ДАЛЬНЕВОСТОЧНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТИХООКЕАНСКИЙ ИНСТИТУТ
ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ И ТЕХНОЛОГИЙ

Корнюшин П.Н.
Костерин С. С.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ВЛАДИВОСТОК
2003 г.

ОГЛАВЛЕНИЕ

Методические указания для студентов

1. Консультации можно получить по адресу: г. Владивосток, ул. Суханова,8, ДВГУ, ауд. 57 или по электронной почте: **korn@ifit.phys.dvgu.ru**.
2. Форма аттестации по курсу – компьютерное тестирование в соответствии с прилагаемыми тестами.
3. Нормы аттестации: сдача **каждого** из 4-х тестирований, соответствующих 4-м модулям, не менее чем на «удовлетворительно».

Аннотация

Учебное пособие содержит основные положения информационной безопасности: концепцию, направления обеспечения информационной безопасности; выявление технических каналов утечки информации и их защита; компьютерная безопасность.

Пособие предназначено для студентов специальностей вузов, изучающих основы информационной безопасности.

Модуль 1. Концепция и основные направления обеспечения информационной безопасности

1.0. Введение

Одним из признаков нынешнего периода является переход от индустриального общества к информационному, в котором *информация* становится более важным ресурсом, чем материальные или энергетические ресурсы. *Ресурсами* принято называть элементы экономического потенциала, которыми располагает общество, и которые при необходимости могут быть использованы для достижения конкретных целей хозяйственной деятельности. Давно стали привычными и общеупотребительными такие категории, как материальные, финансовые, трудовые, природные ресурсы, которые вовлекаются в хозяйственный оборот, и их назначение понятно каждому. Появившееся понятие "информационные ресурсы", хотя и узаконено, но осознано пока еще явно недостаточно. В одном из основополагающих законов в области информационной безопасности, законе "Об информации, информатизации и защите информации", приведено: "*Информационные ресурсы* - отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)". Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учету и защите, т.к. информацию можно использовать не только для производства товаров и услуг, но и превратить ее в наличность, продав кому-нибудь, или, что еще хуже, уничтожить.

Собственная информация для производителя представляет значительную ценность, т.к. нередко получение (создание) такой информации - весьма трудоемкий и дорогостоящий процесс. Очевидно, что ценность информации (реальная или потенциальная) определяется в первую очередь приносимыми доходами. Особое место отводится информационным ресурсам в условиях рыночной экономики, важнейшим фактором которой выступает конкуренция. Побеждает тот, кто лучше, качественнее, дешевле и оперативнее производит и продает. В сущности, это универсальное правило ранка. И в этих условиях основным выступает правило: кто владеет информацией, тот владеет миром.

В конкурентной борьбе широко распространены разнообразные действия, направленные на получение (добывание, приобретение) конфиденциальной информации самыми различными способами, вплоть до прямого промышленного шпионажа с использованием современных технических средств разведки. Установлено, что 47 % охраняемых сведений добывается с помощью технических средств промышленного шпионажа. Достаточно привести в качестве примера случаи шантажа английских фирм преступной международной группой. За 1993 - 1996 годы преступники получили 400 млн. фунтов стерлингов. Жертвам приходилось выплачивать до 13 млн. фунтов стерлингов единовременно после демонстрации шантажистами своих возможностей остановить все сделки или получить доступ к новейшим разработкам фирм. Деньги переводились в банки, расположенные в оффшорных зонах, откуда преступники снимали их в считанные минуты.

Примерами острого информационного межгосударственного противоборства могут служить информационные войны. Элементы такой войны уже имели место в локальных военных конфликтах на Ближнем Востоке и на Балканах. Так, войскам НАТО удалось вывести из строя систему противовоздушной обороны Ирака с помощью информационного оружия. Эксперты предполагают, что войска альянса использовали программную закладку, внедренную заблаговременно в принтеры, которые были закуплены Ираком у французской фирмы и использовались в АСУ ПВО.

В этих условиях защите информации от неправомерного овладения ею отводится весьма значительное место. При этом "*целями защиты информации* являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности

документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при их разработке, производстве и применении информационных систем, технологии и средств их обеспечения".

Как следует из этого определения целей защиты, информационная безопасность - довольно емкая и многогранная проблема, охватывающая не только определение необходимости защиты информации, но и то, как ее защищать, от чего защищать, когда защищать, чем защищать и какой должна быть эта защита.

В первой главе излагается концепция информационной безопасности. Приводятся основные концептуальные положения и модель информационной безопасности. Вторая глава посвящена анализу направлений обеспечения информационной безопасности. Введены понятия правовой, организационной и инженерно-технической защиты. В третьей главе более глубоко рассматриваются правовые основы информационной безопасности. Определяются основополагающие позиции формирования государственной политики в области информационной безопасности, а также излагаются основные принципы реализации этой политики органами контроля, лицензирования и сертификации. Четвертая глава содержит описание характеристