смежные помещения		46	60
Уличное пространство	Улица без транспорта	36	50
	Улица с транспортом	26	40

3. Порядок проведения оценки защищенности помещения

3.1. Провести осмотр и анализ архитектурно-планировочных решений ЗП, на предмет характера и конструктивных особенностей ОК и ИТС, включая их коммуникации (воздуховоды, трубопроводы и пр.), особенностей смежных помещений и прилегающих к ЗП уличных пространств.

3.2. Составить план-схему ЗП.

3.3. Выбрать местоположение контрольных точек и отметить их на план-схеме.

3.4. Собрать аппаратурный комплекс для формирования и контроля тест-сигнала в ЗП.

3.5. Измерить излучаемые уровни тест-сигнала в ЗП перед контролируемыми ОК и элементами ИТС для каждой октавной полосы частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц, Lc1(V c1), дБ.

3.6. Измерить уровни акустических (вибрационных) сигналов и уровни шума в выбранных КТ для каждой октавной полосы частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц , L_{c2} (V_{c2}), дБ.

3.7. Определить для каждой КТ октавные коэффициенты звукоизоляции (виброизоляции) Q, дБ.

3.8. Сопоставить полученные значения октавных коэффициентов звукоизоляции (виброизоляции) с их нормативными значениями (раздел 2, таблица 1).

3.9. Оформить (документально) результаты оценки защищенности помещения от утечки речевой конфиденциальной информации по акустическому и вибрационному каналам.

4. Состав контрольно-измерительной аппаратуры

Для проведения измерения уровней акустических (вибрационных) сигналов в ЗП и КТ должна быть использована аппаратура общего применения, на основе которой собираются формирователь акустического тест-сигнала и измерители акустических (вибрационных) сигналов и шумов.

4.1. В состав формирователя акустического тест-сигнала должны входить:
- генератор стандартных сигналов (ГСС) или генератор шума (ГШ);
- усилитель мощности (УМ);
- акустический излучатель (АИ) — громкоговоритель или звуковая колонка.

4.2. В состав измерителя акустического сигнала и акустического шума должны входить:
- измерительный микрофон;
- микрофонный усилитель;
- измеритель шумов и вибраций (шумомер).

4.3. В состав измерителя вибрационного сигнала и вибрационного шума должны входить:

- измерительный вибродатчик (акселерометр);
- предусилитель вибродатчика;
- измеритель шумов и вибраций (шумомер).

5. Порядок размещения контрольно-измерительной аппаратуры при проведении измерений

5.1. Размещение акустического излучателя :

5.1.1. Если ОК является стена, дверь, окно и т.п., то АИ необходимо размещать на высоте 1…1,5 м от от пола и на расстоянии 1,5 м от ОК. Ось апертуры АИ направляется в сторону ОК по нормали к ее поверхности.

5.1.2. Если ОК является пол, то АИ необходимо размещать в центре помещения на высоте 1…1,5 м от пола. Ось апертуры АИ направляется в сторону пола по нормали к его поверхности.

5.1.3. Если ОК является потолок, то АИ необходимо размещать в центре помещения на высоте 1…1,5 м от пола. Ось апертуры АИ направляется в сторону потолка по нормали к его поверхности.

5.1.4. Аналогичные размещения АИ осуществляются относительно элементов ИТС.

5.2. Размещение измерительного микрофона при измерении уровня излучаемого тест-сигнала в ЗП:

5.2.1. Измерительный микрофон размещается на осевой линии апертуры АИ на расстоянии 1 м от плоскости апертуры и на расстоянии 0,5 м от поверхности ОК (элемента ИТС).

5.3. Размещение измерительного микрофона при измерении уровня акустического сигнала и акустического шума в ТК:

5.3.1. Измерительный микрофон размещается в выбранной точке контроля на расстоянии 0,5 м от поверхности ОК.

5.4. Размещение измерительного вибродатчика (акселерометра) при измерении уровня вибрационного сигнала и вибрационного шума в ТК :

5.4.1. Измерительный вибродатчик (акселерометр) размещается в выбранной ТК непосредственно на поверхности ОК или на поверхности контролируемого элемента ИТС.

6. Условия проведения измерений

Измерения необходимо проводить при минимальных уровнях акустических и вибрационных шумов в ЗП и КТ (при отсутствии персонала в ЗП, при выключенных системах вентиляции, кондиционирования и других источников дискретных шумов, при отсутствии транспортных шумов и пр.)

7. Измерение уровней сигналов и шумов в КТ и расчет звукоизоляции (виброизоляции)

7.1. Комплекс аппаратуры формирования тестового акустического сигнала в ЗП размещается согласно п.п.4.1., измерительный комплекс в КТ- согласно п.4.2 или п.4.3.

7.2. При выключенном АИ с помощью измерительного микрофона, измерительного вибродатчика (акселерометра) и шумомера в КТ измеряется уровень акустического (вибрационного) шума Lш(Vш), дБ.

7.3. При включенном АИ в КТ измеряется суммарный уровень акустического (вибрационного) сигнала и акустического (вибрационного) шума Lс+ш (V с+ш), дБ. Уровень излучаемого тест-сигнала устанавливается из условия его надежной фиксации измерительной аппаратурой в КТ на уровне шума.

7.4. Путем расчетной процедуры определяется уровень акустического (вибрационного) сигнала в контрольной точке

7.5. Путем расчетной процедуры определяется коэффициент звукоизоляции (виброизоляции)

Примечание: Процедуры по п.7.3…7.6 выполняются для каждой из октавной полосы частот со среднегеометрическими частотами 250, 500,1000, 2000, 4000 Гц.

7.6. Проводится сравнительный анализ полученных октавных коэффициентов звукоизоляции (виброизоляции) с их нормативными значениями и делается вывод о защищенности помещения от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.

7.7. Оформляются документально результаты контроля.

Приложение В

Рекомендуемая форма протокола инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации

_____

(Наименование организации, проводящей оценку)

ПРОТОКОЛ №___
инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации

1. Объект оценки (наименование ЗП)
2. Назначение ЗП и его краткое описание (расположение помещения, план-схема помещения).
3. Вид оценки (периодический, аттестация и т.п.).
4. Вид оценки канала перехвата речевой информации (акустический или вибрационный).
5. Оцениваемые ограждающие конструкции и элементы технических систем (например, окно (окна), дверь (двери), стена (стены), пол, потолок, вентиляционный люк, коммуникации систем отопления и кондиционирования и др.).
6. Описание применяемых мер и средств защиты.
7. Контрольно-измерительная аппаратура (наименование, тип, заводской номер, дата поверки).
8. Метод проведения измерений (краткое описание или ссылка на документ).
9. Таблицы результатов измерений и расчетов звукоизоляции или виброизоляции (таблица В.1).
10. Заключение о выполнении требований по защите

_____

(Указывается: требования выполняются, требования не выполняются)

Оценку защищенности выполнили:

_____ _____

(должность, фамилия, инициалы) (подписи)

в присутствии представителей _____

(наименование организации)

_____ _____

(должность, фамилия, инициалы) (подписи)

Дата проведения измерений « » ..... 200_ года.

Таблица В.1. Результаты определения октавных коэффициентов звукоизоляции (виброизоляции) в контрольной точке № ...

Номер октавной полосы, i	Измеренный уровень акустического (вибрационного) шума в контрольной точке $Lш_i$ ($Vш_i$), дБ	Уровень измеренного суммарного акустического (вибрационного) сигнала и акустического (вибрационного) шума в контрольной точке $L(c+ш)_i$, $V(c+ш)_i$, дБ	Расчетный уровень акустического (вибрационного) сигнала в контрольной точке L_{2i} (V_{2i}), дБ. $L_{2i}=L(c+ш)_i-Lш_i$ $V_{2i}=V(c+ш)_i-Vш_i$	Октавные уровни звукоизоляции (виброизоляции в контрольной точке Q_i, дБ . $Q_i= L_{2i}(V_{2i}) - - L_{1i}(V_{1i})$
1				
2				
3				
4				
5				

4.5. Методика оценки защищенности ОТСС от утечки конфиденциальной информации (КИ) за счет наводок на токоведущие коммуникации

Общие положения

Методика предназначена для оценки защищенности ОТСС от утечки конфиденциальной информации (КИ) за счет наводок на токоведущие коммуникации, выходящие за пределы контролируемой зоны (КЗ).

1. Краткое описание метода измерений и расчета

В основу настоящей методики положен экспериментально-расчетный метод оценки защищенности ОТСС от наводок ПЭМИ на линии и коммуникации, выходящие за пределы контролируемой зоны.

1.1. Экспериментальная часть метода заключается в:

- установке режима тестирования для исследуемого ОТСС в соответствии с требованиями к тестовым режимам работы ТС;
- выборе мест проведения измерений;
- проведении поиска компонент тест — сигнала в исследуемой цепи;
- измерении напряжения смеси $U_{c+ш}$ обнаруженных компонент тест-сигнала и помех;
- измерении уровня помех $U_{ш}$ в линии на частотах обнаруженных компонент тест сигнала;
- определении коэффициента затухания информативного сигнала в исследуемой цепи.

1.1.1. Рекомендуемые тестовые режимы работы ОТСС приведены в п.6 настоящей методики.

1.1.2. Частотный спектр тест-сигнала исследуемого ОТСС определяют инструментальным путем по идентификационным признакам заданного (тестового) режима его работы. Для определения полного набора информативных спектральных составляющих ПЭМИ рекомендуется проводить измерения на минимальном допустимом расстоянии от исследуемого ОТСС. Анализ спектра проводят в диапазоне частот от 0,01 до 250 МГц. По результатам анализа определяют набор значений $f_1, f_2, \ldots f_i, \ldots f_{1M}$.

1.2. Расчетная часть метода заключается в:

- расчете значения напряжения сигнала в точке проведения измерений для каждой частотной компоненты.
- расчете показателя защищенности в точке проведения измерений для каждой из частотных компонент.
- расчете величины удельного коэффициента затухания наведенных сигналов в исследуемой цепи для каждой из частот.
- расчете максимальной длинны пробега исследуемой цепи для каждой из частот, на которой возможно выделение информативного сигнала.
- выборе максимального из полученных значений R_i и сравнение его с пробегом цепи до границы КЗ. Если пробег исследуемой цепи до границы КЗ больше максимального из всех R_i, то делается вывод о защищенности информации, обрабатываемой ОТСС, от утечки за счет наводок в исследуемую цепь. Если нет, то делается вывод о необходимости принятия дополнительных мер защиты.

2. Условия проведения измерений

При выполнении измерений соблюдают следующие условия:

А. На исследуемых токопроводящих коммуникациях не должно быть высоковольтных напряжений, превышающих предельные характеристики КИА.

Б. Климатические условия должны соответствовать допустимым условиям работы ОТСС и применяемых средств измерений.

В. Рекомендуемые средства измерений

При выполнении измерений применяют средства измерений, удовлетворяющие требованиям ГОСТ 11001-80. Рекомендуемые средства измерений приведены в таблице 1.

Таблица 1

№ п/п	Наименования средств измерений	Состав	Тип	Диапазон измеряемых параметров
Основные средства измерений				
1	Прибор для измерения радиопомех	Селективный микровольтметр, Измерительная антенна	FSM-11 SMV-11 FMA-11	9 кГц–30 МГц, 9 кГц–30 МГц, 0–125 дБ 9 кГц–30 МГц
2	Прибор для измерения радиопомех	Селективный микровольтметр Измерительные антенны	FSM-8.5 SMV-8.5 DP-1 DP-3 LPA	26–1000 МГц 26–1000 МГц, 0–125 дБ 30–300 МГц 300–1000 МГц 87–1000 МГц
3	Комплект измерительных антенн		АИР3-2 АИР4-2	0,008–40 МГц 0,05–1000 МГц
4	Генераторы сигналов		Г4-158 Г4-116	0,01–100 МГц 4–300 МГц
5	Измерительный пробник	Из состава SMV Из состава С1-116	ТК-4	0,09–300 МГц 0–250 МГц
Вспомогательные средства измерений				
6	Осциллограф		С1-116	0–250 МГц

Примечания:

1. Вместо указанных в таблице средств измерений разрешается применять другие аналогичные, обеспечивающие измерение соответствующих параметров с требуемой точностью.

2. Применяемые средства измерений должны быть исправны, поверены и иметь свидетельства (отметки в формулярах или паспортах) о поверке.

Г. Требования безопасности выполнения работ

При проведении измерений соблюдают следующие требования:

- лица, допущенные к выполнению работ по данной методике, должны иметь третью (до 1000 В) квалификационную группу по электробезопасности;
- до включения приборов в сеть необходимо убедиться в исправности системы заземления.

Д. Требования к квалификации операторов

К выполнению измерений и обработке их результатов допускаются лица, имеющие специальное инженерно — техническое образование и допуск к самостоятельной работе по специальности.

Е. Требования к тестовым режимам работы ОТСС

Тестовый режим должен обеспечивать:

1. Формирование периодической последовательности информативных сигналов;
2. Максимально возможную частоту следования информативных сигналов;
3. Идентификацию информативных тестовых сигналов на фоне других сигналов, помех и шумов;
4. Возможность измерения уровней тестовых сигналов стандартными средствами измерений;
5. Достаточное для измерений время работы ОТСС в тестируемом режиме.

Для проведения специсследований ОТСС, в состав которых входят видеомониторы, рекомендуется применять специальную тестовую программу «Зебра». Для проведения специсследований локальных компьютерных сетей в режиме передачи данных рекомендуется применять специальную тестовую программу «NetTest».

Ж. Подготовка к выполнению измерений

При подготовке к выполнению измерений проводят следующие работы:

- на минимальном удалении от исследуемого ОТСС на испытываемой линии выбирают точку проведения измерений с учетом доступности к токопроводящим коммуникациям и обеспечивают в ней надежный электрический контакт с высокочастотным измерительным пробником;
- на ОТСС устанавливают тестовый режим работы;
- проводят подготовительные мероприятия в соответствии с инструкцией по эксплуатации на применяемые средства измерений (присоединение пробников, выдержка во включенном состоянии, калибровка и т. д.).

З. Выполнение измерений

При выполнении измерений напряжения наведенного в токопроводящих коммуникациях информативного сигнала выполняются следующие операции:

1. По идентификационным признакам определяют частотный спектр ПЭМИ. Допускается использовать частоты $f_1, f_2, \ldots f_i$, выявленные при инструментальном контроле ПЭМИ данного ОТСС;

2. Измеряют напряжение смеси обнаруженных компонент тест-сигнала и помех в соответствии с требованиями инструкций по эксплуатации применяемых средств измерения. Полосу пропускания измерительных приемников выбирают равной 9 кГц в диапазоне частот до 30 МГц и 120 кГц в диапазоне 30–250 МГц. Результаты заносят в табл. 2;

Примечание: Если имеется возможность подключения средств измерений к линиям на границе КЗ (в непосредственной близости) и удается обнаружить информативный сигнал, то делается вывод о неэффективности принятых мер защиты.

3. Производят измерение уровня помех в линии на частотах обнаруженных компонент тест сигнала, при выключенном ОТСС. Полученные результаты заносят в таблицу 2;

4. Определяют коэффициент удельного затухания информативного сигнала в исследуемой цепи, для чего:

- собирают схему измерений согласно рис. 1;
- подают сигнал генератора ВЧ в исследуемую цепь в точке К, отстоящей от точки А 1–3 метра. Во избежание выхода из строя генератора сигналов его подключение в точке А рекомендуется осуществлять индуктивным способом;

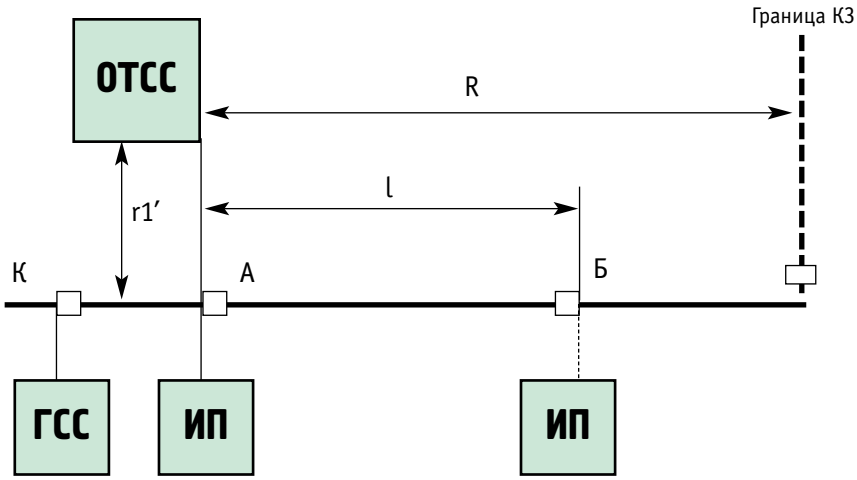


Рис.1. Схема измерения коэффициента затухания

- устанавливают органами управления генератора достаточный уровень выходного сигнала (уровень сигнала должен обеспечить его обнаружение в точках А и Б);
- перестраивая по частоте генератор и приемник измеряют на обнаруженных по п.п 1 частотах напряжение генератора сигналов в точке А. Полученные результаты заносят в таблицу 2;
- выбирают точку проведения вторых измерений Б. Точку Б рекомендуется выбирать на расстоянии не менее 15–25 метров от точки А;
- не изменяя режим работы генератора и измерительного приемника в точке Б производят измерения аналогичные проведенным в точке А. Полученные результаты заносят в таблицу 2, где:

F — частота обнаруженных компонент тест сигнала;

$U_{с+ш}$ — измеренное значение напряжения смеси сигнала и помехи в линиях при работе ОТСС в тестирующем режиме;

$U_{ш}$ — измеренное среднеквадратическое значение напряжения помех в линиях;

$U_{с}$ — значение напряжения информативной составляющей сигнала;

U_{1} — измеренное значение напряжения генератора в точке А;

U_{2} — измеренное значение напряжения генератора в точке В;

$K_{у}$ — коэффициент удельного в цепи;

R_{i} — допустимое значение пробега токоведущих коммуникаций до границы КЗ.

Таблица 2.

F, МГц	$U_{с+ш}$, дБ	$U_{ш}$, дБ	$U_{с}$, дБ	U_{1}, мкВ	U_{2}, мкВ	$K_{у}$, дБ/м	R_{i}, м

И. Обработка и анализ результатов измерений

Объект ОТСС считается защищенным от утечки информации по линиям и коммуникациям, выходящим за пределы КЗ, если для всех частотных компонент тест-сигнала выполняется условие Ri (Rкз.

К. Оформление результатов измерений и расчета

Результаты измерений оформляются протоколом

Образец протокола представлен в приложении 1.

Приложение 1

ПРОТОКОЛ
контроля защищенности информации, обрабатываемой ОТСС (указать тип ОТСС, зав. номер), от ее утечки за счет наводок информативного сигнала на (указать коммуникации)

1. Измерениям подвергался информативный сигнал, наведенный от ОТСС (тип, зав. №) на (коммуникации), расположенные совместно с ОТСС в (место установки ОТСС) и имеющие выход за пределы контролируемой зоны объекта _____. Комплектация ОТСС указана в таблице 1.

Таблица 1

Наименование составной части	Тип (модель)	Заводской номер

Минимальная протяженность (коммуникации) до границы КЗ — (указать протяженность), м.

2. При проведении измерений использовались следующие нормативные документы: (указать использованные нормативные документы).

3. Измерения проводились с применением средств измерений, указанных в таблице 2.

Таблица 2

Наименование средства измерений	Тип	Зав. номер	Диапазон частот, МГц	Дата очередной поверки
Селективный микровольтметр	SMV- 8.5			
Селективный микровольтметр	SMV- 11			
Осциллограф	С1-116			
Генератор сигналов	Г4-116			

В качестве тест-сигнала использовался сигнал, создаваемый специализированной тестирующей программой.

4. Информативный сигнал измерялся на частотах обнаруженных информативных ПЭМИ в диапазоне 0,1–250 МГц путем подключения к (коммуникации) измерительного пробника, соединенного с входом селективного микровольтметра (SMV-8.5 / SMV-11).

Результаты измерений наведенного в ВТСС информативного сигнала и расчета значения допустимого пробега их коммуникаций до границы КЗ, представлены в таблице 3.

Таблица 3

F, МГц	$U_{с+ш}$, дБ	$U_{ш}$, дБ	$U_{с}$, дБ	U_{1}, мкВ	U_{2}, мкВ	$K_{у}$, дБ	R_{i}, м	Вывод
Коммуникации ВТСС								
Коммуникации ВТСС								

Где:
$U_{с+ш}$ — измеренное значение напряжения смеси сигнала и помехи в (коммуникации) при работе ОТСС в тестирующем режиме;
$U_{ш}$ — измеренное значение напряжения помех в (коммуникации);
$U_{с}$ — значение напряжения информативной составляющей сигнала;
U_{1} — измеренное значение напряжения генератора в точке измерения информативных составляющих сигнала;
U_{2} — измеренное значение напряжения генератора в точке, удаленной по (коммуникации) на 15 метров;
$K_{у}$ — коэффициент удельного затухания сигнала в (коммуникация);
R_{i} — рассчитанное допустимое значение пробега токоведущих коммуникаций до границы КЗ.
Измерения производились в полосе частот 9 кГц для диапазона до 30 МГц и 120 кГц свыше 30 МГц;

***Вывод: защищенность информации , обрабатываемой ОТСС** (указать тип ОТСС, зав. номер), **от ее утечки за счет наводок информативного сигнала на** (указать коммуникации) **обеспечивается / не обеспечивается. Требуются / не требуются дополнительные меры защиты**.*

Занимаемая должность

Дата проведения измерений

(подпись) Ф.И.О.

4.6. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований

Список используемых сокращений
ЗП — защищаемые помещения (служебные кабинеты, актовые, конференц-залы и т.д.).
ВТСС — вспомогательные технические средства и системы.
ГСС — генератор стандартных сигналов.
АИ — акустический излучатель.
УМ — усилитель мощности.

1. Общие положения

1.1. Настоящая методика предназначена для проведения инструментально-расчетной оценки защищенности помещений от утечки речевой конфиденциальной информации по электроакустическим каналам при аттестации защищаемых помещений (ЗП) на соответствие требованиям защищенности, при плановом периодическом контроле защищенности, а также после изменения состава вспомогательных технических средств и систем (ВТСС) в ЗП.

1.2. В качестве электроакустических преобразователей могут выступать технические средства и системы, содержащие в своем составе элементы, электрические параметры которых обладают микрофонным эффектом и могут меняться под воздействием звукового давления. Как правило, такими элементами являются: микрофоны, электрические звонки, динамики, катушки индуктивности, и пр. При этом потенциально опасными следует считать ВТСС, функциональные (сигнальные) цепи которых выходят за пределы ЗП.

1.3. Метод оценки заключается в инструментально — расчетном определении совокупности октавных отношений напряжений (отношений «сигнал шум» по напряжению), наводимых в функциональных (сигнальных) цепях ВТСС тестовым акустическим сигналом (тест-сигналом) и шумом за счет их электроакустических преобразований соответствующими системами и средствами и последующим сравнением этих отношений с нормативными значениями.

Определение отношений «сигнал/шум» проводится на разъемах функциональных (сигнальных) цепей ВТСС при отключенных линиях, выходящих за пределы ЗП, в октавных полосах частот со сред-

негеометрическими частотами $f_{ср}$ 250, 500, 1000, 2000, 4000 Гц.

Инструментальным способом определяются величина напряжения шума $U_{ш}$, мкВ, и величина напряжения смеси тест-сигнала и шума $U_{(с+ш)}$, мкВ.

Расчетным способом находятся приведенные к ширине октавной полосы частот напряжения шума $U_{ш\ окт}$ и смеси тест-сигнала и шума $U_{(с+ш)}$, мкВ, напряжение тест-сигнала $U_{с}$, мкВ, отношение напряжений тест-сигнала и шума $\Delta_{(с/ш)} = U_{с} / U_{ш\ окт}$.

1.4. В качестве тест-сигнала необходимо использовать гармонические (тональные) частоты, соответствующие среднегеометрическим частотам октавных полос. Октавные уровни излучаемого тест-сигнала должны соответствовать интегральному уровню речи 70 дБ (для ЗП, не оборудованных системами звукоусиления) и 84 дБ (для остальных ЗП). Значения октавных уровней тест-сигнала приведены в приложении Б.

Уровень излучаемого тест-сигнала должен быть стабилен в процессе проведения измерений.

1.5. Все измерения должны проводиться в соответствии с инструкцией по эксплуатации применяемого контрольно-измерительного средства.

1.6. Нормативные значения октавных отношений «сигнал/шум», обеспечивающих защищенность рабочих помещений от утечки речевой конфиденциальной информации по электроакустическим каналам, приведены в разделе 2 .

2. Нормативное значение отношения «сигнал/шум» по напряжению на разъемах функциональных (сигнальных) цепей ВТСС

Для обеспечения защищенности ЗП от утечки речевой конфиденциальной информации по электроакустическим каналам отношение «сигнал / шум» $\Delta_{с/ш}$ на разъемах функциональных (сигнальных) цепей каждого потенциально опасного ВТСС в каждой октавной полосе с граничными частотами 175…350 Гц ($f_{ср}$ = 250 Гц), 350…700 Гц ($f_{ср}$ = 500Гц), 700…1400 Гц ($f_{ср}$ = 1000 Гц), 1400…2800 Гц ($f_{ср}$ = 2000 Гц) и 2800…5600 Гц ($f_{ср}$ = 4000 Гц) должно отвечать условию $\Delta_{с/ш} \leq 0{,}1$

3. Порядок проведения оценки защищенности помещения

3.1. Составить план-схему размещения ВТСС в рабочем помещении.

3.2. На основе анализа функционального назначения, конструктивных особенностей и схемотехнических решений выявить и отметить на план-схеме потенциально опасные ВТСС.

3.3. Подготовить аппаратурный комплекс для формирования и контроля тест-сигнала и измерения напряжений на разъемах функциональных (сигнальных) цепей потенциально опасных ВТСС.

3.4. Отключить подходящие к ВТСС функциональные (сигнальные) линии, убедиться в отсутствии на разъемах высоких напряжений, превышающих предельные характеристики применяемых средств измерений, подключить к разъему согласующую нагрузку.

3.5. Для каждого оцениваемого ВТСС определить величины напряжений тест-сигнала Uс и шума Uш на выходных разъемах для каждой октавной полосы частот.

3.6. Для каждого ВТСС определить октавные отношения «сигнал/шум» $\Delta_{(с/ш)i}$.

3.7. Измерительные процедуры согласно п.п. 3.4 и 3.5 выполнить для двух режимов работы ВТСС — активного (включенного) и выключенного.

3.8. Для каждого ВТСС и каждого из его режимов сопоставить полученные значения октавных отношений «сигнал/шум» с их нормативными значениями (раздел 2).

3.9. Документально оформить результаты оценки защищенности ЗП от утечки речевой конфиденциальной информации по электроакустическим каналам согласно прилагаемой формы протокола.

4. Состав контрольно-измерительной аппаратуры и ее размещение

Для проведения измерения должна быть использована аттестованная и поверенная аппаратура общего применения, на основе которой собираются формирователь акустического тест-сигнала и измерители напряжений малого уровня.

4.1. В состав формирователя акустического тест-сигнала должны входить:

- генератор стандартных сигналов (ГСС);
- усилитель мощности (УМ);
- акустический излучатель (АИ) — громкоговоритель или звуковая колонка.

4.2. АИ необходимо размещать в непосредственной близости от ВТСС на расстоянии 1 м.

4.3. В качестве измерителя напряжений малого уровня могут использоваться различные типы селективных микровольтметров и нановольтметров.

4.4. Микровольтметр (нановольтметр) необходимо подключать к выходным разъемам оцениваемых ВТСС при отключенных сигнальных цепях.

Перечень рекомендуемой контрольно-измерительной аппаратуры общего применения и их технические характеристики приведены в приложении А.

5. Условия проведения измерений

Измерения необходимо проводить при минимальных уровнях акустических шумов в ЗП (отсутствии персонала в ЗП, выключенных системах вентиляции, кондиционирования и других источников дискретных шумов, ограничении внешних шумов, проникающих в ЗП).

6. Выполнение измерений

6.1. Разместить АИ на расстоянии 1 м от оцениваемого ВТСС.

6.2. При выключенном АИ с помощью селективного вольтметра измерить величину напряжения шума на разъемах ВТСС $U_{ш\ пр}$, мкВ, в минимальной измерительной полосе прибора $\Delta F_{пр}$, отвечающей условию

$\Delta F_{пр} \leq \Delta F_{окт}$.

В случае невыполнения условия $\Delta F_{пр} \leq \Delta F_{окт.}$ выбирается измерительная полоса селективного вольтметра ближайшая к величине октавной полосы.

6.3. Рассчитать величину напряжения шума в октавной полосе $U_{ш\ окт}$, мкВ.

6.4. При включенном АИ с помощью селективного вольтметра измерить величину суммарного напряжения смеси сигнала с шумом $U_{(с+ш)\ пр}$, мкВ, аналогично п.2.

6.5. Рассчитать величину напряжения смеси сигнала с шумом в октавной полосе $U_{(с+ш)\ окт}$, мкВ.

6.6. Рассчитать величину напряжения тест-сигнала $U_{с\ окт}$, мкВ, в каждой октавной полосе.

6.7. Рассчитать отношение «сигнал/шум» $\Delta_{с/ш}$.

6.8. Провести сравнительный анализ полученных отношений «сигнал/шум» с их нормативными значениями.

6.9. Сделать вывод о защищенности ЗП от утечки речевой конфиденциальной информации по электроакустическим каналам.

6.10. Оформить документы результатов оценки.

Приложение А

Перечень аппаратуры общего применения, рекомендуемой для проведения измерения при проведении оценки защищенности помещений от утечки речевой конфиденциальной информации по электроакустическим каналам

Наименование измерительной аппаратуры	Требуемые технические характеристики	Рекомендуемые типы аппаратуры
1	2	3
Генераторы шумовых сигналов	Вид шумового сигнала: «белый шум» (с нормальным распределением плотности вероятности мгновенных значений), хаотическая импульсная последовательность. Диапазон частот: не менее 100 …10 000 Гц	Г2-37, Г2-47, П219 (А, В), «Кабинет», «Шорох-1», «Шорох-2» (Россия), 03000, 03004 (Германия) и др.
Низкочастотные генераторы сигналов	Диапазон рабочих частот: не менее 100…10 000 Гц. Выходное напряжение: не менее 5 В	Г3-36А, Г3-48, Г3-53, (Россия), 02002 (Германия) и др., в т.ч. специализированные
Усилители мощности	Диапазон частот: не менее 100…10 000 Гц. Выходная мощность: не менее 10 Вт	«Степь-102 (103)», серия УМ «Звук» (Россия), LV-102(103) (Германия) и др.
Акустические излучатели	Диапазон воспроизводимых частот: не менее 100…10 000 Гц. Уровень звукового давления на расстоянии 1 м от излучателя в свободном поле не менее 85 дБ. Неравномерность АЧХ: не более ±6 дБ.	Акустические системы (звуковые колонки) 15АС-109 (масса – 6,8 кг.), 15АС-216 (масса – 7 кг.), 6АС-320 (масса – 2,8 кг.) и др. малогабаритные акустические системы 1, 2 и 3 групп сложности (Россия).
Селективные микровольтметры	Диапазон рабочих частот: не менее 100…10 000 Гц. Погрешность измерения напряжения не более ±15 %	В6-9 (Россия), Unipan-233 (Польша) и др.
Селективные нановольтметры	Диапазон рабочих частот: не менее 100…10 000 Гц. Погрешность измерения напряжения не более ±15 %	Unipan-237 (Польша) и др.

Приложение Б

Октавные уровни речевых сигналов с интегральным уровнем 70 дБ (0,06 Па) и 84 дБ (0,3 Па)

Среднегеометрические частоты октавных полос, Гц	Ширина октавной полосы, Гц	Октавные уровни, дБ (Па), речевого сигнала с интегральным уровнем 70 дБ	Октавные уровни, дБ (Па), речевого сигнала с интегральным уровнем 84 дБ
250	175	66 (0,04)	80 (0,2)
500	350	66 (0,04)	80 (0,2)
1000	700	61 (0,02)	75 (0,1)
2000	1400	56 (0,01)	70 (0,06)
4000	2800	53 (0,009)	67 (0,04)

Примечание: Перевод уровней речевого сигнала из размерности (дБ) в размерность (Па) производится по формуле $L_S(\text{Па}) = 2 \cdot 10^{-5}\, 10^{(0{,}05 L_S(\text{дБ}))}$

Приложение В

Рекомендуемая форма протокола оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований

Протокол оценки защищенности помещения от утечки речевой конфиденциальной информации по каналам электроакустических преобразований

1. Название оцениваемого ЗП .....

2. План-схема ЗП с размещением в нем ВТСС (оформляется отдельным листом)

3. Перечень потенциально опасных ВТСС

Таблица 3.1

Наименование ВТСС	Тип (модель) ВТСС	Заводской номер	Место установки ВТСС в ЗП

4. Перечень контрольно-измерительной аппаратуры

Таблица 4.1

Наименование КИА	Тип (модель) КИА	Заводской номер	Дата очередной поверки

5. Результаты измерений и расчетов

5.1. Значения измеренных напряжений

Таблица 5.1

Наименование ВТСС	Режим работы	Выходной разъем цепи	$U_{ш\ пр}$, мкВ, по октавным полосам					$U_{(с+ш)\ пр}$, мкВ, по октавным полосам				

5.2. Значения рассчитанных параметров

Таблица 5.2

Наименование ВТСС	Режим работы	Выходной разъем цепи	$U_{ш\ окт}$, мкВ, по октавным полосам, формула (1)					$U_{(с+ш)\ окт}$, мкВ, по октавным полосам, формула (2)					$U_{с\ окт}$, мкВ, по октавным полосам, формула (3)				

оглавление
1
2
3
4
5
6
7
8

5.3. Соответствие октавных отношений «сигнал/шум» нормативному значению

Таблица 5.3

Наименование ВТСС	Режим работы	Выходной разъем цепи	$\Delta_{c/ш}$ по октавным полосам, формула (4)					Соответствие нормативному значению по октавным полосам				

6. Выводы о защищенности помещений от утечки речевой конфиденциальной информации по электроакустическим каналам

_____

_____

_____ _____

(должность, фамилия, инициалы) (подписи)

в присутствии представителей _____

(наименование организации)

_____ _____

(должность, фамилия, инициалы) (подписи)

Дата проведения измерений « » ..... 200_ года.

5. Требования и рекомендации по защите конфиденциальной информации, обрабатываемой в АС

Система (подсистема) защиты информации, обрабатываемой в автоматизированных системах различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических средств и мер по защите информации при ее автоматизированной обработке и хранении, при ее передаче по каналам связи.

Основными направлениями защиты информации являются:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения и подделки за счет НСД и специальных воздействий;
- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.1. Порядок обеспечения защиты конфиденциальной информации при эксплуатации АС

Организация эксплуатации АС и СЗИ в ее составе осуществляется в соответствии с установленным в учреждении (на предприятии) порядком, в том числе технологическими инструкциями по эксплуатации СЗИ НСД для пользователей, администраторов АС и работников службы безопасности.

Для обеспечения защиты информации в процессе эксплуатации АС рекомендуется предусматривать соблюдение следующих основных положений и требований:

- допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), должен производиться в соответствии с установленным разрешительной системой допуска порядком;
- на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации, допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с разрешения руководителя учреждения (предприятия) или руководителя службы безопасности;
- в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;
- по окончании обработки защищаемой информации или при передаче управления другому лицу, пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;
- изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;
- при увольнении или перемещении администраторов АС, руководителем учреждения (предприятия), по согласованию со службой безопасности, должны быть приняты меры по оперативному изменению паролей и идентификаторов.

Все носители информации на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в технологическом процессе обработки информации в АС, подлежат учету в том производственном, научном или функциональном подразделении, которое является владельцем АС, обрабатывающей эту информацию.

Учет съемных носителей информации на магнитной или оптической основе (гибкие магнитные диски, съемные накопители информации большой емкости или картриджи, съемные пакеты дисков, иные магнитные, оптические или магнито-оптические диски, магнитные ленты и т.п.), а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе осуществляется по карточкам или журналам установленной формы, в том числе автоматизиро-

вано с использованием средств вычислительной техники. Журнальная форма учета может использоваться в АС с небольшим объемом документооборота.

Съемные носители информации на магнитной или оптической основе, в зависимости от характера или длительности использования, допускается учитывать совместно с другими документами по установленным для этого учетным формам.

При этом перед выполнением работ сотрудником, ответственным за их учет, на этих носителях информации предварительно проставляются любым доступным способом следующие учетные реквизиты: учетный номер и дата, пометка «Для служебного пользования», номер экземпляра, подпись этого сотрудника, а также другие возможные реквизиты, идентифицирующие этот носитель.

Распечатки допускается учитывать совместно с другими традиционными печатными документами по установленным для этого учетным формам.

Временно не используемые носители информации должны храниться пользователем в местах, недоступных для посторонних лиц.

5.2. Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ

Автоматизированные рабочие места на базе автономных ПЭВМ являются автоматизированными системами, обладающими всеми основными признаками АС. Информационным каналом обмена между такими АС являются носители информации на магнитной (магнито-оптической) и бумажной основе.

В связи с этим, порядок разработки и эксплуатации АРМ на базе автономных ПЭВМ по составу и содержанию проводимых работ по защите информации, организационно-распорядительной, проектной и эксплуатационной документации должны полностью отвечать требованиям настоящего документа.

АС на базе автономных ПЭВМ в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» должны быть классифицированы и отнесены:

- к 3 группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
- ко 2 и 1 группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.

Примечание: При использовании на автономной ПЭВМ технологии обработки информации на съемных накопителях большой емкости, классификация АС производится на основании анализа режима доступа пользователей АС к информации на используемом съемном накопителе (либо одновременно используемом их комплексе).

5.3. Защита информации в локальных вычислительных сетях

Характерными особенностями ЛВС являются распределенное хранение файлов, удаленная обработка данных (вычисления) и передача сообщений (электронная почта), а также сложность проведения контроля за работой пользователей и состоянием общей безопасности ЛВС.

Средства защиты информации от НСД должны использоваться во всех узлах ЛВС, независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС, и требуют постоянного квалифицированного контроля со стороны администратора безопасности информации.

Информация, составляющая служебную тайну, и персональные данные, могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или в условиях, изложенных в подразделе «Защита информации при межсетевом взаимодействии».

Класс защищенности ЛВС определяется в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Для управления ЛВС и распределения системных ресурсов в ЛВС, включая управление средствами защиты информации, обрабатываемой (хранимой, передаваемой) в ЛВС, в дополнение к системным администраторам (администраторам ЛВС) могут быть назначены администраторы по безопасно-

сти информации, имеющие необходимые права доступа к защищаемой информации ЛВС.

Состав пользователей ЛВС должен устанавливаться по письменному разрешению руководства предприятия (структурного подразделения) и строго контролироваться. Все изменения состава пользователей, их прав и привилегий должны регистрироваться.

Каждый администратор и пользователь должен иметь уникальные идентификаторы и пароли.

5.4. Защита информации при межсетевом взаимодействии

Положения данного подраздела относятся к взаимодействию локальных сетей, ни одна из которых не имеет выхода в сети общего пользования типа Интернет.

Взаимодействие ЛВС с другими вычислительными сетями должно контролироваться с точки зрения защиты информации. Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах КЗ.

При конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС, рекомендуется учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия.

Подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

Для защиты АС при ее взаимодействии с другой АС по каналам связи необходимо использовать:

- в АС класса 1Г — МЭ не ниже класса 4;
- в АС класса 1Д и 2Б, 3Б — МЭ класса 5 или выше.

Для защиты конфиденциальной информации, передаваемой по каналам связи между АС, если каналы связи выходят за пределы КЗ, необходимо использовать защищенные каналы связи, включая защищенные волоконно-оптические линии связи или сертифицированные ФАПСИ криптографические средства защиты.

5.5. Защита информации при работе с системами управления базами данных

При работе с системами управления базами данных (СУБД) и базами данных (БД) необходимо учитывать следующие особенности защиты информации от НСД:

- в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;
- БД могут быть физически распределены по различным устройствам и узлам сети;
- БД могут включать информацию различного уровня конфиденциальности;
- разграничение доступа пользователей к БД средствами операционной системы и/или СЗИ НСД может осуществляться только на уровне файлов БД;
- разграничение доступа пользователей к объектам БД: таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п., может осуществляться только средствами СУБД, если таковые имеются;
- регистрация действий пользователей при работе с объектами БД может осуществляться также только средствами СУБД, если таковые имеются;
- СУБД могут обеспечивать одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

С учетом указанных особенностей при создании БД рекомендуется:

- при выборе СУБД ориентироваться на операционные системы и СУБД, включающие либо штатные сертифицированные средства защиты информации от НСД, либо имеющие соответствующие сертифицированные дополнения в виде СЗИ НСД;

- при использовании СУБД, не имеющих средств разграничения доступа, производить разбиение БД на отдельные файлы, разграничение доступа к которым можно проводить средствами ОС и/или СЗИ НСД;
- при использовании современных СУБД, основанных на модели клиент-сервер, использовать их штатные средства защиты информации от НСД, применять средства регистрации (аудита) и разграничение доступа к объектам БД на основе прав, привилегий, ролей, представлений (VIEW), процедур и т.п.

5.6. Защита информации при использовании съемных накопителей информации большой емкости для автоматизированных рабочих мест

Данная информационная технология предусматривает запись на загружаемый съемный накопитель информации большой емкости одновременно общесистемного (ОС, СУБД) и прикладного программного обеспечения, а также обрабатываемой информации одного или группы пользователей.

В качестве устройств для работы по этой технологии могут быть использованы накопители на магнитном, магнитооптическом или лазерном дисках различной конструкции, как встроенные (съемные), так и выносные. Одновременно может быть установлено несколько съемных накопителей информации большой емкости.

Несъемные накопители должны быть исключены из конфигурации ПЭВМ. Основной особенностью применения данной информационной технологии для АРМ на базе автономных ПЭВМ, с точки зрения защиты информации, является исключение этапа хранения на ПЭВМ в нерабочее время информации, подлежащей защите. Эта особенность может быть использована для обработки защищаемой информации без применения сертифицированных средств защиты информации от НСД и использования средств физической защиты помещений этих АРМ.

На этапе предпроектного обследования необходимо провести детальный анализ технологического процесса обработки информации, обращая внимание, прежде всего, на технологию обмена информацией (при использовании съемных накопителей информации большой емкости или гибких магнитных дисков (ГМД или дискет) с другими АРМ, как использующими, так и не использующими эту информационную технологию, на создание условий, исключающих попадание конфиденциальной информации на неучтенные носители информации, несанкционированное ознакомление с этой информацией, на организацию выдачи информации на печать.

Обмен конфиденциальной информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации.

На рабочих местах исполнителей, работающих по этой технологии, во время работы, как правило, не должно быть неучтенных накопителей информации. В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть «закрыты на запись». Условия и порядок применения таких процедур должны быть отражены в технологии обработки информации, использующей съемные накопители информации большой емкости.

При использовании в этой технологии современных средств вычислительной техники, оснащенных энергонезависимой, управляемой извне перезаписываемой памятью, так называемых Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении, необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

Должна быть разработана и, по согласованию со службой безопасности, утверждена руководителем учреждения (предприятия) технология обработки конфиденциальной информации, использующая съемные накопители информации большой емкости и предусматривающая вышеуказанные, а также другие вопросы защиты информации, имеющие отношение к условиям размещения, эксплуатации АРМ, учету носителей информации, а также другие требования, вытекающие из особенностей функционирования АРМ.

6. Рекомендации по обеспечению защиты конфиденциальной информации, при взаимодействии абонентов с ИНТЕРНЕТОМ

6.1. Условия и порядок подключения абонентов к сети

Подключение к Сети абонентского пункта (АП) осуществляется по решению руководителя учреждения (предприятия) на основании соответствующего обоснования.

Обоснование необходимости подключения АП к Сети должно содержать:

- наименование Сети, к которой осуществляется подключение, и реквизиты организации-владельца Сети и провайдера Сети;
- состав технических средств для оборудования АП;
- предполагаемые виды работ и используемые прикладные сервисы Сети (E-Mail, FTP, Telnet, HTTP и т.п.) для АП в целом и для каждого абонента, в частности;
- режим подключения АП и абонентов к Сети (постоянный, в т.ч. круглосуточный, временный);
- состав общего и телекоммуникационного программного обеспечения АП и абонентов (ОС, клиентские прикладные программы для сети — Browsers и т.п.);
- число и перечень предполагаемых абонентов (диапазон используемых IP- адресов);
- меры и средства защиты информации от НСД, которые будут применяться на АП, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
- перечень сведений конфиденциального характера, обрабатываемых (хранимых) на АП, подлежащих передаче и получаемых из Сети.

Право подключения к Сети АП, не оборудованного средствами защиты информации от НСД, может быть предоставлено только в случае обработки на АП информации с открытым доступом, оформленной в установленном порядке как разрешенной к открытому опубликованию. В этом случае к АП, представляющим собой автономную ПЭВМ с модемом, специальные требования по защите информации от НСД не предъявляются.

Подключение к Сети АП, представляющих собой внутренние (локальные) вычислительные сети, на которых обрабатывается информация, не разрешенная к открытому опубликованию, разрешается только после установки на АП средств защиты информации от НСД, отвечающих требованиям и рекомендациям, изложенным в подразделе 6.3.

6.2. Взаимодействие абонентских пунктов с Сетью

Подключение АП к Сети должно осуществляться в установленном порядке через провайдера Сети.

Подключение ЛВС предприятия (учреждения) к Сети должно осуществляться через средства разграничения доступа в виде МЭ (Firewall, Брандмауэр). Не допускается подключение ЛВС к Сети в обход МЭ. МЭ должны быть сертифицированы по требованиям безопасности информации.

Доступ к МЭ, к средствам его конфигурирования должен осуществляться только выделенным администратором с консоли. Средства удаленного управления МЭ должны быть исключены из конфигурации.

АП с помощью МЭ должен обеспечивать создание сеансов связи абонентов с внешними серверами Сети и получать с этих серверов только ответы на запросы абонентов. Настройка МЭ должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на АП.

При использовании почтового сервера и Web-сервера предприятия, последние не должны входить в состав ЛВС АП и должны подключаться к Сети по отдельному сетевому фрагменту (через маршрутизатор).

На технических средствах АП должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения АП к Сети (обоснование может корректироваться в установленном на предприятии порядке).

Не допускается активизация не включенных в обоснование прикладных серверов (протоколов) и не требующих привязок протоколов к портам.

Установку программного обеспечения, обеспечивающего функционирование АП, должны выполнять уполномоченные специалисты под контролем администратора. Абоненты АП не имеют права производить самостоятельную установку и модификацию указанного программного обеспечения, однако могут обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия «вирусов», замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения, целиком ложится на абонента АП. При обнаружении фактов такого рода администратор обязан логически (а при необходимости — физически вместе с включающей подсетью) отключить рабочее место абонента от Сети и ЛВС и поставить об этом в известность руководство.

Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого АП (АС) и отвечать требованиям РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

СЗИ НСД, устанавливаемая на автономную ПЭВМ, рабочие станции и серверы внутренней ЛВС предприятия при обработке на них конфиденциальной информации, должна осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки НСД;
- регистрацию фактов отправки и получения абонентом сообщений (файлов, писем, документов).

При этом СЗИ НСД должна запрещать запуск абонентом произвольных программ, не включенных в состав программного обеспечения АП.

Модификация конфигурации программного обеспечения АП должна быть доступна только со стороны администратора, ответственного за эксплуатацию АП.

Средства регистрации и регистрируемые данные должны быть недоступны для абонента.

СЗИ НСД должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводится не реже одного раза в год.

Технические средства АП должны быть размещены либо в отдельном помещении (при автономной ПЭВМ, подключенной к Сети), либо в рабочих помещениях абонентов с принятием организационных и технических мер, исключающих несанкционированную работу в Сети. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки зрения электроакустики. В нерабочее время помещение автономной ПЭВМ, либо соответствующего сервера, сдается под охрану в установленном порядке.

6.3. Рекомендации по созданию абонентского пункта

При создании АП рекомендуется:

По возможности размещать МЭ для связи с внешними Сетями, Web-серверы, почтовые серверы в отдельном ЗП, доступ в которое имел бы ограниченный круг лиц (ответственные специалисты, администраторы). Периодически проверять работоспособность МЭ с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. Не следует устанавливать на МЭ какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.).

При предоставлении абонентам прикладных сервисов исходить из принципа минимальной достаточности. Тем пользователям АП, которым не требуются услуги Сети, не предоставлять их. Пользователям, которым необходима только электронная почта (E-mail), предоставлять только доступ к ней.

Максимальный перечень предоставляемых прикладных сервисов ограничивать следующими: E-mail, FTP, HTTP, Telnet.

При создании АП следует использовать операционные системы со встроенными функциями защиты информации от НСД или использовать сертифицированные СЗИ НСД.

Эффективно использовать имеющиеся в маршрутизаторах средства разграничения доступа (фильтрацию), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов.

В целях контроля за правомерностью использования АП и выявления нарушений требований по защите информации осуществлять анализ принимаемой из Сети и передаваемой в Сеть информации, в том числе на наличие «вирусов». Копии исходящей электронной почты и отсылаемых в Сеть файлов следует направлять в адрес защищенного архива АП для последующего анализа со стороны администратора (службы безопасности).

Проводить постоянный контроль информации, помещаемой на Web-серверы предприятия. Для этого следует назначить ответственного (ответственных) за ведение информации на Web-сервере. Предусмотреть порядок размещения на Web-сервере информации, разрешенной к открытому опубликованию.

Приказом по учреждению (предприятию) назначаются лица (абоненты), допущенные к работам в Сети с соответствующими полномочиями, лица, ответственные за эксплуатацию указанного АП и контроль за выполнением мероприятий по обеспечению безопасности информации при работе абонентов в Сети (руководители подразделений и администраторы).

Вопросы обеспечения безопасности информации на АП должны быть отражены в инструкции, определяющей:

- порядок подключения и регистрации абонентов в Сети;
- порядок установки и конфигурирования на АП общесистемного, прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, Browsers), их новых версий;
- порядок применения средств защиты информации от НСД на АП при взаимодействии абонентов с Сетью;
- порядок работы абонентов в Сети, в том числе с электронной почтой (E-mail), порядок выбора и доступа к внутренним и внешним серверам Сети (Web-серверам);
- порядок оформления разрешений на отправку данных в Сеть (при необходимости);
- обязанности и ответственность абонентов и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с Сетью;
- порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой абонентов Сети.

К работе в качестве абонентов Сети допускается круг пользователей, ознакомленных с требованиями по взаимодействию с другими абонентами Сети и обеспечению при этом безопасности информации и допускаемых к самостоятельной работе в Сети после сдачи соответствующего зачета.

Абоненты Сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;
- знать инструкцию по обеспечению безопасности информации на АП;
- знать правила работы со средствами защиты информации от НСД, установленными на АП (серверах, рабочих станциях АП);
- уметь пользоваться средствами антивирусной защиты;
- после окончания работы в Сети проверить свое рабочее место на наличие «вирусов».

Входящие и исходящие сообщения (файлы, документы), а также используемые при работе в Сети носители информации, учитываются в журналах несекретного делопроизводства. При этом на корпусе (конверте) носителя информации наносится предупреждающая маркировка: «Допускается использование только в Сети _____».

Для приемки в эксплуатацию АП, подключаемого к Сети, приказом по учреждению (предприятию) назначается аттестационная комиссия, проверяющая выполнение установленных требований и реко-

мендаций. Аттестационная комиссия в своей работе руководствуется требованиями и рекомендациями настоящего документа.

По результатам работы комиссии оформляется заключение, в котором отражаются следующие сведения:

- типы и номера выделенных технических средств АП, в т.ч. каждого абонента, их состав и конфигурация;
- состав общего и сервисного прикладного коммуникационного программного обеспечения (ОС, маршрутизаторов, серверов, межсетевых экранов, Browsers и т.п.) на АП в целом и на каждой рабочей станции абонента, в частности: логические адреса (IP-адреса), используемые для доступа в Сети;
- мероприятия по обеспечению безопасности информации, проведенные при установке технических средств и программного обеспечения, в т.ч. средств защиты информации от НСД, антивирусных средств, по защите информации от утечки по каналам ПЭМИН, наличие инструкции по обеспечению безопасности информации на АП.

При работе в Сети ***категорически запрещается***:

- подключать технические средства (серверы, рабочие станции), имеющие выход в Сеть, к другим техническим средствам (сетям), не определенным в обосновании подключения к Сети;
- изменять состав и конфигурацию программных и технических средств АП без санкции администратора и аттестационной комиссии;
- производить отправку данных без соответствующего разрешения;
- использовать носители информации с маркировкой: «Допускается использование только в Сети _____» на рабочих местах других систем (в том числе и автономных ПЭВМ) без соответствующей санкции.

Ведение учета абонентов, подключенных к Сети, организуется в устанавливаемом в учреждении (на предприятии) порядке.

Контроль за выполнением мероприятий по обеспечению безопасности информации на АП возлагается на администраторов АП, руководителей соответствующих подразделений, определенных приказом по учреждению (предприятию), а также руководителя службы безопасности.

7. Технические средства защиты информации

Основной целью технических средств защиты информации является защита акустической информации и побочных излучений технических средств хранения, обработки и передачи информации. Для защиты акустической (речевой) информации используются пассивные и активные методы и средства.

Пассивные методы защиты акустической (речевой) информации направлены на:

- ослабление акустических (речевых) сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов (звукоизоляция);
- ослабление информационных электрических сигналов в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства, имеющие в своем составе электроакустические преобразователи (обладающие микрофонным эффектом);
- обнаружение излучений акустических закладок и побочных электромагнитных излучений диктофонов в режиме записи;
- обнаружение несанкционированных подключений к телефонным линиям связи.

Активные методы защиты акустической (речевой) информации направлены на:

- создание маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки (технические средства пространственного и линейного зашумления);
- создание маскирующих электромагнитных помех в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- электромагнитное подавление диктофонов в режиме записи;
- ультразвуковое подавление диктофонов в режиме записи;
- создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом, с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- создание прицельных радиопомех акустическим и телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;
- подавление (нарушение функционирования) средств несанкционированного подключения к телефонным линиям;
- уничтожение (вывод из строя) средств несанкционированного подключения к телефонным линиям.
- шифрование информации

7.1. Пассивные методы защиты

Ослабление акустических (речевых) сигналов осуществляется путем звукоизоляции помещений.

7.1.1. Звукоизоляция помещений

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них и проводится с целью исключения перехвата акустической (речевой) информации по прямо-

му акустическому (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.) и вибрационному (через ограждающие конструкции, трубы водо-, тепло- и газоснабжения, канализации и т.д.) каналам.

Основное требование к звукоизоляции помещений заключается в том, чтобы за его пределами отношение акустический сигнал/шум не превышало некоторого допустимого значения, исключающего выделение речевого сигнала на фоне естественных шумов средством разведки. Поэтому к помещениям, в которых проводятся закрытые мероприятия, предъявляются определенные требования по звукоизоляции.

Звукоизоляция оценивается величиной ослабления акустического сигнала, которое для сплошных однослойных или однородных ограждений (строительных конструкций) на средних частотах.

Учитывая, что средняя громкость звука говорящего в служебном помещении составляет около 50 ... 60 дБ, то в зависимости от категории помещения его звукоизоляция должна быть не менее норм, приведенных в табл.

Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов.

При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Меньшая часть волны проникает в материал звукоизолирующей конструкции и распространяется в нем, теряя свою энергию в зависимости от длины пути и его акустических свойств. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны.

Характер этого поглощения определяется соотношением частот падающей акустической волны и спектральных характеристик поверхности средства звукоизоляции.

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются двери и окна.

Двери имеют существенно меньшие по сравнению со стенами и межэтажными перекрытиями поверхностные плотности и трудноуплотняемые зазоры и щели. Стандартные двери не удовлетворяют требованиям по защите информации.

Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д.

Применение уплотняющих прокладок повышает звукоизоляцию дверей, однако при этом необходимо учитывать, что в процессе эксплуатации в результате обжатия, износа, затвердевая резиновых прокладок звукоизоляция существенно снижается.

Для защиты информации в особо важных помещениях используются двери с тамбуром, а также специальные двери с повышенной звукоизоляцией.

Для повышения звукоизоляции проводится облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями, а двери обиваются материалами со слоями ваты или войлока и используются дополнительные уплотнительные прокладки.

Звукопоглощающая способность окон, так же как и дверей, зависит, главным образом, от поверхностной плотности стекла и степени прижатия притворов.

Звукоизоляция окон с одинарным остеклением соизмерима со звукоизоляцией одинарных дверей и недостаточна для надежной защиты информации в помещении. Существенно большую звукоизоляцию имеют окна с остеклением в раздельных переплетах с шириной воздушного промежутка более 200 мм или тройное комбинированное остекление.

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). Разработаны конструкции окон с повышенным звукопоглощением на основе стекло-пакетов с герметизацией воздушного промежутка между стеклами и с за-

полнением его различными газовыми смесями или создание в нем вакуума. Повышение звукоизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Необходимо отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резонансных явлений в воздушных промежутках и эффекта волнового совпадения.

Для повышения звукоизоляции в помещениях применяют акустические экраны, устанавливаемые на пути распространения звука на наиболее опасных (с точки зрения разведки) направлениях.

Действие акустических экранов основано на отражении звуковых волн и образовании за экраном звуковых теней. С учетом дифракции эффективность экрана повышается с увеличением соотношения размеров экрана и длины акустической волны. Размеры эффективных экранов превышают более чем в 2-3 раза длину волны. Реально достигаемая эффективность акустического экранирования составляет 8... 10дБ.

Применение акустического экранирования целесообразно при временном использовании помещения для защиты акустической информации. Наиболее часто применяются складные акустические экраны, используемые для дополнительной звукоизоляции дверей, окон, технологических проемов, систем кондиционирования, проточной вентиляции и других элементов ограждающих конструкций, имеющих звукоизоляцию, не удовлетворяющую действующим нормам.

Для повышения звукоизоляции помещений также применяют звукопоглощающие материалы.

Звукопоглощение обеспечивается путем преобразования кинетической энергии акустической волны в тепловую энергию в звукопоглощающем материале. Звукопоглощающие свойства материалов оцениваются коэффициентом звукопоглощения, определяемым отношением энергии звуковых волн, поглощенной в материале, к падающей на поверхность материала и проникающей (неотраженной) в звукопоглощающий материал.

Применение звукопоглощающих материалов при защите акустической информации имеет некоторые особенности по сравнению с звукоизоляцией. Одной из особенностей является необходимость создания непосредственно в помещении акустических условий для обеспечения разборчивости речи в различных его зонах. Таким условием является прежде всего обеспечение оптимального соотношения прямого и отраженного от ограждений акустических сигналов. Чрезмерное звукопоглощение приводит к ухудшению уровня сигнала в различных точках помещения, а большое время реверберации — к ухудшению разборчивости в результате наложения различных звуков.

Обеспечение рациональных значений рассмотренных условий определяется как общим количеством звукопоглощающих материалов в помещении, так и распределением звукопоглощающих материалов по ограждающим конструкциям с учетом конфигурации и геометрических размеров помещений.

Звукопоглощающие 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 (плиты минераловатные «Акмигран», «Акмант», «Силаклор», «Винипор», ПА/С, ПА/О, ПП-80, ППМ, ПММ) 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.). Используются также звукопоглощающие облицовки из слоя пористо-волокнистого материала (стеклянного или базальтового волокна, минеральной ваты) в защитной оболочке из ткани или пленки с перфорированным покрытием (металлическим, гипсовым и др.).

Пористые звукопоглощающие материалы малоэффективны на низких частотах.

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.

Перфорированные резонаторные поглотители представляют собой систему воздушных резонаторов (например, резонаторов Гельмгольца), в устье которых расположен демпфирующий материал.

Повышение звукоизоляции стен и перегородок помещений достигается применением однослойных и многослойных (чаще — двойных) ограждений. В многослойных ограждениях целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например, бетон — поролон).

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, коробов, прокладок, глушителей, вязкоупругих заполнителей и т.д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием сложных акустических фильтров и глушителей.

Следует иметь в виду, что в общем случае звукоизоляция ограждающих конструкций, содержащих несколько элементов, должна оцениваться звукоизоляцией наиболее слабого из них.

Для ведения конфиденциальных разговоров разработаны специальные звукоизолирующие кабины. В конструктивном отношении они делятся на каркасные и бескаркасные. В первом случае на металлический каркас крепятся звукопоглощающие панели. Примером таких кабин являются кабины междугородней телефонной связи. Кабины с двухслойными звукопоглощающими плитами обеспечивают ослабление звука до 35… 40 дБ.

Более высокой акустической эффективностью (большим коэффициентом ослабления) обладают кабины бескаркасного типа. Они собираются из готовых многослойных щитов, соединенных между собой через звукоизолирующие упругие прокладки. Такие кабины дороги в изготовлении, но снижение уровня звука в них может достигать 50 … 55 дБ. Для повышения звукоизоляции кабины минимизируют возможное число стыковочных соединений отдельных панелей между собой и с каркасом кабины. Тщательно герметизируют и уплотняют стыковочные соединения, применяют звукопоглощающие облицовки стен и потолка. В системах вентиляции и кондиционирования воздуха устанавливают специальные глушители звука.

Звукоизолирующие кабины в зависимости от требований к звукоизоляции подразделяются на 4 класса. В диапазоне 63 … 8000 Гц кабины должны обеспечивать ослабление звука: кабины 1-го класса — на 25 … 50 дБ; 2-го класса — на 15 … 49 дБ; 3-го и 4-го классов — 15 … 39 и 15 … 29 дБ соответственно. Наименьшие значения соответствуют низким частотам, наибольшие — высоким (2000 … 4000 Гц).

Для защиты от лазерных микрофонов можно использовать и организационные и технические мероприятия.

К ним можно отнести:

1. Использование погодных и климатических условий (дождь, снег, сильный ветер и т.д.)
2. Ведение переговоров в местах с высоким уровнем шумов.
3. Размещение на местности таким образом, чтобы на пути распространения лазерного луча были естественные и искусственные препятствия.
4. Использование недоступных для лазерного прослушивания помещений.
5. Использование оконных стекол с высокой кривизной поверхности и шероховатостью.
6. Использование аппаратуры предупреждения о лазерном облучении и т.д.

7.1.2. Пассивные методы защиты телефонных линий

При защите телефонных аппаратов и телефонных линий необходимо учитывать несколько аспектов:

- телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений, в которых они установлены, то есть для подслушивания разговоров в этих помещениях;
- телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;

- и, конечно, возможен перехват (подслушивание) телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, имеющих способность преобразовывать акустические колебания в электрические, то есть обладающих «микрофонным эффектом». К ним относятся: звонковая цепь, телефонный и, конечно, микрофонный капсюли. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы.

При положенной трубке телефонный и микрофонный капсюли гальванически отключены от телефонной линии и при подключении к ней специальных высокочувствительных низкочастотных усилителей возможен перехват опасных сигналов, возникающих в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

При использовании для съема информации метода «высокочастотного навязывания», несмотря на гальваническое отключение микрофона от телефонной линии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом.

Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для защиты телефонного аппарата от утечки акустической (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 преобразователей (источников) опасных сигналов.

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.

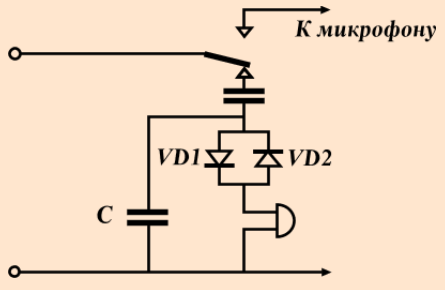


Рис. 7.1. Схема защиты звонковой цепи

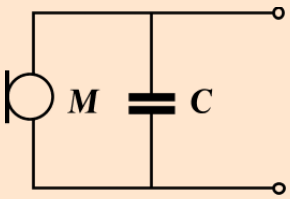


Рис. 7.2. Схема защиты микрофона телефонного аппарата

Диодные ограничители включаются последовательно в линию звонка (см. рис. 7.1) или непосредственно в каждую из телефонных линий (см. рис.7.3).

Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от «высокочастотного навязывания».

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов (см. рис. 7.1, 7.2). 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.

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель. К ним относятся: устройства типа «Экран», «Гранит-8», «Корунд», «Грань-300» и др. (см. рис. 7.3).

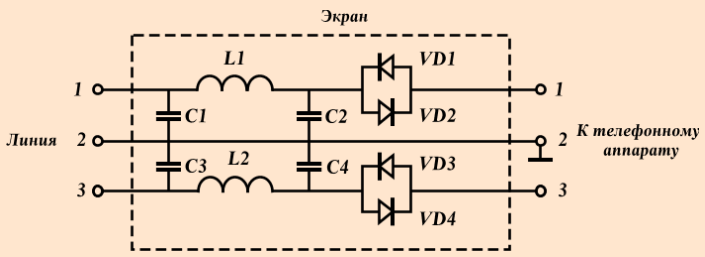


Рис. 7.3. Схема устройства защиты телефонных аппаратов типа «Гранит», сочетающего фильтр и ограничитель

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». В его состав входят:

- электронный коммутатор;
- схема анализа состояния телефонного аппарата, наличия вызывных сигналов и управления коммутатором;
- схема защиты телефонного аппарата от воздействия высоковольтных импульсов.

Устройство работает в следующих режимах: дежурном, передачи сигналов вызова и рабочем.

В дежурном режиме (при положенной телефонной трубке) телефонный аппарат отключен от линии, и устройство находится в режиме анализа поднятия телефонной трубки и наличия сигналов вызова. При этом сопротивление развязки между телефонным аппаратом и линией АТС составляет не менее 20 МОм. Напряжение на выходе устройства в дежурном приеме составляет 5...7В.

При получении сигналов вызова устройство переходит в режим передачи сигналов вызова, при котором через электронный коммутатор телефонный аппарат подключается к линии. Подключение осуществляется только на время действия сигналов вызова.

При поднятии телефонной трубки устройство переходит в рабочий режим и телефонный аппарат подключается к линии. Переход устройства из дежурного в рабочий режим осуществляется при токе в телефонной линии не менее 5 мА.

Изделие устанавливается в разрыв телефонной линии, как правило, при выходе ее из выделенного (защищаемого) помещения или в распределительном щитке (кроссе), находящемся в пределах контролируемой зоны.

Электропитание устройства осуществляется от телефонной линии при токе потребления в дежурном режиме не более 0,3 мА.

Устройство «Барьер -М1» обеспечивает защиту телефонного аппарата не только от утечки информации по электроакустическому каналу, но также и его защиту от воздействия высоковольтных импульсов (напряжением до 1000 В и длительностью до 100 мкс).

Для ***блокировки работы*** (набора номера) несанкционированно подключенных параллельных телефонных аппаратов используются специальные электронные блокираторы.

Принцип работы подобных устройств состоит в следующем. В дежурном режиме устройство защиты производит анализ состояния телефонной линии путем сравнения напряжения в линии и на эталонной (опорной) нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированно подключенного параллельного телефонного аппарата напряжение в линии уменьшается, что фиксируется устройством защиты. Если этот факт зафиксирован в момент ведения телефонного разговора (трубка на защищаемом телефонном аппарате снята), срабатывает звуковая и световая (загорается светодиод несанкционированного подключения к линии) сигнализация. А если факт несанкционированного подключения к линии зафиксирован в отсутствии телефонного разговора (трубка на защищаемом телефонном аппарате не снята), то срабатывает сигнализация и уст-

ройство защиты переходит в режим блокирования набора номера с параллельного телефонного аппарата. В этом режиме устройство защиты шунтирует телефонную линию сопротивлением 600 Ом (имитируя снятие трубки на защищаемом телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата.

Кроме несанкционированного подключения к линии параллельного телефонного аппарата подобные устройства сигнализирует также о фактах обрыва (размыкания) и короткого замыкания телефонной линии.

7.1.3. Фильтрация информационных сигналов

Ослабление информационных электрических сигналов в соединительных линиях ВТСС и исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства осуществляется методами фильтрации сигналов.

Одним из методов ***локализации опасных сигналов***, циркулирующих в технических средствах и системах обработки информации, является фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределы устройства — источника опасного сигнала. Фильтрация в устройствах — рецепторах электромагнитных полей и наводок должна исключить их воздействие на рецептор.

Для фильтрации сигналов в цепях питания ТСПИ используются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы.

Такие трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю. Однако электростатическое поле вокруг экрана также может служить причиной проникновения наводок во вторичную цепь.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

- разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;
- устранения асимметричных наводок;
- ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с малым сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (~104 МОм) и незначительной емкости между обмотками. Указанные особенности трансформаторов для цепей питания обеспечивают более высокую степень подавления наводок, чем обычные трансформаторы [128].

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ.

Средства экранирования, применяемые в разделительных трансформаторах, должны не только устранять влияние асимметричных наводок на защищаемое устройство, но и не допустить на выходе трансформатора симметричных наводок, обусловленных асимметричными наводками на его входе. Применяя в разделительных трансформаторах специальные средства экранирования, можно существенно (более чем на 40 дБ) уменьшить уровень таких наводок.

Помехоподавляющие фильтры.

В настоящее время существует большое количество различных типов фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры и т.д. Основное назначение фильтров — пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы.

Для исключения просачивания информационных сигналов в цепи электропитания используются ***фильтры нижних частот***.

Фильтр нижних частот (ФНЧ) пропускает сигналы с частотами ниже граничной частоты ($f \le f_{гр}$) и подавляет — с частотами выше граничной частоты.

Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем для того, чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность L.

Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот параллельная ветвь должна иметь большую проводимость, тогда колебания этих частот будут ею шунтироваться, и их ток на выходе фильтра будет ослабляться. Таким требованиям отвечает емкость C.

Более сложные многозвенные ФНЧ (Чебышева, Баттерворта, Бесселя и т.д.) конструируют на основе сочетаний различных единичных звеньев.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

- величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
- величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;
- ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;
- габариты и масса фильтров должны быть минимальными;
- фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т.д.);
- конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

- затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц);
- сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;
- ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Рассмотрим влияние этих параметров более подробно.

Напряжение, приложенное к фильтру, должно быть таким, чтобы оно не вызывало пробоя конденсаторов фильтра при различных скачках питающего напряжения, включая скачки, обусловленные переходными процессами в цепях питания. Чтобы при заданных массе и объеме фильтр обеспечивал наилучшее подавление наводок в требуемом диапазоне частот, его конденсаторы должны обладать максимальной емкостью на единицу объема или массы. Кроме того, номинальное значение рабочего напряжения конденсаторов выбирают исходя из максимальных значений допускаемых скачков напряжения цепи питания, но не более их.

Ток через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтра. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное

падение напряжения на ней. Это может привести к тому, что:

- ухудшается эквивалентный коэффициент стабилизации напряжения в цепи питания, содержащей фильтр;
- возникает взаимозависимость переходных процессов в различных нагрузках цепи питания.

Наибольшие скачки напряжения при этом возникают во время отключения нагрузок, так как большинство из них имеет индуктивный характер.

Характеристики фильтров зависят от числа использованных реактивных элементов. Так, например, фильтр из одного параллельного конденсатора или одной последовательной индуктивной катушки может обеспечить затухание лишь 20 дБ/декада вне полосы пропускания, а LC-фильтр из десяти или более элементов — более 200 дБ/декада.

Из-за паразитной связи между входом и выходом фильтра на практике трудно получить затухание более 100 дБ. Если фильтр неэкранированный и сигнал подается на него и снимается с помощью неэкранированных соединений (проводов), то развязка между входом и выходом обычно не превышает 40 … 60 дБ. Для обеспечения развязки более 60 дБ необходимо использовать экранированные фильтры с разъемами и использовать для соединения экранированные провода.

Фильтры с гарантируемым затуханием 100 дБ выполняют в виде узла с электромагнитным экранированием, который помещается в корпус, изготовленный из материала с высокой магнитной проницаемостью магнитного экрана. Этим существенно уменьшается возможность возникновения внутри корпуса паразитной связи между входом и выходом фильтра из-за магнитных электрических или электромагнитных полей.

Из-за влияния паразитных емкостей и индуктивностей фильтр зачастую не обеспечивает требуемого затухания на частотах, превышающих граничную частоту (f_C) на две декады, и полностью может потерять работоспособность на частотах, превышающих граничную частоту на несколько декад.

Ориентировочные значения максимального затухания для сетевых фильтров, приведены в табл. 7.1.

Таблица 7.1

Диапазон частот	Максимальное затухание фильтра вне полосы пропускания, дБ		
	экранированный		неэкранированный
	с разъемами	без разъемов	
Фильтры в цепях питания на токи не более 10 А			
$f_c \le f \le 10 f_c$	80	—	—
$10 f_c \le f \le 100 f_c$	80	—	—
$f > 100 f_c$	70	—	—
Фильтры в цепях питания на токи более 1 0 А			
$f_c \le f \le 10 f_c$	100	—	—
$10 f_c \le f \le 100 f_c$	100	—	—
$f > 100 f_c$	90	—	—

Конструктивно фильтры подразделяются на:

- фильтры на элементах с сосредоточенными параметрами (LC-фильтры) — обычно предназначены для работы на частотах до 300 МГц;
- фильтры с распределенными параметрами (полосковые, коаксиальные или волноводные) — применяются на частотах свыше 1 ГГц;
- комбинированные — применяются на частотах 300 МГц … 1 ГГц.

В настоящее время промышленностью выпускаются несколько серий защитных фильтров (ФП, ФБ, ФПС и др.).

Фильтры серии ФП обеспечивают затухание от 60 до 100 дБ. Они рассчитаны на номинальное напряжение переменного тока от 60 до 500 В и ток — от 2,5 до 70 А. Размеры фильтров составляют от 350×100×60 до 560×210×80 мм, а вес — от 2,5 до 25 кг.

Фильтры серии ФСПК-100 (200) предназначены для установки в четырехпроводных линиях электропитания частотой 50 Гц и напряжением 220/380 В. Максимальный рабочий ток составляет 100 (200) А. В диапазоне частот от 0,02 до 1000 МГц фильтры обеспечивают затухание сигнала не менее 60 дБ.

Конструктивно фильтры ФСПК выполнены в виде двух корпусов (полукомплектов), каждый из которых обеспечивает фильтрацию двухпроводной линии. Размеры одного корпуса составляют 800×320×92 мм, а вес — 18 кг.

7.1.4. Экранирование технических средств

Функционирование любого технического средства информации связано с протеканием по его токоведущим элементам электрических токов различных частот и образованием разности потенциалов между различными точками его электрической схемы, которые порождают магнитные и электрические поля, называемые ***побочными электромагнитными излучениями***.

Узлы и элементы электронной аппаратуры, в которых имеют место большие напряжения и протекают малые токи, создают в ближней зоне электромагнитные поля с преобладанием электрической составляющей. Преимущественное влияние электрических полей на элементы электронной аппаратуры наблюдается и в тех случаях, когда эти элементы малочувствительны к магнитной составляющей электромагнитного поля.

Узлы и элементы электронной аппаратуры, в которых протекают большие токи и имеют место малые перепады напряжения, создают в ближней зоне электромагнитные поля с преобладанием магнитной составляющей. Преимущественное влияние магнитных полей на аппаратуру наблюдается также в случае, если рассматриваемое устройство малочувствительно к электрической составляющей или последняя много меньше магнитной за счет свойств излучателя.

Переменные электрическое и магнитное поля создаются также в пространстве, окружающем соединительные линии (провода, кабели) ТСПИ.

Побочные электромагнитные излучения ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки информации, а также могут оказаться причиной возникновения наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня побочных электромагнитных излучений уделяется большое внимание.

Эффективным методом снижения уровня ПЭМИ является экранирование их источников.

Различают следующие способы экранирования:

- электростатическое;
- магнитостатическое;
- электромагнитное.

Электростатическое и магнитостатическое экранирование основаны на замыкании экраном (обладающим в первом случае высокой электропроводностью, а во втором — магнитопроводностью) соответственно электрического и магнитного полей.

Электростатическое экранирование по существу сводится к замыканию электростатического поля на поверхность металлического экрана и отводу электрических зарядов на землю (на корпус прибора). Заземление электростатического экрана является необходимым элементом при реализации электростатического экранирования. Применение металлических экранов позволяет полностью устранить влияние электростатического поля. При использовании диэлектрических экранов, плотно прилегающих к экранируемому элементу, можно ослабить поле источника наводки в E раз, где E — относительная диэлектрическая проницаемость материала экрана.

Основной задачей экранирования электрических полей является снижение емкости связи между экранируемыми элементами конструкции. Следовательно, эффективность экранирования определяется в основном отношением емкостей связи между источником и рецептором наводки до и после установки заземленного экрана. Поэтому любые действия, приводящие к снижению емкости связи, увеличивают эффективность экранирования.

Экранирующее действие металлического листа существенно зависит от качества соединения экрана с корпусом прибора и частей экрана друг с другом. Особенно важно не иметь соединительных проводов между частями экрана и корпусом.

В диапазонах метровых и более коротких длин волн соединительные проводники длиной в несколько сантиметров могут резко ухудшить эффективность экранирования. На еще более коротких волнах дециметрового и сантиметрового диапазонов соединительные проводники и шины между экранами недопустимы. Для получения высокой эффективности экранирования электрического поля здесь необходимо применять непосредственное сплошное соединение отдельных частей экрана друг с другом.

Узкие щели и отверстия в металлическом экране, размеры которых малы по сравнению с длиной волны, практически не ухудшают экранирование электрического поля.

С увеличением частоты эффективность экранирования снижается.

Основные требования, которые предъявляются к электрическим экранам, можно сформулировать следующим образом:

- конструкция экрана должна выбираться такой, чтобы силовые линии электрического поля замыкались на стенки экрана, не выходя за его пределы;
- в области низких частот (при глубине проникновения ($б$) больше толщины (d), т.е. при $б > d$) эффективность электростатического экранирования практически определяется качеством электрического контакта металлического экрана с корпусом устройства и мало зависит от материала экрана и его толщины;
- в области высоких частот (при $d < б$) эффективность экрана, работающего в электромагнитном режиме, определяется его толщиной, проводимостью и магнитной проницаемостью.

Магнитостатическое экранирование используется при необходимости подавить наводки на низких частотах от 0 до 3…10 кГц.

Основные требования, предъявляемые к магнитостатическим экранам, можно свести к следующим:

- магнитная проницаемость μа материала экрана должна быть возможно более высокой. Для изготовления экранов желательно применять магнитомягкие материалы с высокой магнитной проницаемостью (например, пермаллой);
- увеличение толщины стенок экрана приводит к повышению эффективности экранирования, однако при этом следует принимать во внимание возможные конструктивные ограничения по массе и габаритам экрана;
- стыки, разрезы и швы в экране должны размещаться параллельно линиям магнитной индукции магнитного поля. Их число должно быть минимальным;
- заземление экрана не влияет на эффективность магнитостатического экранирования.

Эффективность магнитостатического экранирования повышается при применении многослойных экранов.

Экранирование высокочастотного магнитного поля основано на использовании магнитной индукции, создающей в экране переменные индукционные вихревые токи (токи Фуко). Магнитное поле этих токов внутри экрана будет направлено навстречу возбуждающему полю, а за его пределами — в ту же сторону, что и возбуждающее поле. Результирующее поле оказывается ослабленным внутри экрана и усиленным вне его. Вихревые токи в экране распределяются неравномерно по его сечению (толщине). Это вызывается явлением поверхностного эффекта, сущность которого заключается в том, что переменное магнитное поле ослабевает по мере проникновения в глубь металла, так как внутренние слои экранируются вихревыми токами, циркулирующими в поверхностных слоях.

Благодаря поверхностному эффекту плотность вихревых токов и напряженность переменного магнитного поля по мере углубления в металл падает по экспоненциальному закону.

Эффективность магнитного экранирования зависит от частоты и электрических свойств материала экрана. Чем ниже частота, тем слабее действует экран, тем большей толщины приходится его делать для достижения одного и того же экранирующего эффекта. Для высоких частот, начиная с диапазона средних волн, экран из любого металла толщиной 0,5 … 1,5 мм действует весьма эффективно. При выборе толщины и материала экрана следует учитывать механическую прочность, жесткость, стойкость против коррозии, удобство стыковки отдельных деталей и осуществления между ними переходных контактов с малым сопротивлением, удобство пайки, сварки и пр.

Для частот выше 10 МГц медная и тем более серебряная пленка толщиной более 0,1 мм дает значительный экранирующий эффект. Поэтому на частотах выше 10 МГц вполне допустимо применение

экранов из фольгированного гетинакса или другого изоляционного материала с нанесенным на него медным или серебряным покрытием.

При экранировании магнитного поля заземление экрана не изменяет величины возбуждаемых в экране токов и, следовательно, на эффективность магнитного экранирования не влияет.

На высоких частотах применяется исключительно ***электромагнитное экранирование.*** Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления. Теория и практика показывают, что с точки зрения стоимости материала и простоты изготовления преимущества на стороне экранированного помещения из листовой стали. Однако при применении сетчатого экрана могут значительно упроститься вопросы вентиляции и освещения помещения. В связи с этим сетчатые экраны также находят широкое применение. Для изготовления экрана целесообразно использовать следующие материалы:

- сталь листовая декапированная ГОСТ 1386-47 толщиной (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм) 0,35; 0,50; 0,60; 0,70; 0,80; 1,00; 1,25; 1,50; 1,75; 2,00;
- сталь тонколистовая оцинкованная ГОСТ 7118-54 толщиной (мм) 0,51; 0,63; 0,76; 0,82; 1,00; 1,25; 1,50;
- сетка стальная тканая ГОСТ 3826-47 номер 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;
- сетка стальная плетеная ГОСТ 5336-50 номер 3; 4; 5; 6;
- сетка из латунной проволоки марки Л-80 ГОСТ 6613-53 0,25; 0,5; 1,0; 1,6; 2,0; 2,5; 2,6.

Металлические листы или полотнища сетки должны быть между собой электрически соединены по всему периметру. Для сплошных экранов это может быть осуществлено электросваркой или пайкой. Шов электросварки или пайки должен быть непрерывным с тем, чтобы получить цельносварную конструкцию экрана,

Для сетчатых экранов пригодна любая конструкция шва, обеспечивающая хороший электрический контакт между соседними полотнищами сетки не реже чем через 10 … 15 мм. Для этой цели может применяться пайка или точечная сварка.

Экран, изготовленный из луженой низкоуглеродистой стальной сетки с ячейкой 2,5 … 3 мм, дает ослабление порядка 55 … 60 дБ, а из такой же двойной (с расстоянием между наружной и внутренней сетками 100 мм) — около 90 дБ. Экран, изготовленный из одинарной медной сетки с ячейкой 2,5 мм, имеет ослабление порядка 65 … 70 дБ.

Необходимая эффективность экрана в зависимости от его назначения и величины уровня излучения ПЭМИН обычно находится в пределах 60… 120 дБ.

Наряду блоками аппаратуры экранированию подлежат и монтажные провода и соединительные линии.

Чтобы уменьшить уровень ПЭМИ, необходимо особенно тщательно выполнять соединение оболочки провода (экрана) с корпусом аппаратуры. Подключение оболочки должно осуществляться путем непосредственного контакта (лучше всего путем пайки или сварки) с корпусом.

Вместе с тем соединение оболочки провода с корпусом в одной точке не ослабляет в окружающем пространстве магнитное поле, создаваемое протекающим по проводу током. Для экранирования магнитного поля необходимо создать поле такой же величины и обратного направления. С этой целью необходимо весь обратный ток экранируемой цепи направить через экранирующую оплетку провода. Для полного осуществления этого принципа необходимо, чтобы экранирующая оболочка была единственным путем для протекания обратного тока.

Высокая эффективность экранирования обеспечивается при использовании витой пары, защищенной экранирующей оболочкой.

На низких частотах приходится использовать более сложные схемы экранирования — коаксиальные кабели с двойной оплеткой (триаксильные кабели).

На более высоких частотах, когда толщина экрана значительно превышает глубину проникновения поля, необходимость в двойном экранировании отпадает. В этом случае внешняя поверхность иг-

рает роль электрического экрана, а по внутренней поверхности протекают обратные токи.

Применение экранирующей оболочки существенно увеличивает емкость между проводом и корпусом, что в большинстве случаев нежелательно. Экранированные провода более громоздки и неудобны при монтаже, требуют предохранения от случайных соединений с посторонними элементами и конструкциями.

Длина экранированного монтажного провода должна быть меньше четверти длины самой короткой волны передаваемого по проводу спектра сигнала. При использовании более длинных участков экранированных проводов необходимо иметь в виду, что в этом случае экранированный провод следует рассматривать как длинную линию, которая во избежании искажений формы передаваемого сигнала должна быть нагружена на сопротивление, равное волновому.

Для уменьшения взаимного влияния монтажных цепей следует выбирать длину монтажных высокочастотных проводов наименьшей, для чего элементы высокочастотных схем, связанные между собой, следует располагать в непосредственной близости, а неэкранированные провода высокочастотных цепей — при пересечении под прямым углом. При параллельном расположении такие провода должны быть максимально удалены друг от друга или разделены экранами, в качестве которых могут быть использованы несущие конструкции электронной аппаратуры (кожух, панель и т.д.). Экранированные провода и кабели следует применять в основном для соединения отдельных блоков и узлов друг с другом.

Кабельные экраны выполняются в форме цилиндра из сплошных оболочек, в виде спирально намотанной на кабель плоской ленты или в виде оплетки из тонкой проволоки. Экраны при этом могут быть однослойными и многослойными комбинированными, изготовленными из свинца, меди, стали, алюминия и их сочетаний (алюминий-свинец, алюминий-сталь, медь-сталь-медь и т.д.).

В кабелях с наружными пластмассовыми оболочками применяют экраны ленточного типа в основном из алюминиевых, медных и стальных лент, накладываемых спирально или продольно вдоль кабеля.

В области низких частот корпуса применяемых многоштырьковых низкочастотных разъемов являются экранами и должны иметь надежный электрический контакт с общей шиной или землей прибора, а зазоры между разъемом и корпусом должны быть закрыты электромагнитными уплотняющими прокладками.

В области высоких частот коаксиальные кабели должны быть согласованы по волновому сопротивлению с используемыми высокочастотными разъемами. При заделке коаксиального кабеля в высокочастотные разъемы жила кабеля не должна иметь натяжения в месте соединения с контактом разъема, а сам кабель должен быть жестко прикреплен к шасси аппаратуры вблизи разъема.

Для эффективного экранирования низкочастотных полей применяются экраны, изготовленные из ферромагнитных материалов с большой относительной магнитной проницаемостью. При наличии такого экрана линии магнитной индукции проходят в основном по его стенкам, которые обладают малым сопротивлением по сравнению с воздушным пространством внутри экрана.

Качество экранирования таких полей зависит от магнитной проницаемости экрана и сопротивления магнитопровода, которое будет тем меньше, чем толще экран и меньше в нем стыков и швов, идущих поперек направления линий магнитной индукции.

Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их информационных кабелей в экранирующий распределительный короб. Когда такого короба не имеется, то приходится экранировать отдельные линии связи.

Для защиты линий связи от наводок необходимо разместить линию в экранирующую оплетку или фольгу, заземленную в одном месте, чтобы избежать протекания по экрану токов, вызванных неэквипотенциальностью точек заземления.

Для защиты линии связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводами линии. Если линия представляет собой одиночный провод, а возвратный ток течет по некоторой заземляющей поверхности, то необходимо максимально приблизить провод к поверхности. Если линия образована двумя проводами, то их необходимо скрутить, образовав бифиляр (витую пару). Линии, выполненные из экранированного провода или коаксиаль-

ного кабеля, в которых по оплетке протекает возвратный ток, также отвечают требованию минимизации площади контура линии.

Наилучшую защиту как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, из которых один используется в качестве электрического экрана), триаксильного кабеля (изолированного коаксильального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского много-проводного кабеля, покрытого с одной или обеих сторон медной фольгой).

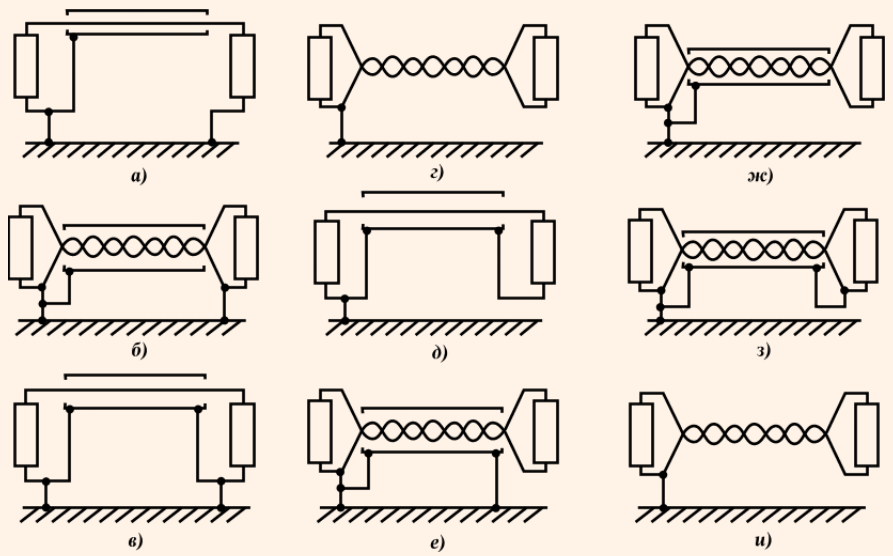


Рис. 7.4. Сравнение защищенности различных цепей от влияния внешних магнитных и электрических цепей: а) 0 дБ; б) –2 дБ; в) –5 дБ; г) –49 дБ, скрученная пара, 18 витков на метр; д) –57 дб; е) –64 дБ, схема предпочтительна на высоких частотах; ж) –64 дБ; з) –71 дБ; и) –79 дБ, скрученная пара (54 витка на метр)

Приведем несколько схем, используемых на частотах порядка 100 кГц. Цепь, показанная на рис. 7.4.*а*, имеет большую площадь петли, образованной «прямым» проводом и «землей». Эта цепь подвержена прежде всего магнитному влиянию. Экран заземлен на одном конце и не защищает от магнитного влияния. Переходное затухание для этой схемы примем равным 0 дБ для сравнения с затуханием схем на рис. 7.4.*б-и*.

Схема на рис. 7.4.*б* практически не уменьшает магнитную связь, так как обратный провод заземлен с обоих концов, и в этом смысле она аналогична схеме на рис. 7.4.*а*. Степень улучшения соизмерима с погрешностью расчета (измерения).

Схема на рис. 7.4.*в* отличается от схемы на рис. 7.4.*а* наличием обратного провода — коаксиального экрана, однако экранирование магнитного поля ухудшено, так как цепь заземлена на обоих концах, в результате чего с «землей» образуется петля большой площади.

Схема на рис. 7.4.*г* позволяет существенно повысить защищенность цепи (–49 дБ) благодаря скрутке проводов. В этом случае (по сравнению со схемой на рис. 7.4.*б*) петли нет, поскольку правый конец цепи не заземлен.

Дальнейшее повышение защищенности цепи достигается применением схемы на рис. 7.4.*с*, коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара на рис. 7.4.*г*.

Площадь петли в схеме на рис. 7.4.*д* не больше, чем в схеме на рис. 7.4.*г*, так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом.

Схема на рис. 7.4.*е* позволяет повысить защищенность цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Кроме того, в этой схеме используется независимый экран.

Схема на рис. 7.4.*ж* имеет ту же защищенность, что и схема на рис. 7.4.*е*: эффект тот же, что и при заземлении на обоих концах, поскольку длина цепи и экрана существенно меньше рабочей длины волны.

Причины улучшения защищенности схемы на рис. 7.4.*з* по сравнению с рис. 7.4.*ж* объяснить трудно. Возможной причиной может быть уменьшение площади эквивалентной петли.

Более плотная скрутка проводов (схема рис. 7.4.*и*) позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь (в обоих проводах токи наводятся одинаково).

Для уменьшения магнитной и электрической связи между проводами необходимо уменьшить площадь петли, максимально разнести цепи и максимально уменьшить длину параллельного пробега линий ТСПИ и посторонними проводниками.

При нулевых уровнях сигналов (0 dB) в соединительных линиях ТСПИ между ними и посторонними проводниками должно обеспечиваться переходное затухание не менее 114 dB (13 Нп). Данное переходное затухание обеспечивается, как правило, при прокладке кабелей ТСПИ на расстоянии не менее 0,1 м от посторонних проводников. При этом допускается прокладка кабелей ТСПИ вплотную с посторонними проводниками при суммарной длине их совместного пробега не более 70 м.

Экранироваться могут не только отдельные блоки (узлы) аппаратуры и их соединительные линии, но и помещения в целом.

В обычных (неэкранированных) помещениях основной экранирующий эффект обеспечивают железобетонные стены домов. Экранирующие свойства дверей и окон хуже. Для повышения экранирующих свойств стен применяются дополнительные средства, в том числе:

- токопроводящие лакокрасочные покрытия или токопроводящие обои;
- шторы из металлизированной ткани;
- металлизированные стекла (например, из двуокиси олова), устанавливаемые в металлические или металлизированные рамы.

В помещении экранируются стены, двери и окна.

При закрытии двери должен обеспечиваться надежный электрический контакт со стенками помещения (с дверной рамой) по всему периметру не реже чем через 10 … 15 мм. Для этого может быть применена пружинная гребенка из фосфористой бронзы, которую укрепляют по всему внутреннему периметру дверной рамы.

Окна должны быть затянуты одним или двумя слоями медной сетки с ячейкой не более 2×2 мм, причем расстояние между слоями сетки должно быть не менее 50 мм. Оба слоя сетки должны иметь хороший электрический контакт со стенками помещения (с рамой) по всему периметру. Сетки удобнее делать съемными и металлическое обрамление съемной части также должно иметь пружинящие контакты в виде гребенки из фосфористой бронзы.

При проведении работ по тщательному экранированию подобных помещений необходимо одновременно обеспечить нормальные условия для работающего в нем человека, прежде всего вентиляцию воздуха и освещение.

Конструкция экрана для вентиляционных отверстий зависит от диапазона частот. Для частот менее 1000 МГц применяются сотовые конструкции, закрывающие вентиляционное отверстие, с прямоугольными, круглыми, шестигранными ячейками. Для достижения эффективного экранирования размеры ячеек должны быть менее одной десятой от длины волны. При повышении частоты необходимые размеры ячеек могут быть столь малыми, что ухудшается вентиляция.

Экранировку электромагнитных волн более 100 дБ можно обеспечить только в специальных экранированных камерах, в которых электромагнитный экран выполнен в виде электрогерметичного стального корпуса, а для ввода электрических коммуникаций используются специальные фильтры.

Размеры экранированного помещения выбирают исходя из его назначения и стоимости. Обычно экранированные помещения строят площадью 6…8 м^2 при высоте 2,5…3 м.

7.1.5. Заземление технических средств

Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.

В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы.

На рис.7.5 представлена одноточечная последовательная схема заземления.

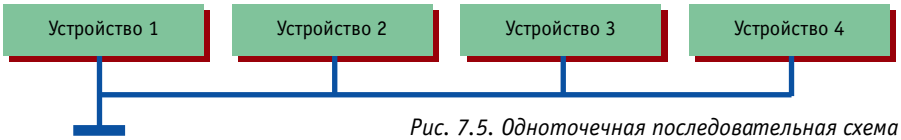


Рис. 7.5. Одноточечная последовательная схема заземления

Эта схема наиболее проста. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

В одноточечной параллельной схеме заземления (рис. 7.6) этого недостатка нет. Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

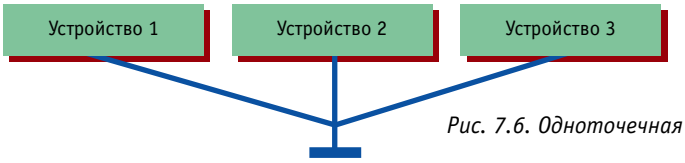


Рис. 7.6. Одноточечная параллельная схема заземления

Многоточечная схема заземления (рис. 7.7) практически свободна от недостатков, присущих одноточечной схеме. В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров.

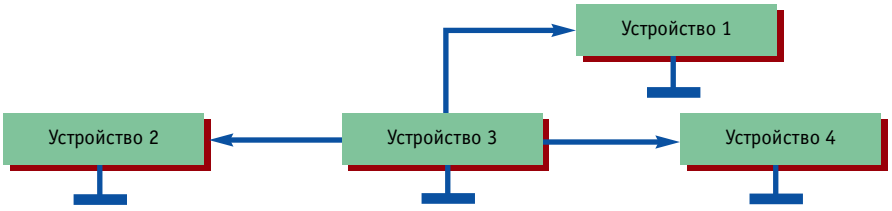


Рис.7.7. Многоточечная схема заземления

Как правило, одноточечное заземление применяется на низких частотах при небольших размерах заземляемых устройств и расстояниях между ними менее 0,5·λ. На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления. В промежуточных случаях эффективна комбинированная (гибридная) система заземления, представляющая собой различные сочетания одноточечной, многоточечной и плавающей заземляющих систем.

Заземление технических средств систем информатизации и связи должно быть выполнено в соответствии с определенными правилами.

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
- сопротивления заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
- в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
- следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;
- качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и вибрации;
- контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
- контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
- запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, имеющие соединение с землей, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации и т.д.

Сопротивление заземления определяется главным образом сопротивлением растекания тока в земле. Величину этого сопротивления можно значительно понизить за счет уменьшения переходного сопротивления между заземлителем и почвой путем тщательной очистки перед укладкой поверхности заземлителя и утрамбовкой вокруг него почвы, а также подсыпкой поваренной соли.

Таким образом, величина сопротивления заземления будет в основном определяться сопротивлением грунта.

Удельное сопротивление различных грунтов (т.е. электрическое сопротивление 1 см^3 грунта) зависит от влажности почвы, ее состава, плотности, температуры и т.п.. и колеблется в очень широких пределах (см. табл. 7.2).

Таблица 7.2. Значения удельного сопротивления различных грунтов

Тип грунта	Удельное сопротивление (ρ), Ом/см^3		
	среднее	минимальное	максимальное
Золы, шлаки, соляные отходы	2370	500	7000
Глина, суглинки, сланцы	4060	340	16300
То же с примесями песка	15800	1020	135 000
Гравий, песок, камни с небольшим количеством глины или суглинков	94000	59000	458 000

Хорошо проводящие грунты теряют свои свойства при отсутствии влаги. Для большинства грунтов 30 % содержания влаги достаточно для обеспечения малого сопротивления. Например, для суглинков удельное сопротивление при влажности 5 % составляет 165 000 Ом/см^3, а при влажности 30 % — 6400 Ом/см^3.

При промерзании сопротивление грунтов резко возрастает. Например, для суглинков удельное сопротивление при влажности 15 % и температуре 20 °С составляет 7200 Ом/см^3,
при температуре –5 °С — 79 000 Ом/см^3, а при температуре –15 °С — 330 000 Ом/см^3.

Орошение почвы вокруг заземлителей 2...5 процентным соляным раствором значительно (в 5...10 раз) снижает сопротивление заземления.

Учесть все факторы, влияющие на проводимость почвы, аналитическим путем практически невозможно, поэтому при устройстве заземления величину удельного сопротивления грунта в тех местах, где предполагается размещение заземления, определяют опытным путем.

Как правило, измерение сопротивления заземления проводится два раза в год (зимой и летом).

При увеличении глубины закапывания l_3 пластины сопротивление заземления уменьшается и при l_3 значительно больше r ($l_3 \ll r$) величина R_3 уменьшается в два раза.

Довольно часто применяют заземляющее устройство в виде вертикально вбитой трубы. Сопротивление заземления зависит в большей степени не от радиуса трубы, а от ее длины. Поэтому при устройстве заземления целесообразнее применять тонкие и длинные трубы (стержни из арматуры).

В табл. 7.3 приведены экспериментально полученные значения сопротивления заземления стержневого заземлителя (∅ 15,9 мм, l = 1,5 м) для различных грунтов.

Таблица 7.3. Значения сопротивления заземления стержневого заземлителя (∅ 15,9 мм, l = 1,5 м) для различных грунтов

Тип грунта	Сопротивление заземления R_3, Ом		
	среднее	минимальное	максимальное
Золы, шлаки, соляные отходы	14	3,5	41
Глина, суглинки, сланцы	24	2	98
То же с примесями песка	93	6	800
Гравий, песок, камни с небольшим количеством глины или суглинков	554	35	2700

В качестве одиночных стержневых заземлителей целесообразно использовать медные заземляющие стержни.

Сопротивление простых одиночных заземлителей оказывается достаточно большим. Поэтому такие заземлители находят применение при невысоких требованиях к заземляющим устройствам или при почвах с очень большой проводимостью.

При повышенных требованиях к величине сопротивления заземления (сопротивление заземления ТСПИ не должно превышать 4 Ом) применяют многократное заземление, состоящее из ряда одиночных симметрично расположенных заземлителей, соединенных между собой.

На практике наиболее часто в качестве заземлителей применяют:

- стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ТСПИ;
- сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

При необходимости устройства высокочастотного заземления нужно учитывать не только геометрические размеры заземлителей, их конструкцию и свойства почвы, но и длину волны высокочастотного излучения. Суммарное высокочастотное сопротивление заземления Z_S складывается из высокочастотного сопротивления магистрали заземления Z_M (провода, идущего от заземляемого устройства до поверхности земли) и из высокочастотного сопротивления самого заземлителя Z_3 (провода, металлического стержня или листа, находящегося в земле).

Величина заземления в основном определяется не сопротивлением заземления, а сопротивлением заземляющей магистрали. Для уменьшения последнего следует стремиться прежде всего к уменьшению индуктивности заземляющей магистрали, что достигается за счет уменьшения ее длины и из-

готовления магистрали в виде ленты, обладающей по сравнению с проводом круглого сечения меньшей индуктивностью. В тех случаях, когда индуктивность заземляющей магистрали можно сделать весьма небольшой или использовать ее для получения последовательного резонанса при блокировании излучающих сетей защитными конденсаторами на землю (например, при комплексном подавлении излучения в помещениях), целесообразно значительно уменьшить величину сопротивления заземлителя Z_3. Уменьшить величину Z_3 можно также многократным заземлением из симметрично расположенных заземлителей.

При этом общее сопротивление заземления будет тем меньше, чем дальше друг от друга расположены отдельные заземлители.

При устройстве заземления в качестве заземлителей чаще всего применяются стальные трубы длиной 2 … 3 м и диаметром 35 … 50 мм и стальные полосы сечением 50 … 100 мм.

Наиболее пригодными являются трубы, позволяющие достигнуть глубоких и наиболее влажных слоев земли, обладающих наибольшей проводимостью и не подвергающихся высыханию или промерзанию. Однако здесь необходимо учитывать, что с уменьшением сопротивления грунта возрастает коррозия металла. Кроме того, применение таких заземлителей не связано со значительными земляными работами, что неизбежно, например, при выполнении заземления из металлических листов или горизонтально закладываемых в землю металлических лент и проводов.

Заземлители следует соединять между собой шинами с помощью сварки. Сечение шин и магистралей заземления по условиям механической прочности и получения достаточной проводимости рекомендуется брать не менее (24×4) мм^2.

Проводник, соединяющий заземлитель с контуром заземления, должен быть луженым для уменьшения гальванической коррозии, а соединения должны быть защищены от воздействия влаги.

Магистрали заземления вне здания необходимо прокладывать на глубине около 1,5 м, а внутри здания — по стене или специальным каналам таким образом, чтобы их можно было внешне осматривать. Соединяют магистрали с заземлителем только с помощью сварки. К заземляемому устройству ТСПИ магистраль подключают с помощью болтового соединения в одной точке.

Для уменьшения сопротивлений контактов наилучшим является постоянное непосредственное соединение металла с металлом, полученное сваркой или пайкой. При соединении под винт необходимо применять шайбы (звездочки или Гровера), обеспечивающие постоянство плотности соединения.

При соприкосновении двух металлов в присутствии влаги возникает гальваническая и (или) электрическая коррозия. Гальваническая коррозия является следствием образования гальванического элемента, в котором влага является электролитом. Степень коррозии определяется положением этих металлов в электрическом ряду.

Электрическая коррозия может возникнуть при соприкосновении в электролите двух одинаковых металлов. Она определяется наличием локальных электротоков в металле, например, токов в заземлениях силовых цепей.

Наиболее эффективным методом защиты от коррозии является применение металлов с малой электрохимической активностью, таких, как олово, свинец, медь. Значительно уменьшить коррозию и обеспечить хороший контакт можно, тщательно изолируя соединения от проникновения влаги.

7.2. Активные методы защиты

В основе активных методов защиты акустической информации лежит использование различного типа генераторов помех, а также применение других специальных технических средств.

7.2.1. Виброакустическая маскировка

В случае если используемые пассивные средства защиты помещений не обеспечивают требуемых норм по звукоизоляции необходимо использовать активные меры защиты.

Активные меры защиты заключаются в создании маскирующих акустических помех средствам разведки, то есть использованием виброакустической маскировки информационных сигналов. В отличие от звукоизоляции помещений, обеспечивающей требуемое ослабление интенсивности звуковой волны за их пределами, использование активной акустической маскировки снижает отношение

сигнал/шум на входе технического средства разведки за счет увеличения уровня шума (помехи).

Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброакустическому и оптико-электронному каналам утечки информации.

Для формирования акустических помех применяются специальные генераторы, к выходам которых подключены звуковые колонки (громкоговорители) или вибрационные излучатели (вибродатчики).

На практике наиболее широкое применение нашли генераторы шумовых колебаний. Именно поэтому активную акустическую маскировку часто называют акустическим зашумлением. Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников шумов. В качестве источников шумовых колебаний используются электровакуумные, газоразрядные, полупроводниковые и другие электронные приборы и элементы.

Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен и с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемые псевдослучайными.

Наряду с шумовыми помехами в целях активной акустической маскировки используют и другие помехи, например, «одновременный разговор нескольких человек», хаотические последовательности импульсов и т.д.

Роль оконечных устройств, осуществляющих преобразование электрических колебаний в акустические колебания речевого диапазона длин волн, обычно выполняют малогабаритные широкополосные громкоговорители, а осуществляющих преобразование электрических колебаний в вибрационные — вибрационные излучатели (вибродатчики).

Громкоговорители систем зашумления устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки, а вибродатчики крепятся на рамах, стеклах, коробах, трубопроводах, стенах, потолках и т.д.

Создаваемые вибродатчиками шумовые колебания в ограждающих конструкциях, трубах, оконном стекле и т.д. приводят к значительному повышению в них уровня вибрационных шумов и тем самым — к существенному ухудшению условий приема и восстановления речевых сообщений средствами разведки.

В настоящее время создано большое количество различных систем активной виброакустической маскировки, успешно используемых для подавления средств перехвата речевой информации. К ним относятся: системы «Заслон», «Кабинет», «Барон», «Фон-В», VNG-006, ANG-2000, NG-101 и др.

В состав типовой системы виброакустической маскировки входят шумогенератор и от 6 до 12 … 25 вибродатчиков (пьезокерамических или электромагнитных). Дополнительно в состав системы могут включаться звуковые колонки (спикеры).

В комплекс «Барон», кроме обычного генератора шума, включены три радиоприемника, независимо настраиваемые на различные радиовещательные станции FM (УКВ-2) диапазона. Смешанные сигналы этих станций используются в качестве помехового сигнала, что значительно повышает эффективность помехи.

Для полной защиты помещения по виброакустическому каналу вибродатчики должны устанавливаться на всех ограждающих конструкциях (стенах, потолке, полу), оконных стеклах, а также трубах, проходящих через помещение. Требуемое количество вибродатчиков для защиты помещения определяется не только его площадью, количеством окон и труб, проходящих через него, но и эффективностью датчиков (эффективный радиус действия вибродатчиков на перекрытии толщиной 0,25 м составляет от 1,5 до 5 м).

В ряде систем виброакустической маскировки возможна регулировка уровня помехового сигнала. Например, в системах «Кабинет» и ANG-2000 осуществляется ручная плавная регулировка уровня помехового сигнала, а в системе «Заслон-2М»- автоматическая (в зависимости от уровня маскируемого речевого сигнала). В комплексе «Барон» возможна независимая регулировка уровня помехового сигнала в трех частотных диапазонах (центральные частоты: 250, 1000 и 4000 Гц).

Для защиты выделенных помещений в основном развертываются стационарные системы виброакустической маскировки, но для защиты временно используемых для проведения закрытых мероприятий могут применяться и мобильные. К таким системам относится, например, мобильная систе-

ма виброакустического зашумления «Фон-В». В состав системы входят: генератор ANG-2000, вибродатчики TRN-2000 и TRN-2000M и металлические штанги для крепления датчиков к строительным конструкциям.

Система обеспечивает защиту помещения площадью до 25 м^2.

Монтаж (демонтаж) системы осуществляется тремя специалистами в течение 30 минут без повреждения строительных конструкций и элементов отделки интерьера.

Для создания акустических помех в небольших помещениях или салоне автомобиля могут использоваться малогабаритные акустические генераторы, например, WNG-023. Генератор имеет размеры 111×70×22 мм и создает помеховый (типа «белый шум») акустический сигнал в диапазоне частот от 100 до 12 000 Гц мощностью 1 Вт. Питание генератора осуществляется от элемента типа «Крона» или сети 220 В.

При организации акустической маскировки необходимо помнить, что акустический шум может создавать дополнительный мешающий фактор для сотрудников и раздражающе воздействовать на нервную систему человека, вызывая различные функциональные отклонения и приводить к быстрой и повышенной утомляемости работающих в помещении. Степень влияния мешающих помех определяется санитарными нормативами на величину акустического шума. В соответствии с нормами для учреждений величина мешающего шума не должна превышать суммарный уровень 45 дБ.

7.2.2. Активные методы и средства защиты телефонных линий

Активные методы защиты от утечки информации по электроакустическому каналу предусматривают линейное зашумление телефонных линий. 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 МП-1А (защита аналоговых телефонных аппаратов) и МП-1Ц П-1А (защита цифровых телефонных аппаратов) и др.

Для защиты акустической (речевой) информации в выделенных помещениях наряду с защитой телефонных аппаратов необходимо принимать меры и для защиты непосредственно телефонных линий, так как они могут использоваться в качестве источников питания акустических закладок, установленных в помещениях, а также для передачи информации, получаемой этими закладками.

При этом используются как пассивные, так и активные методы и средства защиты. Пассивные методы защиты основаны на блокировании акустических закладок, питающихся от телефонной линии в режиме положенной трубки, а активные — на линейном зашумлении линий и уничтожении (электрическом «выжигании») закладных устройств или их блоков питания путем подачи в линию высоковольтных импульсов.

Защита телефонных разговоров от перехвата осуществляется главным образом активными методами. К основным из них относятся:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения);
- подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод «обнуления»);
- подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод);
- подача в телефонную линию высоковольтных импульсов (метод «выжигания»).

Суть ***метода синфазной маскирующей низкочастотной (НЧ) помехи*** заключается в подаче в каждый провод телефонной линии с использованием единой системы заземления аппаратуры АТС и нулевого провода электросети 220 В (нулевой провод электросети заземлен) согласованных по амплитуде и фазе маскирующих сигналов речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 … 3400 Гц). В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не оказывают мешающего воздействия на полезный сигнал (телефонный разговор). Если же информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А так как его уровень значительно превосходит полезный сигнал, то перехват информации (выделение полезного сигнала) становится невозможным.

В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные последовательности импульсов).

Метод синфазного маскирующего низкочастотного сигнала используется для подавления телефонных радиозакладок (как с параметрической, так и с кварцевой стабилизацией частоты) с последовательным (в разрыв одного из проводов) включением, а также телефонных радиозакладок и диктофонов с подключением к линии (к одному из проводов) с помощью индукционных датчиков различного типа.

Метод ***высокочастотной маскирующей помехи*** заключается в подаче во время разговора в телефонную линию широкополосного маскирующего сигнала в диапазоне высших частот звукового диапазона.

Данный метод используется для подавления практически всех типов подслушивающих устройств как контактного (параллельного и последовательного) подключения к линии, так и подключения с использованием индукционных датчиков. Однако эффективность подавления средств съема информации с подключением к линии при помощи с индукционных датчиков (особенно не имеющих предусилителей) значительно ниже, чем средств с гальваническим подключением к линии.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы типа «белого шума» или дискретные сигналы типа псевдослучайной последовательности импульсов.

Частоты маскирующих сигналов подбираются таким образом, чтобы после прохождения селективных цепей модулятора закладки или микрофонного усилителя диктофона их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии во время разговоров абонентов), но в то же время эти сигналы не ухудшали качество телефонных разговоров. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на полезный сигнал. Обычно используются частоты в диапазоне от 6 … 8 кГц до 16 … 20 кГц. Например, в устройстве Sel SP-17/T помеха создается в диапазоне 8 … 10 кГц.

Такие маскирующие помехи вызывают значительные уменьшение отношения сигнал/шум и искажения полезных сигналов (ухудшение разборчивости речи) при перехвате их всеми типами подслушивающих устройств. Кроме того, у радиозакладок с параметрической стабилизацией частоты («мягким» каналом) как последовательного, так и параллельного включения наблюдается «уход» несущей частоты, что может привести к потере канала приема.

Для исключения воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты устанавливается специальный низкочастотный фильтр с граничной частотой 3,4 кГц, подавляющий (шунтирующий) помеховые сигналы и не оказывающий существенного влияния на прохождение полезных сигналов. Аналогичную роль выполняют полосовые фильтры, установленные на городских АТС, пропускающие сигналы, частоты которых соответствуют стандартному телефонному каналу (300 Гц … 3,4 кГц), и подавляющие помеховый сигнал.

Метод ультразвуковой маскирующей помехи в основном аналогичен рассмотренному выше. Отличие состоит в том, что используются помеховые сигналы ультразвукового диапазона с частотами от 20 …25 кГц до 50… 100 кГц.

Метод повышения напряжения заключается в поднятии напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных радиоза-

кладок. Поднятие напряжения в линии до 18 ... 24 В вызывает у радиозакладок с последовательным подключением и параметрической стабилизацией частоты «уход» несущей частоты и ухудшение разборчивости речи вследствие размытия спектра сигнала. У радиозакладок с последовательным подключением и кварцевой стабилизацией частоты наблюдается уменьшение отношения сигнал/шум на 3 ... 10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде случаев просто отключаются.

Метод «обнуления» предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Этот метод используется для нарушения функционирования подслушивающих устройств с контактным параллельным подключением к линии и использующих ее в качестве источника питания. К таким устройствам относятся: параллельные телефонные аппараты, проводные микрофонные системы с электретными микрофонами, использующие телефонную линию для передачи информации, акустические и телефонные закладки с питанием от телефонной линии и т.д.

Метод низкочастотной маскирующей помехи заключается в подаче в линию при положенной телефонной трубке маскирующего сигнала (наиболее часто, типа «белого шума») речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала: 300 ... 3400 Гц) и применяется для подавления проводных микрофонных систем, использующих телефонную линию для передачи информации на низкой частоте, а также для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки в режиме записи шума (то есть при отсутствии полезного сигнала).

Компенсационный метод используется для односторонней маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии.

Суть метода заключается в следующем. При передаче скрываемого сообщения на приемной стороне в телефонную линию при помощи специального генератора подается маскирующая помеха (цифровой или аналоговый маскирующий сигнал речевого диапазона с известным спектром). Одновременно этот же маскирующий сигнал («чистый» шум) подается на один из входов двухканального адаптивного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет полезный сигнал, который подается на телефонный аппарат или устройство звукозаписи.

Недостатком данного метода является то, что маскировка речевых сообщений односторонняя и не позволяет вести двухсторонние телефонные разговоры.

Метод «выжигания» реализуется путем подачи в линию высоковольтных (напряжением более 1500 В) импульсов, приводящих к электрическому «выжиганию» входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

При использовании данного метода телефонный аппарат от линии отключается. Подача импульсов в линию осуществляется два раза. Первый (для «выжигания» параллельно подключенных устройств) — при разомкнутой телефонной линии, второй (для «выжигания» последовательно подключенных устройств) — при закороченной (как правило, в центральном распределительном щитке здания) телефонной линии.

Для 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.

На отечественном рынке имеется большое разнообразие средств защиты. Среди них можно выделить следующие: «SP 17/T», «SI-2001», «КТЛ-3»,»КТЛ-400», «Ком-3», «Кзот-06», «Цикада-М», «Прокруст» (ПТЗ-003), «Прокруст-2000», «Консул», «Гром-ЗИ-6», «Протон», «Скит»(обеспечивающий защиту от ПЭМИН в соответствии с требованиями ФСТЭК) и др.

В активных устройствах защиты телефонных линий наиболее часто реализованы метод высокочастотной маскирующей помехи («SP 17/T», «КТЛ-3»,»КТЛ-400», «Ком-3», «Прокруст» (ПТЗ-003), «Прокруст-2000»,»Гром-ЗИ-6», «Протон» и др.) и метод ультразвуковой маскирующей помехи («Прокруст» (ПТЗ-003), «Гром-ЗИ-6»).

Метод синфазной низкочастотной маскирующей помехи используется в устройстве «Цикада-М», а метод низкочастотной маскирующей помехи — в устройствах «Прокруст», «Протон», «Кзот-06» и др.

Метод «обнуления» применяется, например, в устройстве «Цикада-М», а метод повышения напряжения в линии — в устройстве «Прокруст».

Компенсационный метод маскировки речевых сообщений, передаваемых абоненту по телефонной линии, реализован в изделии «Туман».

Большинство устройств защиты производят автоматическое измерение напряжения в линии и отображают его значение на цифровом индикаторе. В приборе «Гром-ЗИ-6» на цифровом индикаторе отображается уровень уменьшения напряжения в линии.

Устройства защиты телефонных линий имеют сравнительно небольшие размеры и вес (например, изделие «Прокруст» при размерах 62×155×195 мм весит 1 кг). Питание их, как правило, осуществляется от сети переменного тока 220 В. Однако некоторые устройства (например, «Кзот-06») питаются от автономных источников питания.

Для вывода из строя («выжигания» входных каскадов) средств несанкционированного съема информации с гальваническим подключением к телефонной линии используются устройства типа «ПТЛ-1500, «КС-1300», КС-1303», «Кобра» и т.д.

Приборы используют высоковольтные импульсы напряжением не менее 1500 ... 1600 В. Мощность «выжигающих» импульсов составляет 15 ... 50 ВА. Так как в схемах закладок применяются миниатюрные низковольтные детали, то высоковольтные импульсы их пробивают и схема закладки выводится из строя.

«Выжигатели» телефонных закладок могут работать как в ручном, так и автоматическом режимах. Время непрерывной работы в автоматическом режиме составляет от 20 секунд до 24 часов.

Устройство «КС-1300» оборудовано специальным таймером, позволяющим при работе в автоматическом режиме устанавливать временной интервал подачи импульсов в линию в пределах от 10 минут до 2 суток.

Наряду со средствами активной защиты на практике широко используются различные устройства, позволяющие контролировать некоторые параметры телефонных линий и устанавливать факт несанкционированного подключения к ним.

Методы контроля телефонных линий в основном основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: амплитуд напряжения и тока в линии, а также значений емкости, индуктивности, активного и реактивного сопротивления линии.

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения. При настройке оператор фиксирует значение напряжение, соответствующее нормальному состоянию линии (когда к линии не подключены посторонние устройства), и порог тревоги. При уменьшении напряжения в линии более установленного порога устройством подается световой или звуковой сигнал тревоги.

На принципах измерения напряжения в линии построены и устройства, сигнализирующие о размыкании телефонной линии, которое возникает при последовательном подключении закладного устройства.

Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет «микрофонного эффекта» в элементах телефонного аппарата и высокочастотного «навязывания».

Устройства контроля телефонных линий, построенные на рассмотренном принципе, реагируют на изменения напряжения, вызванные не только подключением к линии средств съема информации, но и колебаниями напряжения на АТС (что для отечественных линий довольно частое явление), что приводит к частым ложным срабатываниям сигнализирующих устройств. Кроме того, эти устройства не позволяют выявить параллельное подключение к линии высокоомных (с сопротивлением в несколько МОм) подслушивающих устройств. Поэтому подобные устройства не находят широкого применения на практике.

Принцип работы более сложных устройств основан на периодическом измерении и анализе нескольких параметров линии (наиболее часто: напряжения, тока, а также комплексного (активного и реактивного) сопротивления линии). Такие устройства позволяют определить не только факт подключения к линии средств съема информации, но и способ подключения (последовательное или параллельное). Например, контроллеры телефонных линий «КТЛ-2», «КТЛ-3» и «КТЛ-400» за 4 минуты позволяют обнаружить закладки с питанием от телефонной линии независимо от способа, места и времени их подключения, а также параметров линии и напряжения АТС. Приборы также выдают световой сигнал тревоги при кратковременном (не менее 2 секунд) размыкании линии.

Современные контроллеры телефонных линий, как правило, наряду со средствами обнаружения подключения к линии устройств несанкционированного съема информации, оборудованы и средствами их подавления. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии.

Шифрование информации

Шифраторы обеспечивают кодирование телефонных и радиопереговоров.

Различают три класса кодирования информации. ***Маскираторы*** — наиболее распространенный и наименее устойчивый к декодированию класс приборов. Защита от прослушивания обеспечивается тем, что аппарат кодирования, подключенный к телефону, разбивает речь абонента на определенные отрезки времени и тасует их как колоду карт. Этот метод шифрации называется инверсией спектра, а аппараты, в которых он использован — инверторами. Чаще всего они имеют форму подставки под телефонный аппарат или накладки на телефонную трубку. Для радиостанций выпускаются специальные инверсионные платы, встраиваемые внутрь корпуса. Несмотря на кажущуюся надежность подобной системы защиты, время, требуемое на дешифрацию подобной системы защиты исчисляется несколькими часами.

Надежнее ***аппаратура временной стойкости***. Время, необходимое для подбора ключей, варьируется от нескольких дней до многих месяцев. И, наконец, ***системы постоянной стойкости*** обеспечивают своим пользователям гарантированное сохранение конфиденциальной информации: Принцип действия таких систем заключается в непрерывной смене не только ключей кодирования, но и самой системы смены ключей.

Защиту (шифровку) специалисты делят на мягкую и жесткую. К мягкой относят такую, которую можно взломать (расшифровать) за десять минут, к жесткой — над которой ломать голову придется несколько лет. Качественная защита обеспечивается качественной техникой. Получить разрешение на приобретение такой аппаратуры можно только с благословения ФАПСИ (Федеральное агентство правительственной связи и информации при Президенте Российской Федерации и их органы на местах).

7.2.3. Пространственное и линейное зашумление

Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) ТСПИ и тем самым к уменьшению отношения опасный сигнал/шум (с/ш). Однако в ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение с/ш превышает допустимое значение. В этом случае применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

Защита от перехвата побочных электромагнитных излучений и наводок (ПЭМИН) самого различного характера предполагает:

- размещение источников ПЭМИН на максимально возможном удалении от границы охраняемой зоны;
- использование средств пространственного и линейного электромагнитного зашумления;

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется *пространственное зашумление*, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС — *линейное зашумление*.

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются следующие требования:

- система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- создаваемые помехи не должны иметь регулярной структуры;
- уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ТСПИ;
- система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);
- на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по ЭМС.

Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ТСПИ.

В системах пространственного зашумления в основном используются помехи типа «*белого шума*» или «*синфазные помехи*».

Системы, реализующие метод «синфазной помехи», в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, система зашумления генерирует «имитационную помеху», по спектральному составу соответствующую скрываемому сигналу.

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа «белый шум», то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д.

Генераторы шума выполняются или в виде отдельного блока с питанием от сети 220В («Гном», «Волна», «ГШ-1000» и др.), или в виде отдельной платы, вставляемой (встраиваемой) в свободный слот системного блока ПЭВМ и питанием от общей шины компьютера («ГШ-К-1000», «Смог» и др.).

Основные характеристики генераторов шума, используемых для пространственного зашумления, представлены в каталоге. Генераторы, выполненные в виде отдельного блока, имеют сравнительно небольшие размеры и вес. Например, генератор шума «Гном-3» при размерах 307×95×49 мм весит 1,8 кг.

Диапазон рабочих частот генераторов шума от 0,01 … 0,1 до 1000 МГц. При мощности излучения около 20 Вт обеспечивается спектральная плотность помехи 40 … 80 дБ.

В системах пространственного зашумления в основном используются слабонаправленные рамочные жесткие и гибкие антенны. Рамочные гибкие антенны выполняются из обычного провода и разворачиваются в двух-трех плоскостях, что обеспечивает формирование помехового сигнала как с вертикальной, так и с горизонтальной поляризацией во всех плоскостях.

При использовании систем пространственного зашумления необходимо помнить, что наряду с помехами средствам разведки создаются помехи и другим радиоэлектронным средствам (например, системам телевидения, радиосвязи и т.д.). Поэтому при вводе в эксплуатацию системы пространственного зашумления необходимо проводить специальные исследования по требованиям обеспечения электромагнитной совместимости (ЭМС). Кроме того, уровни помех, создаваемые системой зашумления, должны соответствовать санитарно-гигиеническим нормам. Однако нормы на уровни электромагнитных излучений по требованиям ЭМС существенно строже санитарно-гигиенических норм. Следовательно, основное внимание необходимо уделять выполнению норм ЭМС.

Пространственное зашумление эффективно не только для закрытия электромагнитного, но и электрического каналов утечки информации, так как помеховый сигнал при излучении наводится в соединительных линиях ВТСС и посторонних проводниках, выходящих за пределы контролируемой зоны.

Системы линейного зашумления применяются для маскировки наведенных опасных сигналов в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны. Они используются в том случае, если не обеспечивается требуемый разнос этих проводников и ТСПИ (то есть не выполняется требование по Зоне № 1), однако при этом обеспечивается требование по Зоне № 2 (то есть расстояние от ТСПИ до границы контролируемой зоны больше, чем Зона № 2).

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который гальванически подключается в зашумляемую линию (посторонний проводник). На практике наиболее часто подобные системы используются для зашумления линий электропитания (например, линий электропитания осветительной и розеточной сетей).

8. Средства защиты информации в вычислительных системах

8.1. Средства защиты от НСД

8.1.1. Программно-аппаратные комплексы защиты информации

В соответствии с ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» (дата введения 1.07.97 г.) под ***средством защиты информации*** понимают — техническое, программное средство, вещество и/или материал, предназначенное или используемое для защиты информации. А под ***защитой информации*** — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

К *аппаратным* — относятся средства защиты информации, входящие в состав аппаратуры АС.

Программными называются средства защиты информации, функционирующие в составе программного обеспечения АС.

Рынок средств информационной безопасности представлен многочисленными продуктами, реализующими различные технологии защиты. В таблице 8.1. приведены основные средства защиты информации автоматизированных систем. Многие из этих средств имеют действующие сертификаты ФЭСТЭК России.

Условно можно выделить две категории средств защиты — традиционные и все остальные. К ***традиционным средствам защиты*** можно отнести ***системы разграничения доступа и межсетевые экраны***. Первые средства реализуют разграничение доступа конкретных пользователей к ресурсам конкретного компьютера или всей сети, а вторые — разграничивают доступ между двумя участками сети с различными требованиями по безопасности.

Программно-аппаратные комплексы Secret Net версии 4.0. предназначены для защиты информации, хранимой и обрабатываемой на автономных персональных компьютерах и рабочих станциях и серверах ЛВС, работающих под управлением операционных систем (ОС) Windows 95/98 и Windows NT/ 2000.

Основные возможности комплекса Secret Net:

- идентификация пользователей при помощи специальных аппаратных средств (Touch Memory, Smart Card, Smarty, Proximity и т.п.);
- аутентификация по паролю длиной до 16 символов;
- поддержка автоматической смены пароля пользователя по истечении заданного интервала времени;
- аппаратная поддержка защиты от несанкционированной загрузки ОС с гибкого диска и CD-ROM диска;
- разграничение доступа пользователей к ресурсам компьютера с помощью механизмов дискреционного и мандатного управления доступом;
- создание для любого пользователя ограниченной замкнутой среды программного обеспечения (списка разрешенных для запуска программ);
- управление временем работы всех пользователей;
- возможность объединения пользователей в группы для упрощения управления их доступом к совместно используемым ресурсам;
- регистрация действий пользователя в системном журнале;
- поддержка для каждого пользователя индивидуальных файлов Config.sys и Autoexec.bat;
- защита компьютера от проникновения и размножения вредоносных программ;
- контроль целостности средств защиты, среды выполнения программ и самих прикладных программ;
- гибкие средства администрирования системы защиты с использованием механизма привилегий, позволяющего распределить административные функции между различными пользователями компьютера.

Особенности сетевого варианта:

- усиленная идентификация и аутентификация;
- криптографическая защита данных;
- централизованный мониторинг состояния безопасности информационной системы и управление защитными механизмами.

Сетевой вариант Secret Net предоставляет администратору безопасности возможность централизованного управления защитными механизмами клиентов Secret Net, мониторинга состояния безопасности информационной системы, оперативного управления рабочими станциями в случае попыток НСД, централизованной обработки журналов регистрации и генерации отчетов.

Таблица 8.1. Средства защиты информации

Средства защиты информации автоматизированных систем			
наименование	**тип**		**пример**
межсетевые экраны	сегментные		*Check Point* FireWall-1*; *ОАО Элвис*+ Застава**, *ОАО ИнфоТеКС* VIPNet Office Firewall**, *ООО АМИКОН* ФПСУ-IP**
	встраиваемые		*Network -1* Cyberwall-Plus
	персональные		*ОАО ИнфоТеКС* VIPNet Personal Firewall**, *McAfee* Personal Firewall; *Agnitum* Outpost Firewall
системы разграничения доступа	сетевые		*НИП Информзащита* Secret Net**; *ГУП СЦПС «Спектр»* Спектр-Z(M)**, *ОКБ САПР* Аккорд**, *НИИ ПУИиМ академии ВН* Страж NT 2.0**, *Конфидент* Dallas Lock**
	локальные		
	системы идентификации и аутентификации (СИА)		*НИП Информзащита* Соболь-PCI**, *ОКБ САПР* Аккорд-АМД3**, *АНКАД* КРИПТОН-Замок/ PCI**
системы построения VPN	на основе	сетевых ОС	Windows NT, 2000 и др.
		маршрутизаторов	Cisco IOS 12.x*
		МЭ	*Check Point* FireWall-1* Cisco PIX 520*
		специализированного ПО	*Digital Equipment* Alta Vista Tunnel 97; *ОАО Элвис*+ Застава 2.5/3.3**, *ОАО ИнфоТеКС* VipNet Office**
		специализированных аппаратно-программных средств	*НИП Информзащита* Континент-К**; *МО ПНИЭИ* Шифратор IP пакетов
системы обнаружения атак (СОА)	средства антивирусной защиты	рабочих станций	*ЗАО ДиалогНаука* Антивирусный пакет Doctor Web 4.x**, *ЗАО Лаборатория Касперского* Антивирус Касперского 3.5**, *SYMANTEC* Norton Antivirus Suite v.3.0**
		серверов ЛВС	
		МЭ — антивирусных шлюзов	*ЗАО Лаборатория Касперского* Антивирус Касперского для CheckPoint Firewall**
	СОА на уровне сети		*ISS* RealSecure Network Engine, NFR, Snort
	СОА на уровне хоста		*ISS* RealSecure System Agent, RealSecure Desktop
средства анализа защищенности	сетевого уровня		*ISS* Internet Scanner, Wireless Scanner, Network Mapper, *Symantec* NetRecon, Nessus, *Positive Technologies* XSpider 7.0
	системного уровня		*ISS* System Scanner, *Symantec* Enterprise Security Manager
			ISS Database Scanner
средства защиты электронных документов	программно-аппаратный комплекс		Удостоверяющий центр КриптоПро
	средства заверения электронных документов		*ЛАН Крипто* Нотариус, Веста, КриптоБанк, КриптоПро (CSP,TLS)

Курсивом выделены названия компаний-производителей.
** На отдельные изделия имеется сертификат Гостехкомиссии России.*
*** На производство данного изделия имеется сертификат Гостехкомиссии РФ (использована информация с Интернет-сайта www.lissi.ru).*

Система защиты информации от НСД «Страж NT 2.0» предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах. СЗИ «Страж NT 2.0» функционирует в среде операционных систем Windows NT 4.0, Windows 2000, Windows XP и устанавливается как на автономных рабочих местах, так и на рабочих станциях и файл-серверах локальной вычислительной сети. Сертификат Гостехкомиссии России № 837 от 29.12.2003 года.

Основные возможности:

- идентификация и аутентификация пользователей при входе в систему по идентификатору и паролю;
- блокировка клавиатуры на время загрузки операционной системы (за исключением администратора безопасности);
- управление запуском всех системных компонентов, включая драйверы, службы и прикладные программы пользователей;
- создание изолированной программной среды для пользователей;
- дискреционный контроль доступа к ресурсам системы;
- мандатный контроль доступа к защищаемым ресурсам, в т.ч. прикладных программ;
- контроль потоков защищаемой информации;
- автоматическое затирание защищаемых файлов при их удалении;
- контроль целостности информационных массивов и программной среды.

В качестве идентификатора пользователя в данной версии СЗИ «Страж NT 2.0» могут применяться стандартная дискета (3,5"), устройства iButton, USB — ключи eToken R2, eToken Pro, Guardant.

Программно-аппаратные комплексы «АККОРД-1.95» и «АККОРД-NT/2000»

Предназначены для применения на ПЭВМ типа IBM PC AT в качестве средства защиты информационных ресурсов от несанкционированного доступа. В состав программно-аппаратного комплекса «АККОРД» входит программное обеспечение разграничения доступа и аппаратный модуль «Аккорд-АМД3». Программное обеспечение реализует возможности разграничения доступа к аппаратно-программным ресурсам ПЭВМ при работе пользователя в ОС DOS, Windows 9.x («АККОРД-1.95») и Windows NT, Windows 2000/XP («АККОРД-NT/2000»).

Программное обеспечение позволяет:

- описать правила разграничения доступа к программным и аппаратным ресурсам с использованием полного набора атрибутов;
- реализовать индивидуальную изолированную программную среду для каждого пользователя;
- вводить временные ограничения работы пользователя на защищаемой ПЭВМ;
- создавать каждому пользователю индивидуальный пакет файлов для контроля целостности;
- реализовать контроль доступа пользователей к печати;
- фиксировать все действия пользователей в расширенном журнале регистрации.

Комплекс «АккордСеть-NDS» обеспечивает защиту сетевых ресурсов в гетерогенных вычислительных сетях с операционными системами Netware 4.11, IntraNetware, Netware 4.2, Netware 5, BorderManager 3.5, Windows NT Server 4.0, HP-UX 10.20, HP-UX 10.30, Sun Solaris 2.6, Sun Solaris 7, Linux Red Hat, NCR Unix SVR4 MP-RAS 3.0.

Главной особенностью комплекса «АккордСеть-NDS» является использование и усиление защитных функций, предоставляемых службами единого каталога фирмы Novell (Novell Directory Services — NDS), развернутыми на Сервере безопасности, который функционирует в среде Novell Netware 5. В качестве устройства аппаратной поддержки используется контроллер «Аккорд-АМД3».

Другой особенностью комплекса АккордСеть-NDS является то, что защита устанавливается не на все компьютеры сети, а только на те Сервера и рабочие станции, защита которых необходима при функционировании в сети конкретного экземпляра защищаемой АС.

Для защиты сетей, не содержащих серверов netware, устанавливается сервер безопасности комплекса, функционирующий в среде netware5, который и становится одним из основных звеньев системы защиты сетевых ресурсов.

Система Dallas Lock предназначена для защиты от несанкционированного доступа к информации, хранимой и обрабатываемой в автономных ПЭВМ под управлением ОС Windows 95/98 (Dallas Lock 4.1), Windows NT 4.0 (Dallas Lock 5.0), Windows 9x (Dallas Lock 6.0.) и Windows 2000/XP (Dallas Lock 7.0.). В качестве средства идентификации пользователей используются персональные электронные идентификаторы Touch Memory или Proximity.

Комплекс Dallas Lock 4.1 for Administrator предназначен для удаленного управления и контроля сетевых рабочих станций пользователей с рабочей станции администратора.

На сегодняшний день существует несколько версий комплекса Dallas Lock:

- Программно-аппаратные — Dallas Lock 4.1 и Dallas Lock 5.0;
- Программные — Dallas Lock 6.0. и Dallas Lock 7.0.

Аппаратная часть системы предлагается как для ISA, так и PCI-слотов.

Основные возможности:

- идентификация пользователей до загрузки ОС при помощи идентификаторов Touch Memory;
- аутентификация пользователей по паролю длиной до 16 символов;
- регистрация всех попыток включения ПЭВМ и входа в систему;
- разграничение доступа пользователей к защищаемым ресурсам;
- регистрация событий операционной системы и действий пользователей;
- контроль целостности защищаемых ресурсов.

Система защиты информации от НСД «Спектр-М» предназначена для защиты от НСД двоичной информации, обрабатываемой и хранимой на средствах вычислительной техники (СВТ) как в однопользовательском, так и в многопользовательском режиме эксплуатации.

Система обеспечивает защиту информации от НСД при использовании СВТ автономно и в составе вычислительных сетей. Система «Спектр-М» функционирует на ЭВМ, под управлением операционных систем (ОС) Windows 95 — 98. Сертификат Гостехкомиссии России № 251 от 20.07.1999 г.

Основные функциональные характеристики системы «Спектр-М»:

- идентификация и аутентификация пользователя;
- хранение и обработка информации в преобразованном виде;
- управление доступом по дискреционному принципу контроля доступа;
- управление доступом по мандатному принципу контроля доступа;
- объединение пользователей в группы с общими файлами;
- индивидуальная и групповая настройка;
- контроль целостности программного обеспечения;
- сигнализация об изменении целостности эталонного состояния ПЭВМ;
- выборочное ознакомление с регистрационной информацией.

8.1.2. Аппаратно-программные системы идентификации и аутентификации

Важное место в области систем разграничения доступа занимают аппаратно-программные системы идентификации и аутентификации (СИА), или устройства ввода идентификационных признаков (термин соответствует ГОСТ Р 51241-98), предназначенные для обеспечения защиты от НСД к компьютерам. При использовании СИА доступ пользователя к компьютеру осуществляется только после успешного выполнения процедуры идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности пользователю предъявленного им идентификационного признака осуществляется в процессе аутентификации.

В состав СИА входят:

- аппаратные идентификаторы,
- устройства ввода-вывода (считыватели, контактные устройства, адаптеры, разъемы системной платы и др.)
- и соответствующее ПО.

Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме этого они могут хранить и обрабатывать конфиденциальные данные. Устройства ввода-вывода и ПО осуществляют обмен данными между идентификатором и защищаемым компьютером.

Сегодня на российском рынке компьютерной безопасности системы разграничения доступа обладают привлекательностью в силу их высокой эффективности и приемлемой цены.

Слабым звеном названных средств является уникальный элемент. Если нарушитель каким-либо образом получил этот самый элемент и предъявил системе защиты, то она воспринимает его, как «своего» и разрешает действовать в рамках того субъекта, секретным элементом которого несанкционированно воспользовались.

Для устранения данных недостатков были разработаны различные механизмы, из которых широкое распространение получили *системы построения защищенных виртуальных сетей (Virtual Private Network, VPN), обнаружения атак и анализа защищенности*.

Системы построения VPN позволяют организовать прозрачное для пользователей соединение локальных сетей, сохраняя секретность и целостность передаваемой информации с помощью шифрования. Более подробно вопросы защиты информации с использованием систем построения VPN изложены в разделе 8.3.

Обнаружение атак — это новая технология, которая получила распространение в последние годы. Ее отличительная особенность обнаружение любых атак, в том числе исходящих и от авторизованных пользователей и пропускаемых межсетевыми экранами и средствами разграничения доступа. На этом рынке лидирует компания ISS со своей системой обнаружения атак RealSecure. Можно сказать, что антивирусные средства тоже являются представителями систем обнаружения атак (аномального поведения).

Анализ защищенности заключается в поиске в вычислительной системе и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак. Именно наличие этих уязвимостей приводит к возможности несанкционированного проникновения в компьютерные сети и системы. Не было бы уязвимостей, не было бы и возможности реализовать атаки. Но программы пишут люди, которым свойственно ошибаться, а поэтому существует необходимость в средствах поиска и устранения таких ошибок. Наиболее известные продукты в области анализа защищенности, обнаруживающие уязвимости и ошибки в программном обеспечении, приведены в таблице 8.1.

8.2. Средства защиты операционных систем

Windows 2000 Security Benchmark

CIS Windows 2000 Security Benchmark является программой, позволяющей осуществлять проверку соответствия настроек ОС MS Windows 2000 минимальному набору требований безопасности, определяющих базовый уровень защищенности, который, в общем случае, является достаточным для коммерческих систем. Требования к базовому уровню защищенности ОС Windows 2000 были выработаны в результате обобщения практического опыта. Свой вклад в разработку этих спецификаций внесли такие организации, как SANS Institute, Center for Internet Security, US NSA и US DoD.

В состав инструментария CIS Windows 2000 Security Benchmark входит шаблон политики безопасности (cis.inf), позволяющий осуществлять сравнение текущих настроек ОС с эталонными и производить автоматическую переконфигурацию ОС для обеспечения соответствия базовому уровню защищенности, задаваемому данным шаблоном.

CIS Windows 2000 Security Benchmark позволяет осуществлять количественную оценку текущего уровня защищенности анализируемой ОС по 10-бальной шкале. Уровень 0 соответствует минимальному уровню защищенности (после установки ОС, ее уровень защищенности как раз и будет равен 0). Уровень 10 является максимальным и означает полное соответствие анализируемой системы требованиям базового уровня защищенности для коммерческих систем.

Все проверки, выполняемые при анализе системы, делятся на 3 категории:

1. Service Packs and Hotfixes (Пакеты обновлений и программные коррекции);

2. Account and Audit Policies (Политика управления пользовательскими бюджетами и политика аудита безопасности)

3. Security Options (Опции безопасности).

Первая категория включает проверку установки последних пакетов обновлений (Service Packs) и текущих программных коррекций (Hotfixes) от Microsoft.

Вторая категория включает проверки параметров политики безопасности по управлению пользовательскими бюджетами (включая политику управления паролями) и осуществлению аудита безопасности.

Третья категория включает проверки всех остальных параметров безопасности ОС, не относящиеся к первым двум категориям, включая запрет анонимных сессий (NULL sessions), правила выделения внешних устройств, параметры защиты протокола TCP/IP, установки прав доступа к системным объектам и т.п.

Для проверки наличия установленных текущих программных коррекций используется утилита MS Network Security Hotfix Checker (HFNetCheck), которая автоматически скачивается с сайта Microsoft и устанавливается во время осуществления проверок.

Подробную информацию об этой утилите можно получить по адресу:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp.

Используя список недостающих программных коррекций (Hotfixes), сгенерированный утилитой HFNetCheck, следует осуществить поиск и установку этих коррекций. Для этого используется Microsoft Security Bulletin Search Web-сайт:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Def ult.asp).

Для осуществления мониторинга установки необходимых программных коррекций, помимо утилит Microsoft, можно использовать более мощные средства третьих фирм, например программу UpdateExpert, разработки St. Bernard Software (www.stbernard.com). Для настройки ОС с использованием шаблона CIS.INF используется Security Configuration and Analysis Snap-In — стандартное средство ОС Windows 2000 для осуществления анализа и настройки параметров безопасности ОС.

Порядок подключения данного средства к MMC (Microsoft Management Console), загрузки шаблона, его использования для анализа и изменения конфигурации ОС описывается в «CIS Win2K Level 1 Implementation Guide», входящем в комплект программной документации, которая содержит также подробное описание всех производимых проверок и соответствующих параметров настройки ОС.

8.3. Встроенные средства защиты СУБД

Если рассматривать средства обеспечения безопасности в части доступа к БД, хранения информации и передачи по сети, то сегодня явный лидер рынка систем управления базами данных — СУБД Oracle. Она предоставляет разработчикам ПО и администраторам прикладных систем полный спектр средств и инструментов, необходимых для построения защищенных систем. Среди них стоит выделить следующие.

Virtual Private Database (VPD) — средства разграничения доступа к данным на уровне строк (в версии 10g — и на уровне колонок) и возможность организации работы пользователя только с виртуальной регламентированной частью данных, а не с реальной базой данных.

Oracle Advanced Security — комплекс средств аутентификации и обеспечения сетевой безопасности, включающий в себя поддержку защищенных протоколов передачи данных, в том числе SSL.

Oracle Label Security (OLS) — средства, аналогичные VPD, но с возможностью проверки уровня доступа пользователя.

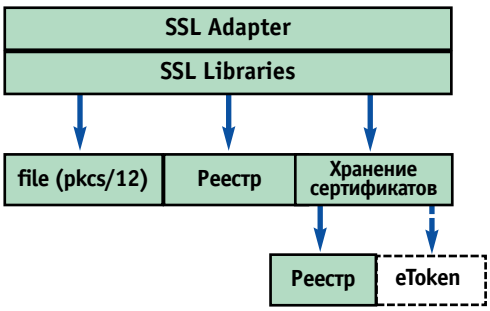
Fine Grained Audit Control (FGAC) — инструмент подробного аудита.

Штатные средства Oracle + eToken

Кардинально повысить безопасность работы приложений БД позволяет защита клиентского ПО СУБД Oracle 9i с помощью электронных ключей eToken. Существенно усилить защиту удалось благодаря применению нескольких технологических решений.

Прежде всего метод аутентификации пользователей по имени и паролю был заменен более надежной — двухфакторной аутентификацией с использованием цифровых сертификатов стандарта X.509. И хотя встроенные средства Oracle Advanced Security поддерживают аутентификацию по циф-

ровым сертификатам, вопрос о хранении сертификатов и личных ключей остается открытым. Предлагаемые Oracle способы хранения сертификатов в виде файлов-контейнеров формата PKCS#12 или реестра ОС Windows имеют ряд существенных недостатков. Суть встроенных в Advanced Security возможностей иллюстрирует схема хранения сертификатов.



Файл-контейнер, например, может быть похищен злоумышленником, имеющим права на чтение соответствующего ключа реестра или файла-контейнера. В то же время работа с СУБД разрешена только пользователю, для которого сформирован соответствующий контейнер и, более того, он «привязан» к определенной рабочей станции (где находится файл-контейнер). Чтобы избежать этих «неприятностей», необходимо хранить цифровые сертификаты непосредственно в памяти электронного ключа eToken, а для выполнения криптографических операций с закрытым ключом использовать встроенный в него криптопроцессор с дополнительной PIN-авторизацией пользователя.

Очевидно, что, помимо повышения надежности, аутентификация с использованием eToken дает ряд преимуществ по сравнению с традиционными (логин/пароль) методом. Прежде всего электронный ключ дает возможность пользователю различных приложений не хранить «где попало» и не запоминать необходимые имена и пароли. Зная один PIN-код и выбрав сертификат из предложенного списка, можно, имея соответствующие права и привилегии, обращаться к конкретной БД, причем с любой рабочей станции.

Администратор безопасности получает при этом дополнительные удобства в виде централизованного управления доступом и контроля работы системных администраторов. Все эти возможности управления обеспечивает единый инструмент — служба каталогов Oracle Internet Directory. Существующие получают в «лице» службы каталогов единую точку входа — своего рода портал архитектуры клиент-сервер. При этом в большинстве случаев изменений в прикладном ПО не требуется.

8.4. Межсетевые экраны

В глобальной сети Интернет остро стоят вопросы информационной безопасности. Одним из методов защиты сетевых информационных ресурсов организации, имеющей выход в Интернет, является использование специальных программных (программно-аппаратных) средств, называемых Fire Wall (огненная стена). В отечественной литературе их принято называть межсетевыми экранами (МЭ). Иногда встречается название «брандмауэр», но сейчас этот термин используется редко.

Индустрия МЭ постоянно развивается. Вслед за развитием новых способов нарушения информационной безопасности создавались и новые технологии защиты, предотвращающие такие нарушения.

Межсетевые экраны первого поколения — фильтры пакетов — появились в конце 1980-х годов. В 1985 г. компания Cisco представила законченное решение фильтрующего маршрутизатора. Однако первые публикации, описывающие процесс экранирования, появились только в 1988 г.

В 1989-1990 годах была разработана архитектура МЭ второго поколения, известная как МЭ уровня соединения.

Третье поколение межсетевых экранов прикладного уровня разрабатывалось в США в конце 1980 начале 1990-х годов. Публикации, описывающие МЭ прикладного уровня, впервые появились в 1990-1991 годах.

Компания Check Point Software реализовала в 1994 г. первый коммерческий продукт, основанный на технологии динамической фильтрации пакетов.

Следующим толчком в развитии технологии стало появление МЭ Fire Wall-1 компании Check Point. Впервые МЭ имел дружественный графический интерфейс пользователя, облегчающий процесс настройки и обслуживания.

Начиная примерно с середины 1990-х годов, рынок продуктов межсетевых экранов получил бурное развитие и на сегодняшний день насчитывает более ста реализаций различных производителей.

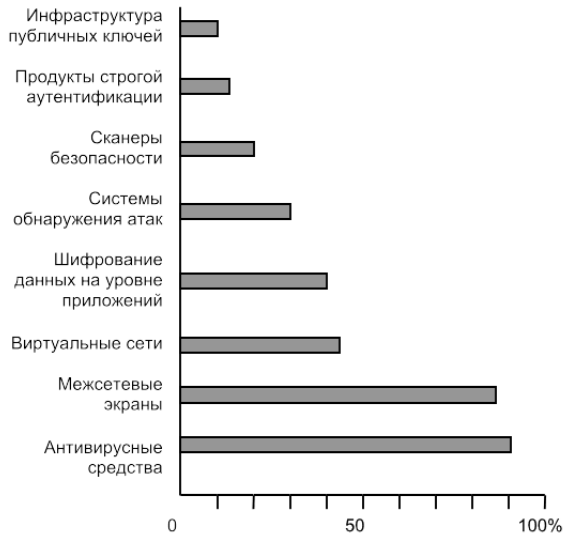


Рис. 8.1. Распределение средств защиты

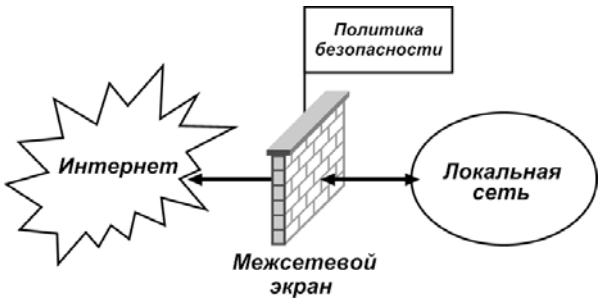


Рис. 8.2. Обобщенная схема межсетевогоэкранирования

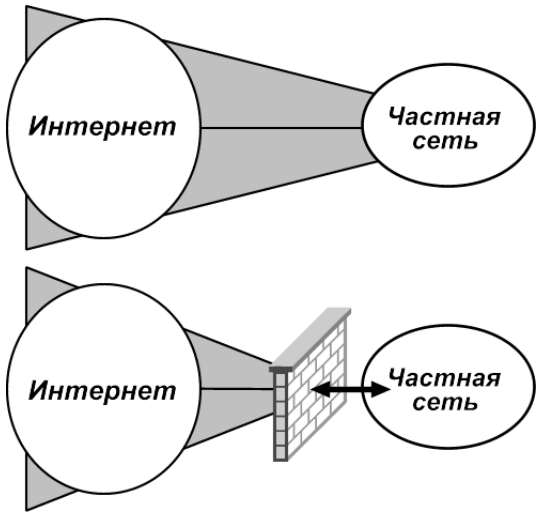


Рис. 8.3. Зоны риска незащищённой и защищённой частной сети

Сегодня ни одна организация, использующая Интернет, не обходится без использования МЭ или отдельных технологий межсетевого экранирования.

Современные коммерческие МЭ представляют собой сложные многофункциональные системы, использующие последние достижения в области информационных технологий и защиты информации. Сегодня МЭ представляют до 85 % всех используемых в локальных сетях средств защиты и по прогнозу некоторых аналитических компаний МЭ, поддерживающие технологию виртуальных частных сетей, длительное время будут составлять основу средств защиты информации при подключении организаций к сети Интернет (рис. 8.1).

Межсетевой экран представляет собой программный или программно-аппаратный комплекс, реализующий функции фильтрации сетевого трафика (информационных потоков) между двумя и более компьютерными сетями по некоторому набору правил, определяемых политикой безопасности защищаемой сети (рис. 8.2)

Программные МЭ ориентированы на конкретную платформу (Windows, Solaris Sun и другие). Программно-аппаратные МЭ выполняются в виде «черного ящика», конфигурируемого через интерфейсы удаленного управления на основе собственных приложений либо с использованием стандартных интерфейсов (Web, SSH и другие). Преимуществами последних, по сравнению с программными МЭ, являются:

- в случае неполадок ОС, нарушений информационной безопасности не будет;
- простота эксплуатации;
- более высокая производительность и надежность.

В большинстве случаев подключение локальных сетей к Интернету (и сетей между собой) осуществляется таким образом, что в точке соединения сетей существует возможность контроля всего сетевого трафика, проходящего между этими сетями. Исключение составляет случай, когда локальная сеть одновременно подключена к Интернету более чем одним соединением, например, для резервирования каналов связи или повышения пропускной способности.

МЭ позволяет значительно уменьшить, а в некоторых случаях и полностью исключить зону возможных рисков при подключении к потенциально опасным сетям, таким как Интернет (рис. 8.3). В идеальном случае МЭ должен блокировать все угрозы информационной безопасности, имеющие место в Интернете, на своем внешнем сетевом интерфейсе.

Другими словами, МЭ — это компонент сетевой инфраструктуры, устанавливающий барьер безопасности между сетями или сетевыми сегментами. МЭ представляет собой устройство, частично реализующее политику безопасности сети организации. Межсетевой экран разделяет физически и логически две и более, как правило, IP-сети на сети с различными политиками безопасности. В большинстве случаев МЭ разделяет две сети, одна из которых является сетью защищаемой организации, а другая — Интернет.

Под ***фильтрацией трафика*** понимается возможность его блокирования (запрещения), разрешения или изменения. Такие действия и выполняет МЭ, обеспечивая защиту («экранирование») сети.

Говоря о МЭ, прежде всего подразумевают, что они используются в сети Интернет, которая основывается на стеке протоколов TCP/IP. Сети на основе протокола IP являются сетями с коммутацией пакетов. В таких сетях пакеты выступают единицей передачи данных между участниками сетевого обмена. Межсетевые экраны реализуют механизмы контроля доступа путем фильтрации всего входящего и исходящего трафика, пропуская только авторизованные данные.

Фильтры пакетов работают, применяя набор правил, установленных в ядре TCP/IP стека МЭ. Этот набор правил содержит определенные действия, которые будут применены ко всем входящим и исходящим пакетам.

Действие над поступающим на сетевой интерфейс или исходящим из него пакетом имеет одно из двух значений: запретить (deny) или разрешить (allow). Запрещение прохождения пакета выполняется одним из следующих способов:

1) пакет отбрасывается без каких-либо дополнительных действий;

2) пакет отбрасывается и отправителю посылается пакет с установленным флагом «сброс соединения». Это правило используется только для TCP-пакетов;

3) пакет отбрасывается и отправителю посылается сообщение — хост недостижим или порт недоступен.

Последние два способа запрещения пакетов позволяют создать видимость отсутствия средств защиты (фильтрации) на пути прохождения сетевых пакетов.

В ядре МЭ создаются и обрабатываются два списка — запрещенный список и список доступа. Сетевой пакет, проходящий через МЭ, должен пройти оба списка доступа. В большинстве МЭ применяется правило: что явно не разрешено, то запрещено. Некоторые фильтры пакетов, включенные в состав маршрутизаторов, используют другую политику: пакет должен быть явно запрещен или иначе он будет разрешен. По этой причине необходимо ясно понимать политику фильтрации, используемой в активном оборудовании и МЭ. При задании правил фильтра пакетов используют и более сложные подходы, реализующие многоуровневую иерархическую структуру.

Классификация МЭ по типам защищаемых объектов приведена на рис. 8.4.

Рис. 8.4. Классификация МЭ по типу защищаемых объектов

Под ***сегментными*** понимают МЭ, установленные на границе двух и более сетей. Они предназначены для контроля сетевых потоков между двумя и более сетями, т. е. выполняют защиту сетей. Сегментные МЭ позволяют контролировать весь сетевой трафик между сетями, к которым подключен МЭ.

Контроль трафика осуществляется на всех уровнях модели OSI, начиная с сетевого. Сегментный МЭ можно представить как сетевой маршрутизатор, который не только осуществляет маршрутизацию пакетов между сетями, но и выполняет анализ пакетов и информационных потоков на соответствие

требованиям политики безопасности. Пакеты и информационные потоки, не удовлетворяющие этим требованиям, блокируются. Именно сегментные МЭ являются одним из основных средств обеспечения информационной безопасности.

Персональные МЭ защищают рабочие станции пользователей от внешних сетевых угроз и сетевых троянских программ. Персональные МЭ предназначены для защиты рабочих станций пользователей как отдельно подключенных к сети Интернет, так и функционирующих в составе локальных сетей. В последнем случае персональные МЭ создают дополнительный уровень защиты, в том числе и от внутренних угроз, и не исключают использования сетевых МЭ на границе локальной сети.

Среди ***персональных*** МЭ выделяют следующие разновидности экранов:

- пакетные фильтры,
- прокси-серверы,
- гибридные МЭ.

Пакетные фильтры отслеживают только сетевые пакеты на сетевом и транспортном уровне и не могут отслеживать соответствие пакетов и сетевых приложений. Пакетные фильтры требуют высокой квалификации пользователей.

Прокси-серверы отслеживают активность сетевых приложений. Такой подход не требует высокой квалификации пользователей и обеспечивает повышенный уровень защиты (по сравнению с пакетными фильтрами). Прокси-серверы могут иметь в своем составе прикладных посредников.

Гибридные персональные МЭ поддерживают функциональность и пакетных фильтров, и мониторов приложений, что позволяет реализовывать политику безопасности как на уровне сетевых приложений, так и на пакетном уровне.

Встраиваемые МЭ устанавливаются на прикладных серверах и предназначены для их защиты. Иногда возникает необходимость в усилении защиты прикладных служб, реализуемых одним или несколькими серверами. При этом использование сегментных МЭ может быть не оправдано по причине их высокой стоимости или условий эксплуатации (например, выделенный сервер на территории провайдера). В этом случае можно использовать встраиваемые МЭ, которые функционируют на одной платформе с защищаемыми серверами, обеспечивая их защиту. Низкая стоимость встраиваемых МЭ позволяет установить их на каждый защищаемый сервер.

Встраиваемые МЭ обеспечивают защиту по принципу персональных фильтрующих МЭ и предоставляют более широкие возможности управления (удаленное управление, резервное копирование, временные ограничения политики безопасности и др.) и анализа событий. Но в отличие от персональных, они не обеспечивают интерактивности взаимодействия с администратором прикладного сервера.

Все межсетевые экраны функционируют на основе информации, получаемой от различных уровней эталонной модели OSI, и чем выше уровень OSI, на основе которого построен межсетевой экран, тем выше уровень защиты, им обеспечиваемый. На рис.8.5 представлены уровни модели OSI (самый низкий — канальный, высокий — прикладной) и классификация сегментных МЭ.

Выделяют следующие типы ***сегментных МЭ***: управляемые коммутаторы, статические и динамические фильтры пакетов, инспекторы состояния, посредники сеансового уровня, посредники прикладного уровня и МЭ экспертного уровня.

Управляемые коммутаторы попадают под определение МЭ, но действуют они на самом нижнем уровне модели взаимодействия (канальном), что не позволяет управлять на уровне протокола IP. Тем не менее, появление коммутаторов 3-го уровня, стандартизация протоколов коммутации, расширение возможностей коммутаторов 2-го уровня позволяют использовать возможности коммутаторов в целях повышения безопасности локальных сетей и на более высоких уровнях — на сетевом и транспортном.

8.3.1. Схемы подключения сегментных МЭ

Для защиты АС применяются различные схемы подключения сегментных МЭ. Наибольшую известность из них получили следующие:

- на основе фильтрующего маршрутизатора;
- на основе двухпортового шлюза (Dual-homed);
- на основе демилитаризованной зоны;

- на основе экранирующего экрана (бастион-хост);
- на основе экранирующей подсети;

МЭ на основе ***фильтрующего маршрутизатора*** является самым распространенным и простым в реализации. Он состоит из фильтрующего маршрутизатора, расположенного между ЛВС и сетью Интернет. Он может осуществлять фильтрацию входящих и исходящих пакетов на основе анализа их адресов и портов.

МЭ на основе ***двухпортового шлюза*** (Dual-homed) означает, что МЭ имеет два сетевых адаптера подключенных к двум различным сетям. Это наиболее распространенная схема подключения МЭ. Со стороны внешней сети МЭ подключен к маршрутизатору (чаще всего провайдера). После МЭ располагают сетевой коммутатор или концентратор (см. рис.8.5). Внутренний маршрутизатор (на рис 8.6, 8.7, 8.8 маршрутизаторы обозначены как «М») используется в больших корпоративных сетях или для усиления ПБ.

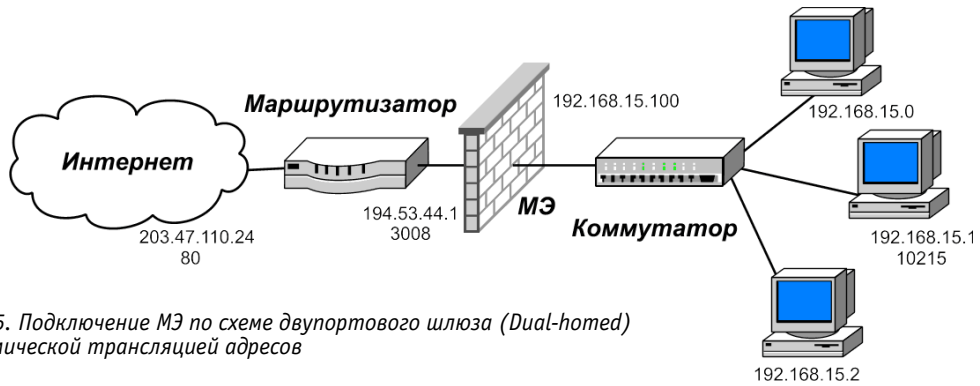


Рис. 8.5. Подключение МЭ по схеме двупортового шлюза (Dual-homed) с динамической трансляцией адресов

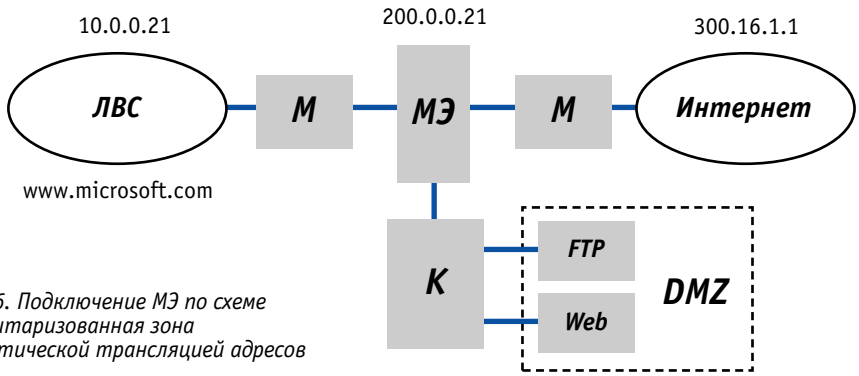


Рис.8.6. Подключение МЭ по схеме демилитаризованная зона со статической трансляцией адресов

МЭ на основе демилитаризованной зоны — это МЭ с несколькими сетевыми адаптерами, с возможностью установления различных ПБ между подключаемым к ним сетям, а также с образованием так называемой демилитаризованной зоны (DMZ-demilitarized zone). Как правило, в которой размещаются службы, которые должны быть доступны и клиентам сети Интернет и клиентам ЛВС. В демилитаризованной зоне определяются менее жесткие требования к сетевой безопасности, но достаточные для организации защиты от внешних угроз. МЭ на основе демилитаризованной зоны, имеющий три сетевых адаптера, изображен на рис. 8.6.

МЭ на основе экранирующего экрана (ранее в технической литературе его называли бастион-хост) — это МЭ подключенный только ко внутренней сети и имеющий один сетевой интерфейс (см. рис. 8.7). Маршрутизатор настраивается так, чтобы весь входящий трафик отправлялся на МЭ, а в ЛВС в качестве шлюза указывается адрес интерфейса МЭ. Данная схема подключения имеет меньшую защищенность, чем на основе МЭ с несколькими сетевыми интерфейсами поэтому используется редко.

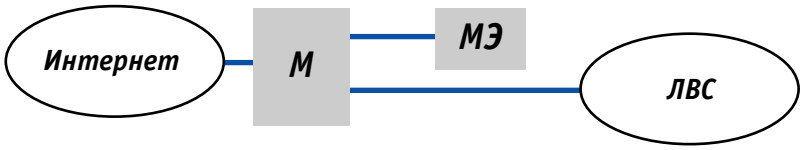


Рис. 8.7. Подключение МЭ по схеме экранирующий экран

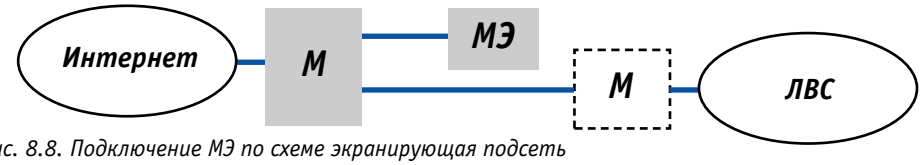


Рис. 8.8. Подключение МЭ по схеме экранирующая подсеть

МЭ на основе экранирующая подсеть по сравнению с предыдущей схемой подключения добавляет дополнительный уровень безопасности путем внесения дополнительного маршрутизатора для улучшения изоляции защищенной сети от Интернет (см. рис. 8.8). Два экранирующих маршрутизатора образуют внутреннюю фильтрующую подсеть, которая может выполнять функции демилитаризованной зоны.

Технология сетевой трансляции адресов (NAT — Network address translation) широко используется в большинстве МЭ. При использовании NAT МЭ выступает посредником между двумя IP-узлами, организуя два канала передачи данных. Он взаимодействует с внешним IP-узлом от имени внутреннего, но со своим IP-адресом, что позволяет скрыть внутреннюю структуру сети и иметь всего один зарегистрированный внешний IP-адрес. Сетевая трансляция адресов осуществляется в следующих режимах:

1. ***Динамическом*** (трансляция на уровне портов) — МЭ имеет один внешний IP адрес (см. рис. 8.5). МЭ при обращении к нему клиента выделяет ему уникальный порт транспортного протокола (TCP, UDP) для внешнего IP адреса. Выделяемый пул портов может составлять 65535 портов, но чаще всего 10000 — 20000 портов. В ряде ОС Unix динамический режим трансляции называют маскарадингом. В основном он предназначен для сетей, хосты которых выступают клиентами сети Интернет.
2. ***Статическом*** — внешнему интерфейсу МЭ назначается столько зарегистрированных IP адресов, сколько хостов имеется во внутренней сети (см. рис. 8.6). Каждому хосту внутренней сети ставится в соответствие уникальный внешний IP адрес МЭ. Он используется, если хосты внутренней сети являются серверами Интернет.
3. ***Комбинированном*** — может использовать сразу несколько режимов. Его применяют в сетях, где необходимо обеспечить работу и клиентов и серверов расположенных в защищенной сети. Далеко не все МЭ поддерживают комбинированный режим трансляции адресов.

На сегодняшний день рынок МЭ представлен более 50-ю компаниями-производителями. Наблюдается бурный рост и на рынке персональных экранов. Продукты даже одного производителя могут сильно отличаться от версии к версии или в зависимости от платформы, что также затрудняет выбор конкретного продукта. В таблице 8.2 приведены наиболее известные модели МЭ.

Отметим, что в последнее время на российском рынке появилось большое количество как сегментных, так и персональных МЭ отечественного производства. Некоторые выпускаются большими сериями, некоторые — в единичных экземплярах. И хотя почти все они уступают общеизвестным мировым лидерам в области МЭ по производительности, однако по остальным техническим параметрам вполне конкурентоспособны с аналогичными западными образцами, а по такому показателю как цена выглядят намного привлекательнее.

Высокая сложность МЭ и их большое разнообразие делают выбор МЭ для защиты АС не простой задачей. Сказать, что «этот» МЭ однозначно лучше остальных будет не правильно. Кроме того, компании производители постоянно совершенствуют свои продукты, улучшая их производительность, расширяя функциональность, повышая управляемость и т. п. Поэтому функциональность и свойства, присутствующие сегодня только в одном МЭ, завтра будут реализованы и в остальных.

Таблица 8.2. Модели МЭ

тип	производитель модель	адрес	уровень	класс	инспектор состояний	версия	Сертификат Гостехкомиссии
1	2	3	4	5	6	7	8
сегментный	*Check Point* FireWall-l	www.checkpoint.com	экспертный	Enterprise	да	4.1 SP2	да
встраиваемый	*Network-1* CyberwallPLUS	www.network-1.com	фильтр пакетов	SOHO	–	6.03	–
персональный	*ConSeal* PC Firewall (McAfee PF)	www.consealfirewall.com	гибридный	–	–	2.06	–
сегментный	*Axent* (*Symantec*) Raptor FireWall	www.axent.com	экспертный	Enterprise	да	6.5	–
сегментный	*Cisco* IOS Firewall	www.cisco.com	экспертный	SOHO/ Enterprise	да	12.1	–
сегментный	*Microsoft* Internet Connection Firewall	www.microsoft.com	фильтр пакетов	SOHO	да	1.0	–
сегментный	*ОАО «ЭЛВИС+»* «ЗАСТАВА»	www.elvis.ru	экспертный	Enterprise	да	2.5	да
сегментный	*ОАО «ИнфоТеКС»* VipNet Office Firewall	www.infotecs.ru	экспертный	SOHO/ Enterprise	да	–	да
персональный	*ОАО «ИнфоТеКС»* VipNet Personal Firewall	www.infotecs.ru	гибридный	SOHO	–	–	да
сегментный	*ООО «АМИКОН»* ФПСУ-Х.25	–	экспертный	SOHO	да	–	да
сегментный	*ЗАО «Сигнал-Ком»* Net-Pro	www.signal-com.ru	экспертный	SOHO	да	1.27	да

** Enterprise — промышленные системы, отвечающие самым жёстким требованиям безопасности и надежности*
** SOHO — средства для небольших офисов и домашнего использования*

Все современные МЭ достаточно хорошо справляются со своей основной задачей — защитой внутренней сети от различных угроз со стороны внешней сети и могут выполнять ряд дополнительных функций, таких как трансляция сетевых адресов, антивирусная защита и т.п.

В качестве инструмента МЭ обладает рядом характеристик, позволяющих в зависимости от конкретной ситуации предпочесть тот или иной МЭ. Наиболее важными характеристиками МЭ являются его стоимость, производительность, простота использования, расширяемость и функциональность. Основные технические характеристики МЭ приведены в таблице 7.1. Большое значение имеют также репутация производителя (как долго находится в эксплуатации, перспективы дальнейшего развития МЭ), поддерживаемая программно-аппаратная платформа, обеспечиваемый уровень защищенности согласно требований руководящих документов ФСТЭК России и др.

Еще одним немаловажным плюсом, при выборе МЭ, в направлении отечественных продуктов является то, что почти все они имеют действующие сертификаты ФСТЭК России (см. табл. 8.1). Причем, что немаловажно, отечественные МЭ, как правило, имеют сертификат на всю серию данных продук-

тов, а зарубежные только на отдельную партию из десятков единиц. Сертификат выдается сроком на три года и по истечении этого времени он может быть продлен. Информацию о выданных сертификатах на конкретные средства защиты информации от несанкционированного доступа можно получить на Интернет-сайте www.gtk.lissi.ru.

Приходим к следующим выводам:

1. Однозначного решения проблемы выбора МЭ не существует. В каждом конкретном случае выбор определяется экономическими и политическими соображениями (ПБ организации), требованиями заказчика и средой функционирования.

2. Для предприятий и организаций работающих с информацией, представляющей государственную тайну и для всех государственных учреждений нет иного пути, кроме изначальной ориентации на отечественных производителей МЭ, имеющих соответствующие лицензии и сертификаты Гостехкомиссии России. Причем в соответствии с СТР-К для защиты конфиденциальной информации, передаваемой по каналам связи между АС, если каналы связи выходят за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, включая защищенные волоконно-оптические линии связи или сертифицированные криптографические средства защиты.

3. Для негосударственных предприятий и организаций не работающих с государственной тайной документ СТР-К носит рекомендательный характер, и они могут использовать для защиты своих информационных ресурсов (составляющих коммерческую, банковскую тайну и т.д.) любые МЭ, в том числе и иностранного производства. Тут на первый план выходят такие параметры, как стоимость, функциональность, качество, производительность, криптостойкость, трудоемкость обслуживания, совместимость с уже имеющимся парком оборудования и.т.д.

8.5. Защита информации с помощью защищенных виртуальных сетей

Угроза информационной безопасности при использовании Интернет для организации бизнес — связей между филиалами компаний, бизнес-партнерами, мобильными пользователями сводит на нет удобство и низкую стоимость такого решения. На сегодняшний день практически ни одна крупная компания, использующая Интернет в своем бизнесе, не обходится без применения технологии ***VPN (Virtual Private Network)*** — защищенной виртуальной частной сети.

8.5.1. Общие принципы построения защищенных виртуальных сетей

В основе концепции построения защищенных виртуальных сетей VPN лежит следующая идея: если в глобальной сети есть два узла, которые хотят обменяться информацией, то для обеспечения конфиденциальности и целостности передаваемой по открытым сетям информации между ними необходимо построить виртуальный туннель, доступ к которому должен быть затруднен всем возможным активным и пассивным внешним наблюдателем.

Под термином «*защищенная виртуальная сеть*» чаще всего понимается организация защищенных информационных потоков между объектами виртуальной сети, организованных через сети общего пользования. При этом потоки данных частной и общей сетей не должны влиять друг на друга. Термин «виртуальная» указывает на то, что соединение между двумя узлами сети не является постоянным и существует только во время прохождения трафика по сети. Объектами виртуальной корпоративной сети могут выступать объединения локальных сетей и отдельных компьютеров.

Инфраструктура сети VPN «моделируется» на основе реальных каналов связи: выделенных линий — это проводная линия соединенная с провайдером Интернет, который обладает высокоскоростными магистральными каналами (оптоволоконными, спутниковыми, радиорелейными) объединенных в Интернет или коммутируемых линий — обычных телефонных каналов. При этом реальная открытая сеть может служить основой для целого множества VPN, конечное число которых определяется только пропускной способностью открытых каналов связи.

VPN позволяют организовать прозрачное для пользователей соединение локальных сетей, сохраняя секретность и целостность передаваемой информации с помощью шифрования. При этом при передаче по ИНТЕРНЕТ шифруются не только данные пользователя, но и сетевая информация — сетевые адреса, номера портов и т.д. Технология виртуальных частных сетей позволяет использовать се-

ти общего пользования для построения защищенных сетевых соединений.

Технология VPN выполняет две основные функции:

- шифрование данных, за счет чего обеспечивается безопасность сетевых соединений. При шифровании, как правило, используют стандартные общеизвестные протоколы RC4, CAST, DES, 3DES и др;
- туннелирование протоколов.

Под ***туннелированием*** понимают безопасную передачу данных через открытые сети. Между каждой парой «отправитель-получатель данных» устанавливается своеобразный туннель — безопасное логическое соединение, позволяющее упаковывать данные одного протокола в пакеты другого. Протоколы туннелирования чаще называют протоколами VPN (IPSec, PPTP, L2TP и др.).

Защищенные потоки (каналы) виртуальной частной сети могут быть созданы между VPN-шлюзами сети, VPN-шлюзами и VPN-клиентами, а также между VPN-клиентами (рис. 8.9). Создание виртуальных защищенных каналов достигается за счет шифрования трафика и туннелирования протоколов между объектами VPN-сети.

VPN-шлюз — сетевое устройство, установленное на границе сети, выполняющее функции образования защищенных VPN-каналов, аутентификации и авторизации клиентов VPN-сети. VPN-шлюз располагается аналогично МЭ таким образом, чтобы через него проходил весь сетевой трафик организации. В большинстве случаев VPN-сеть для пользователей внутренней сети остается прозрачной и не требует установки специального программного обеспечения.

VPN-клиент — программное обеспечение (иногда с аппаратным акселератором), устанавливаемое на компьютеры пользователей, осуществляющих подключение к сети VPN (через VPN-шлюзы). VPN-клиент выполняет функции передачи параметров аутентификации и шифрования/ дешифрования трафика.

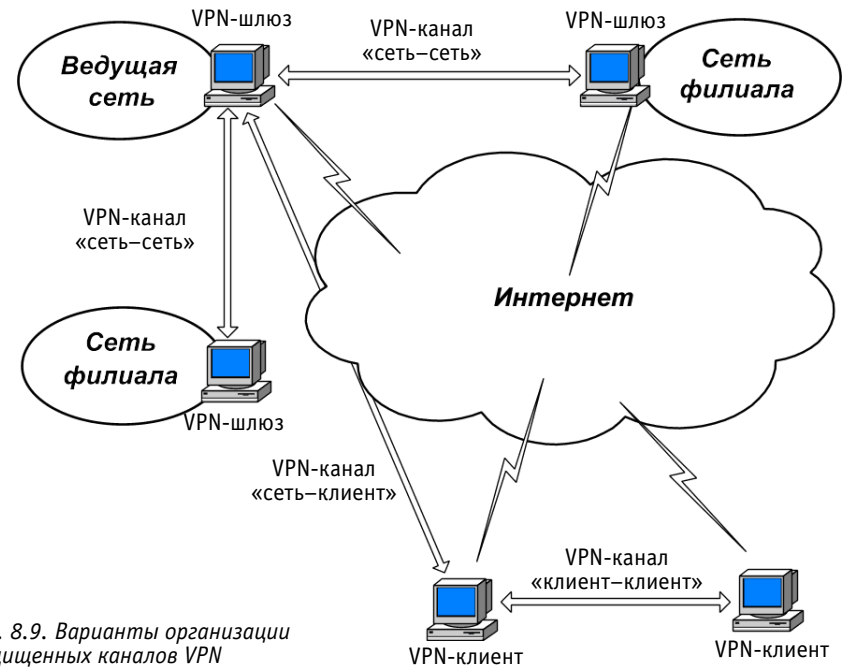
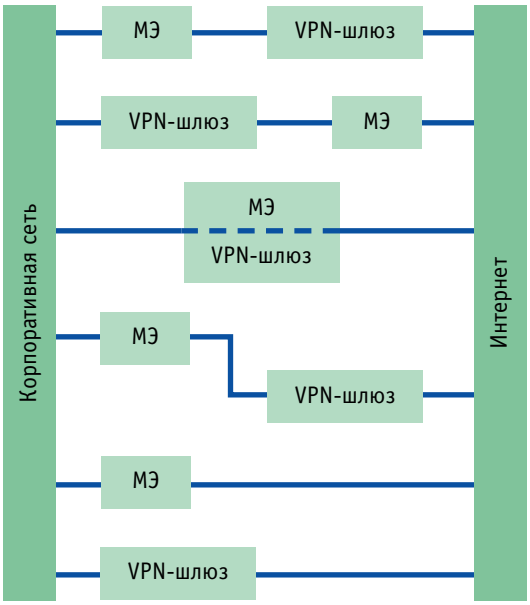


Рис. 8.9. Варианты организации защищенных каналов VPN

В большинстве случаев необходимо одновременно обеспечить функционирование двух каналов — Интернет и VPN. При этом можно использовать или различные физические линии связи или одну. Однако стоимость эксплуатации одного канала связи для доступа к сети Интернет и поддержки VPN обходится значительно ниже.



На рис.8.10. представлены возможные варианты взаимного расположения МЭ и VPN-шлюза при использовании одного физического канала. МЭ и VPN-шлюзы могут быть как независимыми продуктами, так и дополнять функции друг друга.

Преимущество использования МЭ, поддерживающего функции VPN-шлюза (см. рис. 8.10., в), заключается в возможности прозрачного управления политикой безопасности в едином интерфейсе управления как открытого, так и защищенного трафика Интернет. Такое решение значительно облегчает процесс управления МЭ и VPN-шлюзом, но предъявляет повышенные требования к производительности аппаратных средств.

Рис. 8.10. Варианты расположения VPN-шлюза и МЭ

8.5.2. Обзор средств построения защищенных виртуальных сетей

При выборе средств построения корпоративных VPN необходимо учитывать следующие важные факторы:

- технические характеристики открытой внешней среды передачи информации;
- преимущества и недостатки протоколов, используемых для построения VPN;
- варианты построения VPN;
- регулирование использования VPN-технологий со стороны российского законодательства;
- специфику (форма собственности, категорирование информации и т.д.) и финансовые возможности предприятия.

Открытую внешнюю среду передачи информации можно разделить на среду скоростной передачи данных, в качестве которой может использоваться сеть Интернет, а также более медленные общедоступные каналы связи, в качестве которых чаще всего применяются каналы телефонной сети. Наиболее эффективным способом объединения локальных сетей и удаленных компьютеров является объединение на основе глобальной сети Интернет. В случае отсутствия непосредственного подключения доступ к Интернет может осуществляться и через телефонную сеть.

Организация виртуальных защищенных сетей на основе Интернет обладает рядом преимуществ:

- гарантирует высокое качество информационного обмена, так как магистральные каналы и маршрутизаторы Интернет имеют большую пропускную способность, и характеризуются надежностью передачи ин формации;
- обеспечивает масштабируемую поддержку удаленного доступа к ресурсам локальной сети, позволяя мобильным пользователям связываться по местным телефонным линиям с поставщиками услуг Интернет и через них входить в свою корпоративную сеть в защищенном режиме;
- для организации удаленного доступа пользователей к локальной сети исключается необходимость в наличии модемных пулов, а трафиком дистанционного доступа можно управлять точно так же, как любым другим трафиком Интернет;
- сокращаются расходы на информационный обмен через открытую внешнюю среду:
- использование Интернет для объединения локальных сетей значительно дешевле аренды каналов связи телефонных и других глобальных сетей, например, сетей frame relay, не говоря уже о стоимости самостоятельного построения коммуникаций;
- при удаленном доступе вместо того, чтобы устанавливать дорого стоящие непосредственные со-

единения с локальной сетью по междугородной или международной телефонной связи, удаленные пользователи могут подключаться к Интернет и, далее, связываться с сетью своей организации через эту глобальную сеть.

Технически реализация защищенных виртуальных сетей стала возможной достаточно давно. Однако специализированные протоколы для создания защищенных виртуальных сетей разработаны сравнительно не давно (1992-94 годы) и сейчас продолжается работа над их совершенствованием и расширением. Большинство из них являются открытыми, т. е. свободными для распространения и реализации.

Для независимости от прикладных протоколов и приложений защищенные виртуальные сети формируются на одном из низших уровней модели OSI — канальном, сетевом или сеансовом. Канальному (второму) уровню соответствуют такие протоколы реализации VPN, как PPTP, L2F и L2TP, сетевому (третьему) уровню — IPSec, SKIP, а сеансовому (пятому) уровню — SSL/TLS и SOCKS. Чем ниже уровень эталонной модели, на котором реализуется защита, тем она прозрачнее для приложений и незаметнее для пользователей. Однако при снижении этого уровня уменьшается набор реализуемых услуг безопасности и становится сложнее организация управления VPN.

Чем выше защитный уровень в соответствии с моделью OSI, тем шире набор услуг безопасности, надежнее контроль доступа (он определяет порядок доступа объектов (пользователей и процессов) к различным информационным ресурсам на основе некоторых исходных данных (имя и пароль пользователя, IP-адрес клиента, время суток и др.) и проще конфигурирование системы защиты. Однако в этом случае усиливается зависимость от используемых протоколов обмена и приложений.

В VPN криптозащита может одновременно выполняться на нескольких уровнях эталонной модели. При этом увеличивается криптостойкость, но по причине снижения общей скорости криптографических преобразований уменьшается пропускная способность виртуальной сети. Поэтому на практике защищенные виртуальные сети формируются на одном уровне модели OSI (канальном, сетевом, транспортном или сеансовом).

Варианты построения VPN, а также достоинства и недостатки каждого из вариантов представлены в таблице 8.3., а примеры наиболее известных моделей систем построения VPN в таблице 8.3.

В настоящее время на российском рынке VPN-технологий имеется несколько реализаций решений по защите и фильтрации трафика отечественных производителей (см. табл. 8.3). Их функциональные возможности в некоторых случаях шире, чем у западных конкурентов, а крипкостойкость используемых криптоалгоритмов многократно превышает соответствующие параметры поставляемых в Россию западных аналогов.

Среди них наибольшую известность и распространенность приобрели:

1. Криптографический комплекс «Шифратор IP пакетов» производства МО ПНИЭИ (www.security.ru)
2. Комплект программных продуктов серии «ЗАСТАВА» от компании «ЭЛВИС+» (www.elvis.ru).
3. Криптографический комплекс «Континент-К» производства ЗАО «НИП Информзащита» (www.infosec.ru).

1. Криптографический комплекс «Шифратор IP пакетов» представляет собой отдельное программно-аппаратное устройство (криптошлюз), осуществляющее шифрование на основе протокола SKIP. Имеет сертификат ФАПСИ.

В состав криптографического комплекса «Шифратор IP пакетов» (ШИП) входят:

- программно-аппаратный комплекс ШИП, осуществляющий защиту данных в соответствии с ГОСТ 28147-89;
- центр управления ключевой структурой (ЦУКС), используемый для периодической смены ключей шифрования, аудита работы VPN и т.д.;
- устанавливаемый на рабочую станцию программный комплекс «Игла-П».

2. Комплект сертифицированных Гостехкомиссией РФ (№376 от 25.10.2003 г.) и ФАПСИ программных продуктов ЗАСТАВА версии 3.3, осуществляющих шифрование на основе протокола SKIP, включает в себя следующие программы:

- МЭ ЗАСТАВА (с возможностью организации VPN);

Таблица 8.3. Достоинства и недостатки средств создания VPN различных категорий

Варианты построения VPN	Достоинства	Недостатки
VPN на основе сетевых ОС	Низкая стоимость решения, данное решение является оптимальным для построения VPN внутри локальной сети	Уязвимость протокола шифрования в одноранговых сетях (MPPE) и протокола аутентификации (CHAP), открытость для атак на этапе конфигурации соединения и атак типа «отказ в обслуживании», недостаточная проработанность вопросов обеспечения безопасности в данной ОС.
VPN на основе маршрутизаторов	Функции поддержки сетей VPN могут быть встроены в маршрутизирующие устройства, что не потребует дополнительных расходов на приобретение средств, реализующих эти функции. Упрощается администрирование VPN.	Функционирование VPN может отрицательно повлиять на выполнение функций маршрутизации. Канал между получателем информации внутри локальной сети и маршрутизатором может стать уязвимым звеном в системе защиты. Необходимо использование идентичного каналообразующего оборудования всеми участниками VPN канала
VPN на основе МЭ	Возможен контроль туннелируемого трафика. Достигается высокая эффективность администрирования защищенных виртуальных сетей. Обеспечивается комплексная защита информационного обмена. Отсутствует избыточность аппаратных платформ для средств сетевой защиты.	Операции, связанные с шифрованием данных, могут чрезмерно загружать процессор и снижать производительность МЭ Если защищенный туннель завершается на МЭ, то канал между получателем информации внутри локальной сети и МЭ может стать уязвимым звеном в системе защиты. При повышении производительности серверных продуктов аппаратное обеспечение потребуется модернизировать. Необходимо согласование использования МЭ всеми сторонами защищенного взаимодействия.
VPN на основе специализированного программного обеспечения	Высокая масштабируемость, гибкость и переносимость решения. Не требуются специальные аппаратные средства. Низкая стоимость решения.	Администрирование VPN может потребовать отдельного приложения, возможно, даже выделенного каталога. При повышении производительности серверных продуктов аппаратное обеспечение может потребоваться модернизировать.
VPN на основе специализированных аппаратно-программных средств	Обеспечивается более высокая производительность. Многофункциональные аппаратные устройства облегчают конфигурацию и обслуживание. Однофункциональные аппаратные устройства допускают тонкую настройку для достижения наивысшей производительности.	В многофункциональных блоках производительность одного приложения повышается зачастую в ущерб другому. Однофункциональные устройства могут требовать отдельных инструментов администрирования и каталогов. Модернизация для повышения производительности нередко оказывается слишком дорогостоящей или невозможной. Канал между получателем информации внутри локальной сети и аппаратным устройством шифрования трафика может стать уязвимым звеном в системе защиты Высокая стоимость решения

- ЗАСТАВА-персональный клиент;
- ЗАСТАВА-корпоративный клиент;
- центр управления ЗАСТАВА;
- ЗАСТАВА-сервер;
- ЗАСТАВА-офис;
- персональный центр сертификации ЗАСТАВА;
- корпоративный центр сертификации ЗАСТАВА;
- сервер сертификатов ЗАСТАВА.

3. Аппаратно-программный комплекс «Континент-К» предназначен для работы в сетях, использующих для передачи данных протоколы семейства TCP/IP. Он включает в свой состав следующие компоненты:

- центр управления сетью криптографических шлюзов;
- криптографический шлюз;
- программу управления сетью криптографических шлюзов.

Комплекс «Континент-К» имеет сертификат Гостехкомиссии России №352 от 28.08.2003 г.

Из российских VPN-продуктов криптографический комплекс ШИП можно рекомендовать к использованию в случаях, когда имеющиеся партнеры по производству/бизнесу уже работают с этим продуктом и если компания имеет надежные каналы связи для поддержки работоспособности ключевой системы.

Сертифицированные Гостехкомиссией России VPN-продукты ЗАСТАВА целесообразно использовать в ситуации, когда компании необходимо одновременно обеспечить наличие как защищенных, так и открытых соединений в Интернет с удаленными подразделениями/сотрудниками. Кроме того, ЗАСТАВА представляет собой оптимальное решение также и в тех случаях, когда компания предпочитает иметь масштабируемое решение по созданию собственной ключевой инфраструктуры для работы с изменяющимся количеством абонентов.

Оптимальным решением с точки зрения обеспечения информационной безопасности является построение VPN на базе МЭ. Хорошие кандидаты на эту роль — CheckPoint FW-1/VPN.-1 в случае, если необходима богатая функциональность продукта, а также Cisco PIX Firewall, если требуются большая производительность и меньшая стоимость решения. Из отечественных МЭ можно рекомендовать продукт ФПСУ-IP компании «Амикон», DataGuard компании «Сигнал-Ком», а также комплекс МЭ ЗАСТАВА с модулем построения VPN.

При правильном выборе VPN корпорация получает следующие преимущества:

- защищенные каналы связи и защищенный трафик отдельных приложений по цене доступа в Интернет;
- при установке VPN не требуется изменять топологию сетей, переписывать приложения, обучать пользователей;
- обеспечивается масштабирование сети.

Рынок VPN-продуктов, в том числе и отечественных, постоянно растет и, видимо, будет расширяться впредь, поскольку интерес к этой технологии в последнее время только усиливается. Вместе с тем информационная безопасность корпоративных сетей и применение криптографии для защиты информации при передаче по открытым каналам связи являются достаточно «тонкими» областями знаний, поэтому даже малейшая ошибка при проектировании корпоративной VPN может привести к фатальным результатам. По этой причине необходимо быть особенно осмотрительным и даже скрупулезным как при выборе VPN-продуктов, так и при проектировании самой VPN.

Заметим, что перспективным протоколом построения защищенных виртуальных сетей является протокол IPSec. Соответственно желательно, чтобы выбираемые средства создания VPN поддерживали данный протокол. Однако при этом необходимо учитывать, что стандарт IPSec характеризуется недостаточной зрелостью и пока еще не гарантирует совместимости решений разных производителей. Разработчики, поддерживающие IPSec, только приступили к выявлению и устранению проблем несовместимости. Поэтому при выборе соответствующего средства целесообразно запросить у его поставщика отчет о поддерживаемых совместимых продуктах, особенно если в объединяемых локальных сетях используются средства создания VPN разных производителей.

Нестандартные схемы туннелирования и алгоритмы шифрования хороши только в том случае, если нет необходимости взаимодействовать с другими системами. Однако с учетом роста масштабности компьютерных сетей вопросы взаимодействия и совместимости становятся приоритетными для любой организации.

8.6. Проблемы защиты информации при взаимодействии с сетью Интернет

Сетевая атака — любое действие, выполняемое нарушителем путем использования уязвимостей информационной системы для реализации угрозы.

Уязвимость информационной системы — любая характеристика или элемент информационной системы, использование которых нарушителем может привести к реализации угрозы.

Прежде всего, атакующий должен выполнять ряд действий по сбору информации об атакуемой системе. На основе полученной информации строится дальнейший план действий. На рис. 8.11 представлена обобщенная схема действий сетевого злоумышленника, описывающая порядок его действий в большинстве случаев.

Причем на этапе сбора информации злоумышленник не выполняет каких-либо разрушительных или противоправных действий. Первичные данные об интересующей системе могут быть получены из следующих открытых источников:

- в системе DNS — организационная структура предприятия, соответствие IP-адресов и доменных имен, почтовые серверы. Как правило, внутренняя структура доменных имен локальной сети отображает организационную структуру предприятия;
- на сайтах организаций — электронные адреса, комментарии кода web-страниц могут содержать отладочную информацию (пароли доступа к БД, имена разработчиков и др.);
- из других источников (например — из реестров БД).

Определив объект атаки и используя активные методы сбора информации, злоумышленник попытается выяснить — находится ли на его пути МЭ. Объектом воздействия может выступать и МЭ. Злоумышленник может идентифицировать МЭ, т. е. определить его название, производителя и версию. А дальше он может приступать к планированию и непосредственному воздействию на «понравившейся» узел сети.

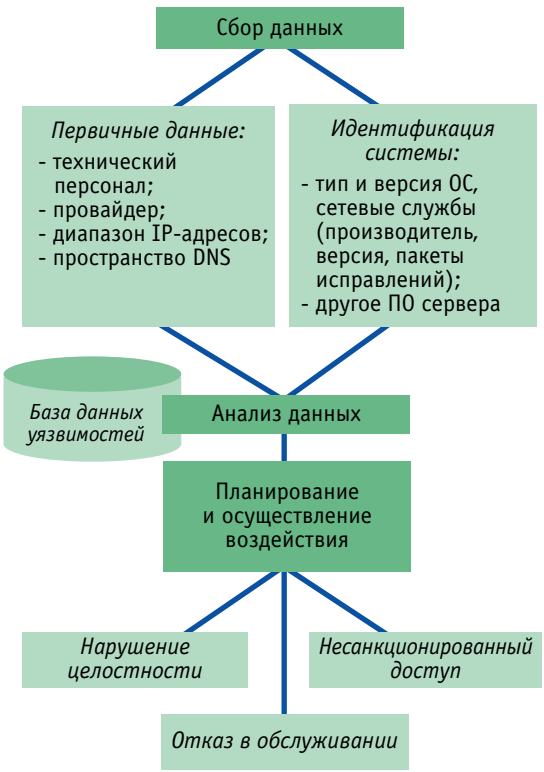


Рис. 8.11. Обобщенная схема действий злоумышленника

Наиболее распространенными сетевыми атаками являются ***атаки типа «отказ в обслуживании»*** («denial of service»), это такое воздействие на ресурсы (сетевые и локальные), которое приводит к снижению производительности или блокировке доступа к ресурсу. Выделяют две основные причины возможности DoS-атак — захват ресурсов (оперативная память, дисковое пространство, полоса пропускания канала связи) и ошибки разработки программного обеспечения. Причем, если для реализации атак, направленных на захват ресурсов, требуется выполнение большого количества операций, то для атак, основанных на ошибках программного обеспечения, часто достаточно отправки единственного сетевого пакета или некорректно сформированной команды прикладного протокола.

Особую опасность представляют атаки типа «распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS). Распределенная атака строится следующим образом. Злоумышленник управляет небольшим числом т.н. «мастеров» (master), каждый из которых в свою очередь управляет большим числом «демонов» (daemon). Именно эти демоны и используются для непосредственной атаки на выбранную жертву. В распределенной атаке могут использоваться от нескольких сотен до нескольких тысяч демонов.

Злоумышленник использует десятки и сотни незащищенных узлов для координации нападения. Эти узлы могут принадлежать различным провайдерам и находиться в различных странах и даже на различных материках, что существенно затрудняет обнаружение злоумышленника, координирующего атаку.

Каждый узел, участвующей в скоординированной атаке, не позволяет получить информацию о том, кто и откуда инициировал нападение. Кроме того, на этих узлах нет полного списка, участвующих в атаке, узлов. Поэтому выявление одного узла не приводит к превращению всей атаки.

Вторыми по распространенности являются атаки на отсутствующие, «слабые» или заданные по умолчанию пароли. Тройку лидеров замыкают атаки на Web-сервера, использующие программное обеспечение компании Microsoft.

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят отсутствие механизмов безопасности, их неправильное использование, либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Основными уязвимостями информационной системы являются:

1) использование недостатков в политике безопасности,
2) ошибки администрирования,
3) поиск ошибок в программных реализациях.

Политика безопасности (ПБ) — это взгляд руководства организации на проблему информационной безопасности. В нее входят правила и инструкции для всего персонала организации, призванные защитить ее информационные ресурсы. Политику безопасности разрабатывают документально и она должна описывать:

- какие данные представляют ценность и как они должны быть защищены;
- какие информационные ресурсы доступны различным категориям пользователей и каков порядок доступа к ним;
- что понимается под нарушением информационной безопасности;
- права и обязанности всех сотрудников в области ИБ;
- ответственные должностные лица;
- инструкции пользователям и должностным лицам на случай обнаружения нарушений ИБ.

С точки зрения безопасности к самой информации, как объекту защиты, могут быть выдвинуты три важных требования:

- конфиденциальность (никто, кроме легальных пользователей, не может получить доступ к данным);
- целостность (никто, кроме легальных пользователей, не может выполнять операции изменения данных);
- доступность (данные всегда должны быть доступны легальным пользователям).

Каждая организация должна четко понимать, насколько для нее опасны те или иные формы утечки или потери информации. В ПБ входят правила и инструкции для всего персонала организации, призванные защитить ее информационные ресурсы, как от внешних, так и от внутренних угроз. Большинство всех случаев реализаций угроз сетевой безопасности происходит во внутренней сети или по причинам, вызванным персоналом компании.

Атаки, направленные из внутренней сети на внутренние корпоративные ресурсы, не видны для МЭ, поскольку сетевые пакеты, реализующие эти атаки, не проходят через него. В этом случае МЭ, установленный на границе сети, не может обеспечить защиты.

Ошибки администрирования. Установка МЭ, его первичная настройка, установка пакетов исправлений и дополнений МЭ и ОС и, конечно, редактирование ПБ — неотъемлемые этапы жизненного цикла МЭ. И на любом из этих этапов некорректные действия администратора МЭ могут создать условия нарушения информационной безопасности.

Основные ошибки администрирования:

1. Установка ОС и софта по умолчанию. Наверное, не стоит лишний раз говорить, что настройки, заданные производителем, надо менять и как можно скорее. Это относится и к Windows, и к Unix, и даже к сетевому оборудованию. Например, один из распространенных взломов роутеров Cisco — вход на него по дефолтовому, админскому паролю.

2. Слабые или отсутствующие пароли. Тем более что существуют средства, автоматизирующие подбор паролей. Часто «почтовый» пароль пользователя совпадает с «системным» (например в ОС Unix), многие пользователи для «удобства» используют один и тот же пароль для получения почты и входа в различные системы предприятия (Unix-узлы, сеть Windows).

3. Отсутствие резервного копирования, что может привести к тому, что после атаки системы восстанавливать ее содержимое будет не с чего.

4. Слишком большое количество открытых на компьютере портов, что облегчает злоумышленнику проникновение на него. Следуйте правилу — «все, что не разрешено, — запрещено».

5. Отсутствие фильтрации исходящих и входящих адресов (редактирование ПБ), которая могла бы быть включена на персональном или сегментном МЭ. Не стоит облегчать жизнь злоумышленнику, допуская в сеть или на компьютер пакеты с такими Internet-адресами, как 192.168.x.x, 10.x.x.x, 172.16.x.x и т.п. Эти пакеты никогда не могут встретиться в Интернете, поэтому их необходимо смело блокировать.

6. Отсутствие или неполная регистрация событий. Если ничего не фиксировать, то и обнаруживать следы хакерской деятельности очень затруднительно.

7. Своевременная установка пакетов исправлений и дополнений МЭ и ОС

На любом из этих этапов некорректные действия администратора могут создать условия нарушения информационной безопасности.

Ошибки при определении правил доступа могут образовать дыру, через которую может быть взломана система. Поэтому в большинстве МЭ реализованы служебные утилиты, облегчающие ввод, удаление, просмотр набора правил. Наличие этих утилит позволяет также производить проверки на синтаксические или логические ошибки при вводе или редактирования правил. Как правило, эти утилиты позволяют просматривать информацию, сгруппированную по каким либо критериям — например, все, что относится к конкретному пользователю или службе.

Компетентности администратора должно уделяться особое внимание. Все усилия и немалые денежные затраты на обеспечение безопасности могут быть перечеркнуты одним неверным действием. Редактирование политики безопасности — одна из самых важных операций. Администратор должен четко представлять, что реализует каждое правило политики безопасности. Ценой совершенной ошибки будет потерянная информация — самое ценное в этом тысячелетии, как уверяют социологи.

Поиск ошибок в программных реализациях. Ошибки разработчиков общего программного обеспечения (ПО) и средств защиты, сетевых администраторов — основные причины известных нарушений информационной безопасности компьютерных систем. Это непреднамеренные ошибки ПО и ошибки администрирования систем. Но существуют и преднамеренные действия, как разработчиков, так и злоумышленников, специально разрабатывающих программные закладки, троянские программы и оставляющих «потайные ходы» в своих программах.

К сожалению, МЭ, как и другим продуктам, присущи ошибки, заложенные на различных этапах разработки. Успешно реализованная атака типа «отказ в обслуживании», основанная на ошибках программного обеспечения, может привести к отказу в обслуживании всех ресурсов защищаемой сети, в том числе и ее пользователей.

Сообщения о проникновении в корпоративные сети и атаках на Web-сервера в последнее время появляются с большой частотой. Число и сложность предлагаемых на рынке информационных технологий периодически растет. Не редко злоумышленники преодолевают установленные в компании или банке защитные средства (системы аутентификации, межсетевые экраны и т.д.), установленные для разграничения доступа к ресурсам корпоративной сети. С увеличением квалификации злоумышленники становятся более изощренными в разработке и применении методов проникновения за защитную преграду.

Обнаружить таких злоумышленников очень трудно. Они маскируются под авторизованных пользователей, используют промежуточные узлы для сокрытия своего истинного адреса, осуществляют атаки, распределенные во времени (в течение нескольких часов) и пространстве (одновременно с нескольких узлов) и т.д. Многие атаки осуществляются за очень короткое время (минуты и даже секунды), что также не позволяет обнаружить и предотвратить их стандартными защитными средствами. Связано это с тем, что большинство компьютерных защитных систем построено на классических моделях разграничения доступа, разработанных в 70-х, 80-х годах. Согласно этим моделям субъекту (пользователю или программе) на основе заданных правил разрешается или запрещается доступ к какому-либо объекту (например, файлу). Однако действия, производимые субъектом над объектом, никак не регламентируется и таким образом невозможно, например, предотвратить копирование файла пользователем, которому доступ к данному файлу разрешен.

Существуют несколько различных средств защиты информации по противодействию сетевым атакам (см. таб. 8.1). Рассмотрим преимущества использования МЭ.

Функциональные возможности современных МЭ позволяют в ряде случаев возложить на них до 100 % всех требований политики безопасности организации. Основными преимуществами использования МЭ для противодействия сетевым атакам являются следующие:

1. Управляемый доступ к сетевым ресурсам.
2. Защита сетевых ресурсов от внешних угроз.
3. Обнаружение и защита от типовых атак отказа в обслуживании.
4. Скрытие структуры локальной сети.
5. Конфиденциальность внешних сетевых соединений.
6. Аудит событий безопасности.
7. Управление сетевым трафиком.

1. МЭ реализует политику безопасности организации, которая, в частности, исходя из решаемых ею задач, определяет службы и порядок доступа к ним всех категорий пользователей. Основным преимуществом использования МЭ является его способность обеспечения управляемого доступа пользователей к информационным ресурсам.

Под *управляемым доступом* понимается метод защиты, основанный на регулировании использования всех ресурсов системы.

Реализация управляемого доступа к сетевым ресурсам позволяет:

- значительно повысить уровень информационной безопасности путем ограничения числа разрешенных служб;
- повысить уровень защиты разрешенных служб за счет разграничения доступа на уровне пользователей и групп пользователей;
- ограничить доступ к ресурсам сомнительного содержания;
- пресекать использование рабочего времени не по назначению.

2. Внешние факторы являются основным источником угроз информационной безопасности и основная задача МЭ — *это обеспечение надежной защиты именно от внешних угроз*. МЭ позволяет значительно усилить защищенность потенциально уязвимых сетевых элементов, непосредственное использование которых может привести к нарушению информационной безопасности. Существует немало полезных и удобных прикладных служб, использование которых в ряде случаев запрещается политикой безопасности по причине их потенциальной уязвимости. Примером такой службы может быть интерфейс NetBIOS. Удаленные пользователи операционных систем (ОС) MS Windows с легкостью бы использовали встроенные возможности этой ОС при подключении к корпоративным файловым ресурсам.

МЭ позволяет решить проблемы использования уязвимых служб и усилить защищенность используемых прикладных служб путем установления специальных посредников между клиентами и сервером службы. Контроль МЭ содержимого сетевых соединений позволяет обнаруживать и блокировать на входе в защищаемую сеть деструктивный код (вирусы, троянские программы, Java, ActiveX).

3. МЭ обеспечивают *защиту от большинства типовых атак типа отказа в обслуживании*, а также позволяют обнаруживать и многие другие типы атак, частично выполняя функции систем обнаружения атак (в некоторых реализациях МЭ).

4. Большинству сетевых вторжений злоумышленников в корпоративные сети предшествуют подготовительные действия, целью которых является изучение физической и логической структур сети, а также поиска в ней уязвимых мест.

Использование МЭ позволяет практически полностью решить эту проблему. В большинстве случаев *корпоративная сеть может быть представлена с внешней стороны всего одним IP-адресом*, даже если она состоит из сотен компьютеров!

5. Непосредственное использование сети Интернет для передачи конфиденциальных данных между подразделениями организации, мобильными пользователями и в ряде других случаев не обеспечивает безопасности соединений. Кроме того, очень немногие приложения используют защищенные соединения, а большинство известных реализаций таких распространенных протоколов, как TELNET, FTP, POP3, передают данные и пароли в открытом виде. Некоторые МЭ обеспечивают конфиденциальность внешних соединений посредством *использования технологии виртуальных частных сетей*.

6. Аудит событий безопасности является одним из методов обеспечения информационной безопасности. Аудит событий — основывается на анализе сообщений генерируемых различными средствами и подсистемами безопасности. МЭ состоит из нескольких взаимосвязанных функциональных модулей, каждый из которых генерирует собственные сообщения событий безопасности. Непрерывное накопление и анализ этих событий позволяют:

- выявлять попытки нарушения информационной безопасности;
- обнаруживать источники угроз и нарушителей информационной безопасности;
- усиливать защищенность сети за счет обнаружения слабых и уязвимых мест.

По результатам анализа данных аудита могут быть приняты дополнительные меры защиты. Кроме того, совокупный анализ событий, полученных от различных систем, позволяет «видеть» комплексную картину состояния безопасности информационной системы в целом.

7. МЭ в некотором приближении можно рассматривать как сетевой маршрутизатор с расширенными функциями. Подобно сетевым маршрутизаторам, *МЭ управляют прохождением трафика между сетями*, что позволяет:

- накапливать и предоставлять различную учетную информацию (время работы пользователей, распределение объема трафика между пользователями и службами, статистика ошибок и др.);
- распределять нагрузку между прикладными службами (балансировка нагрузки).

Доля участия МЭ в реализации политики безопасности (ПБ) зависит в первую очередь от требований политики безопасности, а также от его функциональных возможностей. По этой причине администраторам безопасности очень важно знать потенциальные возможности МЭ и используемых в них технологий защиты.

К сожалению, МЭ не может защитить информационные ресурсы сети от ***атак, направленных из внутренней сети*** и от ***несанкционированного использования модемов*** подключенных к рабочим станциям.

Атаки, направленные из внутренней сети не видны для МЭ, поскольку сетевые пакеты, реализующие эти атаки, не проходят через него. В этом случае МЭ, установленный на границе сети, не может обеспечить защиты.

Политика безопасности организации должна предусматривать и защиту от внутренних угроз, что достигается как административными мерами, так и техническими (физическая защита доступа к носителям, разграничение доступа к внутренним прикладным службам и др.).

Иногда целесообразно установить МЭ во внутренней сети организации между сетевыми сегментами, в которых циркулируют данные с разными уровнями доступа (конфиденциальности) или необходимо обеспечить защиту критически важных служб.

Несанкционированное использование модемов, подключенных к рабочим станциям пользователей, является одной из самых опасных и трудно обнаруживаемых угроз безопасности. Действитель-

но, все усилия по обеспечению надежной защиты сети могут быть сведены на нет при непосредственном подключении рабочего места к Интернет через модемное (коммутируемое) соединение. Причем подключение не обязательно может использоваться для доступа в Интернет. Возможны соединения и к серверам других организаций, и к отдельным компьютерам, например домашним.

Часто модемы входят в состав рабочих мест пользователей. Пользователям достаточно лишь настроить сетевое соединение. Причины наличия модемов:

- модемы встроены в портативные компьютеры или поставлялись вместе с компьютерами;
- модемы предназначены для обеспечения факсимильной связью рабочих мест пользователей.

И в первом, и во втором случае проблема может быть решена только организационным путем — модемы должны быть изъяты из системных блоков, а факсимильная связь должна быть организована, например, через сетевой факс-сервер.

Развитие современных систем и средств связи (мобильная связь, беспроводные устройства доступа, персональные цифровые помощники и органайзеры) только усугубляет проблему несанкционированных сетевых подключений.

Так как в системе защиты самым слабым элементом является человек, то именно ему нужно оказывать максимальное внимание. Можно построить систему защиты АС за миллион долларов, но если сторож ее отключит и проведет злоумышленника, то возникает вопрос о целесообразности такой защиты.

Германский промышленник А. Крупп еще в 50-е годы прошлого века писал, что «нужно было бы иметь второго сторожа, который контролировал первого, и третьего, который бы наблюдал бы за вторым «. Как отмечает А.И. Доронин, автор книги «Основы экономической разведки» (Тула. Гриф и К, 2000 г. стр.23), на своих предприятиях «Крупп организовал строго охраняемые секретные отделы, а у прусского правительства просил разрешения на приведение всего персонала к присяге на сохранение производственной тайны».

Основатель компании SONY А. Морита замечает по этому поводу: «когда нет преданности, которая приходит с долговременной занятостью, я не вижу возможности положить когда-либо конец утечке информации и воровству, от которых повседневно страдает американский бизнес, вследствие предательства и нечестности». (А. В. Ковров, «Предатели: « Пятая колонна» в организации «, М. 1999г. АР-СИН, стр. 16).

Таким образом, самым уязвимым местом информационной безопасности АС являются пользователи защищаемой сети.

8.7. Антивирусная защита

Под ***компьютерным вирусом*** будем понимать компьютерную программу, разработанную с целью нанесения ущерба пользователям вычислительной системы. Основной особенностью большинства компьютерных вирусов является способность к скрытому саморазмножению. Саморазмножение, или репродуцирование вируса, выполняется путем включения в исполняемые или хранящиеся программы своей, возможно модифицированной копии, сохраняющей способность к дальнейшему саморазмножению.

В последние несколько лет наибольшим источником компьютерных вирусов является именно глобальная сеть Интернет. Из нее к пользователям попадают минимум 95% всех вредоносных программ.

В узком смысле вирусами являются программы, которые имеют возможность создавать свои копии, которые в свою очередь сохраняют способность к размножению (размножение — главное свойство вируса). В широком же смысле слова мы называем вирусами как собственно сами вирусы, так и: Интернет — черви, сетевые черви, троянские программы, утилиты скрытого администрирования.

Сами вирусы в узком смысле этого слова ранее были наиболее массовым типом вредоносных программ. Наиболее распространенные из них нынче: Win95.CIH, Win32.Funlove, Win32.Elkern. Но сейчас они потеряли былую «популярность». Связано это, прежде всего с тем, что переносятся такие вирусы с компьютера на компьютер через исполняемые файлы. Нынче же пользователи все реже и реже переписывают друг у друга программы. Чаще меняются компакт дисками или ссылками все в той же глобальной сети. Хотя естественно полностью этот класс вредоносных программ не вымер.

Самым распространенным типом вирусов в последние два года являются ***Интернет черви***. Именно они представляют главную угрозу для всех пользователей глобальной сети. Червем называют ви-

рус, обладающий способностью распространения в вычислительной сети на основе маскировки под системные средства поиска ее свободных ресурсов.

Почти все Интернет черви — это почтовые черви, и лишь малая доля — это не почтовые черви, применяющие уязвимости программного обеспечения (как правило, серверного). Примеры не почтовых Internet-червей: IIS-Worm.CodeRed, IIS-Worm.CodeBlue, Worm.SQL.Helkern.

Почтовые черви можно делить на подклассы по-разному, но для конечного пользователя они делятся на два основных класса:

- Черви, которые запускаются сами (без ведома пользователя);
- Черви, которые активизируются, только если пользователь сохранит присоединенный к письму файл и запустит его.

К *первому* типу относятся черви, которые используют уязвимости (ошибки) почтовых клиентов. Чаще всего такие ошибки находятся в почтовом клиенте Outlook, а вернее даже не в нем, а в Интернет браузере Internet Explorer. Дело в том, что MS Outlook создает письмо в виде HTML страницы и при отображении этих страниц он использует функции браузера Internet Explorer.

Наиболее распространенная уязвимость, применяемая червями, ошибка IFRAME. Применяя соответствующий код, вирус имеет возможность при просмотре письма автоматически сохранить присоединенный к письму файл на диск и запустить его. Самое обидное то, что данная уязвимость обнаружена более двух лет назад. Тогда же компанией Microsoft выпущены заплатки для всех версий браузера Internet Explorer, исправляющие эту ошибку. И, тем не менее, черви, применяющие данную уязвимость, по-прежнему являются наиболее распространенными (I-Worm.Klez, I-Worm.Avron, I-Worm.Frethem, I-Worm.Aliz).

Почтовые черви *второго* типа рассчитаны на то, что пользователь, по каким то соображениям сам запустит программу, присоединенную к письму. Для того чтобы подтолкнуть пользователя к запуску инфицированного файла авторами червей применяются различные психологические ходы. Самый распространенный прием — выдать зараженный файл, за какой то важный документ, картинку или полезную программку (I-Worm.LovGate создает ответы на письма, содержащиеся в почтовой базе; I-Worm.Ganda маскируется под информацию о боевых действиях в Ираке). Практически всегда червями применяются «двойные расширения». В этом случае присоединенный файл имеет имя вроде: «Doc1.doc.pif», «pict.jpg.com». Данный принцип рассчитан на то, что почтовые клиенты не отображают полное имя файла (если оно слишком длинное), и пользователь не увидит второго расширения, которое и является «реальным». То есть пользователь думает, что файл является документом или картинкой, а тот на самом деле является исполняемым файлом с расширением вроде: EXE, COM, PIF, SCR, BAT, CMD и т.п. Если такой файл «открыть», то тело червя активизируется.

Кроме основной функции, размножения, черви почти всегда несут в себе и боевую нагрузку. Действительно, зачем писать червя и выпускать его «в свет», предварительно не заложив бомбу. Вложенные функции чрезвычайно разнообразны. Так, например, очень часто почтовые черви призваны для того, чтобы установить на зараженный компьютер троянскую программу или утилиту скрытого администрирования и сообщить адрес компьютера творцу червя. Не редко просто уничтожают информацию или просто делают невозможной дальнейшую работу на компьютере. Так червь I-Worm.Magistr выполнял те же действия, что и печально-известный WinCIH — стирал содержимое FLASH BIOS и затирал мусорными данными информацию на жестком диске.

В любом случае, независимо от наличия или отсутствия вредоносных функций и их «опасности» почтовые черви вредны уже только потому, что они существуют. Это связано с тем, что при размножении они загружают каналы связи и нередко настолько, что полностью парализуют работу человека или целой организации.

Вторыми по распространенности в диком виде являются ***макро-вирусы***. Данные вирусы являются макросами, хранящимися во внешних файлах программного обеспечения (документах Microsoft Office, Autocad, CorelDRAW и пр.) и при открытии документа исполняются внутренними интерпретаторами данных программ. Широкое распространение они получили благодаря огромным возможностям интерпретатора языка Visual Basic, интегрированного в Microsoft Office.

Излюбленным местом обитания этих вирусов являются офисы с большим документооборотом. В таких организациях людям, работающим за компьютерами (секретари, бухгалтеры, операторы ЭВМ) некогда заниматься такими мелочами как компьютерные вирусы. Документы лихо переносятся с компьютера на компьютер, без какого либо контроля (особенно при наличии локальной сети).

К сожалению, людям свойственно не воспринимать всерьез макровирусы, а напрасно. На самом деле макрос, написанный на языке VBA и интегрированный в документ того же Word или Excel, обладает всеми теми же возможностями, что и обычное приложение. Он может отформатировать Ваш винчестер или просто удалить информацию, украсть какие то файлы или пароли и отправить их по электронной почте. Фактически вирусы этого класса способны парализовать работу целого офиса, а то даже и не одного.

Опасность макровирусов заключается еще и в том, что распространяется вирус целиком в исходном тексте. Если человек, к которому попал вирус, более-менее умеет писать на Visual Basic, то он без труда сможет модифицировать вирус, вложить в него свои функции и сделать его невидимым для антивирусов. Не забывайте, что авторы вирусов пользуются теми же антивирусными программами и модифицируют свои вирусы до тех пор, пока те не перестают детектироваться антивирусами. Фактически, таким образом, рождаются новые модификации уже известных вирусов, но для того, чтобы данный вирус обнаруживался антивирусом, он сначала должен попасть в антивирусную лабораторию и только после этого будут добавлены функции детектирования и обезвреживания новой модификации.

Следующими по распространенности являются ***троянские программы и утилиты скрытого администрирования*** (backdoor).

Отличие этих двух типов программ заключается в том, что троянская программа выполняет активные действия (уничтожение данных, сбор данных и отправка через Internet, выполнение каких либо действий в определенное время), в то время как утилиты скрытого администрирования открывают удаленный доступ к компьютеру и ожидают команды злоумышленника. Для простоты будем называть оба этих класса троянскими программами.

Под троянской программой понимается программа, имеющая законный доступ к компьютерной системе, но выполняющая вместе с основные и скрытые (необъявленные) функции, реализуемые посредством ее вирусоподобного компонента.

Главное отличие «троянов» от всех перечисленных выше творений человеческого разума является то, что троянские программы не размножаются сами. Они единоразово устанавливаются на компьютер и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы по какой либо причине) выполняет свои функции. При этом троянский конь не может самостоятельно переместиться с одного компьютера в локальной сети на другой.

Так почему же Трояны так распространены. Причина таится именно в том, что они максимально «полезны» и незаметны. Часто они являются спутниками сетевых или почтовых червей. Так, почтовый червь I-Worm.LovGate при попадании на компьютер устанавливает в систему (backdoor) модуль, открывающий доступ к компьютеру по TCP/IP и отправляет разработчику червя письмо, в котором указывается имя пользователя, имя компьютера и сетевой адрес зараженного компьютера.

Все троянские программы можно разделить на три основных класса по выполняемым действиям:

1. Логические (временные) бомбы — программы, различными методами удаляющие/модифицирующие информацию в определенное время, либо по какому то условию.
2. Шпионы — собирающие информацию (имена, пароли, нажатия на клавиши) и складирующие ее определенным образом, а не редко и отправляющие собранные данные по электронной почте или другим методом.
3. Собственно BackDoor программы — удаленное управление компьютером или получение команд от злоумышленника (через локальную/глобальную сеть, по электронной почте, в файлах, от других приложений, например тех же червей или вирусов).

Одинаково опасны все три типа программ. Каждый из них способен либо уничтожить данные, либо украсть ценную информацию (хотя бы те же имена и пароли доступа к различным ресурсам).

Противодействие компьютерным вирусам:

1. Необходимо регулярно обновлять базы антивирусного продукта. И если вы активно пользуетесь Интернетом, рекомендуется обновлять антивирус минимум раз в неделю (хотя конечно идеально было бы обновляться каждый день).
2. Весь почтовый трафик между АС и Интернетом должен проходить через один почтовый сервер.
3. Никогда не настраивать свою почтовую программу на автоматическое открытие приложений.
4. Если Ваша почтовая программа не проверяет вложения на наличие вирусов автоматически, то при получении письма с вложением его следует извлекать в отдельный файл на диске и проверять антивирусной программой.

Идеальный подход должен обеспечивать решение следующих задач:

- Обнаружение. Если заражение произошло, оно должно быть немедленно обнаружено с установлением места обитания вируса.
- Идентификация. Обнаружив заражение вирусом, необходимо идентифицировать его тип.
- Удаление. Как только вирус будет идентифицирован, следует удалить все следы вируса из инфицированных программ и восстановить программы в их исходном виде. Важно удалить вирус из всех инфицированных систем, чтобы болезнь не распространялась дальше.

Если вирус обнаружен, но его не удается идентифицировать или удалить из системы, альтернативой является удаление инфицированной программы с последующей ее новой загрузкой с резервной копии.

Технологии разработки вирусов и антивирусов идут рука об руку. Первые вирусы представляли собой сравнительно простые фрагменты кода и могли быть удалены с помощью относительно простых антивирусных программ. По мере усложнения вирусов антивирусное программное обеспечение тоже становилось все сложнее и изощреннее.

Антивирусные программы разделяются на четыре поколения.

- Первое поколение: обычные сканеры.
- Второе поколение: эвристические анализаторы.
- Третье поколение: мониторы.
- Четвертое поколение: полнофункциональные системы защиты.

Антивирусные ***программы-сканеры*** *первого поколения* для идентификации вирусов использовали характерные для соответствующих вирусов сигнатуры. Вирусы могли содержать «групповые символы», но все копии вируса имели в основном одну и ту же структуру и неизменный код. Такие программы-сканеры (Aids Test), использующие сигнатуры, могут обнаруживать только известные вирусы. Существуют транзитные (загружаемые в оперативную память только для поиска и обезвреживания вирусов) и резидентные, которые после запуска остаются в оперативной памяти резидентно и проверяют программные файлы при возникновении с ними определенных событий (запуск, копирование, переименование, создание) программы-сканеры.

Сканеры второго поколения — ***эвристические анализаторы*** уже не ориентированы на конкретные сигнатуры. Вместо этого в них начали применять эвристический анализ, с помощью которого можно сделать вывод о вероятном наличии вируса в программе. Одна из разновидностей таких сканеров предполагала поиск в программе фрагментов кода, характерного для вирусов. Например, сканер мог искать начало цикла шифрования, используемого полиморфным вирусом, и пытаться открыть ключ шифрования. Получив ключ, сканер мог расшифровать тело вируса, идентифицировать вирус, удалить его из программы и вернуть программу в рабочее состояние.

Другим подходом, применявшимся в антивирусных программах второго поколения, была проверка целостности. С каждой программой можно связать контрольную сумму. Если вирус инфицирует программу, не меняя при этом контрольной суммы, то проверка целостности обязательно это обнаружит. Чтобы противостоять вирусам, которые при заражении меняют соответствующую контрольную сумму, можно использовать некоторую шифрованную функцию хэширования. Ключ шифра хранится отдельно от программы, чтобы вирус не мог сгенерировать новый хэш-код и зашифровать его. Использование функции хэширования с шифрованием вместо обычной контрольной суммы не дает ви-

русу возможности модифицировать программу так, чтобы результат хэширования после инфицирования не изменился (Примеры: Aidinf, DWeb).

Программы *третьего поколения* — ***мониторы***, представляют собой резидентные программы, выявляющие вирусы по выполняемым ими действиям, а не по их коду в инфицированной программе. Преимущество таких программ заключается в том, что для них не требуется постоянно обновлять базу данных сигнатур и эвристик для все большего числа новых вирусов. Вместо этого достаточно определить относительно небольшой набор действий, характеризующих возможные проявления вируса (Примеры: AVP лаборатория Касперского, Spider DWeb).

Продукты *четвертого поколения* — ***полнофункциональные системы защиты*** представляют собой пакеты, объединяющие в единое целое все существующие антивирусные технологии. Такой подход, помимо выполнения сканирования и наличия компонентов, позволяющих регистрировать определенные действия вирусов, предполагает наличие средств управления доступом. Эти средства позволяют ограничить возможности вирусов по проникновению в систему и внесению изменений в файлы под видом обновления (Примеры: AVP Antihaker, AVP for Fire Wall (лаборатория Касперского), Norton AntiVirus for Fire Wall (Symantec), DWeb).

Вирусная «гонка вооружений» продолжается. С появлением пакетов четвертого поколения появилась возможность построить всеобъемлющую стратегию антивирусной защиты, являющейся органической частью общей безопасности компьютерных систем.

В настоящее время имеют сертификат ФСТЭК следующие антивирусные средства:

1. Программный комплекс средств защиты информации «Антивирусный пакет Doctor Web» компании ЗАО «Диалог Наука» версии 4.х №591 действителен до 4.03.2008 г.
2. Комплект антивирусных программных средств Norton AntiVirus Solution Suite компании SYMANTEC версии 3.03 №255 действителен до 23.07.2005 г., срок действия сертификата продлен.
3. Программый комплекс средств защиты информации «Антивирус Касперского (AVP)» версии 3.5 № 456 действителен до 8.05.2007 г.

Защита ресурсов корпоративной сети от компьютерных вирусов достигается за счет внедрения и поддержания в работоспособном состоянии комплексной системы антивирусной защиты, предназначенной для решения следующих задач:

1. Перекрытия всех возможных каналов распространения вирусов, к числу которых относятся: электронная почта, разрешенные для взаимодействия с сетью Интернет сетевые протоколы (HTTP и FTP), съемные носители информации (дискеты, CD-ROM и т.п.), разделяемые папки на файловых серверах.

2. Непрерывный антивирусный мониторинг и периодическое антивирусное сканирование всех серверов и рабочих станций, подключаемых к корпоративной сети.

3. Автоматическое реагирование на заражение компьютерными вирусами и на вирусные эпидемии, включающее в себя: оповещения, лечение вирусов, удаление троянских программ и очистку системы, подвергнувшейся заражению.

Система комплексной антивирусной защиты корпоративной сети строится из следующих компонентов:

1. Средства управления, включающие в себя управляющую консоль, серверные компоненты системы антивирусной защиты, средства протоколирования и генерации отчетов;
2. Средства антивирусной защиты серверов ЛВС;
3. Средства антивирусной защиты рабочих станций;
4. Средства антивирусной защиты почтовой системы (внутренних почтовых серверов и внешних шлюзов);
5. Антивирусный шлюз, работающий совместно с МЭ, который осуществляет антивирусный контроль HTTP и FTP трафика.

Наиболее надежная защита от компьютерных вирусов может быть обеспечена только в том случае, если проверка на их наличие производится во всех точках доступа в сеть предприятия. Поскольку МЭ с точки зрения прохождения сетевого трафика обеспечивает единую точку входа (выхода)

в сеть, то целесообразно возложить на него также и функции антивирусной защиты.

Межсетевой экран, поддерживающий протокол перенаправления содержания CVP, выступает как клиент сервера CVP. На сервере CVP осуществляется обработка информационных потоков (в данном случае — обнаружение вирусов), поступающих от клиента.

При обнаружении вируса антивирусный сервер производит его удаление либо осуществляет другие необходимые действия. Результат обработки возвращается обратно МЭ.

Например, организации необходимо обеспечить проверку всех вложений электронной почты на наличие компьютерных вирусов. Это легко обеспечить, проводя проверку почты проходящей через шлюз с FireWall-1. В этом случае FireWall-1 перехватит все потоки данных, отвечающие соответствующим правилам политики безопасности и, используя протокол перенаправления содержания (CVP), перенаправит их на сервер антивирусной проверки. Прежде, чем вернуть полученные данные, сервер антивирусной проверки выполнит необходимые действия по сканированию вложений почты на наличие в них вирусов и лечению зараженных данных. Получив данные обратно, FireWall-1 отправляет их получателю. Таким образом, ни одно соединение не будет организованно напрямую без соответствующей проверки.

Антивирусный сервер для повышения производительности может быть расположен как на отдельно выделенном компьютере, так и на компьютере с МЭ. Благодаря такому подходу, администратор информационной безопасности предприятия может легко реализовать оптимальную схему борьбы с компьютерными вирусами, быстро развернуть ее и администрировать весь комплекс из общего центра управления.

Вместо настройки двух совершенно независимых программных продуктов, администратор безопасности определяет правила разграничения доступа и правила проверки информационных потоков в общей политике безопасности, посредством ее редактора (FireWall-1 Security Policy Editor).

По умолчанию для сервера CVP выделяется транспортный порт TCP 18181. Протокол CVP поддерживают такие хорошо зарекомендовавшие себя антивирусные программы, как AVP for Fire Wall (лаборатория Касперского), Norton AntiVirus for Fire Wall (Symantec).

Известны и другие решения реализации антивирусной защиты. Так, например, в МЭ BlackHole 4.11 компании Milky Way.

Некоторые производители МЭ ранее включали в состав своих продуктов антивирусные средства. Однако из-за сложности поддержки антивирусных баз самими производителями МЭ такие решения быстро «умирали». Следует обратить внимание на совместимость МЭ и CVP-сервера. К сожалению, протокол CVP на сегодняшний день не стандартизирован и его реализации сильно отличаются у различных производителей.

Список сокращений

АС — автоматизированная система
БД — база данных
ЗИ — защита информации
ИБ — информационная безопасность
ИО — информационное обеспечение
МЭ — межсетевой экран
НСД — несанкционированный доступ
ПБ — политика безопасности
ПО — программное обеспечение
РД — руководящий документ
СВТ — средства вычислительной техники
СЗИ — средство защиты информации
СРД — система разграничения доступа
ФСТЭК — Федеральная служба по техническому и экспортному контролю

Литература

1. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. - Спб.:НТЦ им. Л.Т. Тучкова, 2005. - 149 с.
2. Гавриш В.Ф — Практическое пособие по защите коммерческой тайны — Симферополь: Таврида, 1994
3. Гайкович В. — Безопасность электронных банковских систем — М.: Единая Европа, 1994
4. Герасименко В.А — Защита информации в автоматизированных системах обработки данных — М.: Энергоатомиздат, 1994
5. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. - М.: МГТУ им. Н.Э. Баумана, 2002. -304 с.
6. Лысов А.В. — Промышленный шпионаж в России: методы и средства — С-Пб.: Бум Техно, 1994
7. Магауенов Р.Г — Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации — М.: Мир безопасности, 1997
8. Общесистемные вопросы защиты информации. Коллективная монография/ под ред. Е.М. Сухорева. Кн. 1 - М.: Радиотехника, 2003. - 296 с.
9. Петраков А.В., Лагутин В.С — Утечка и защита информации в телефонных каналах — М.: Энергоатомиздат, 1996

Руководящие документы Гостехкомиссии

1. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения - М.: Гостехкомиссия России, 1992
2. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации - М.: Гостехкомиссия России, 1997
3. Руководящий документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) - М.: Гостехкомиссия России, 2001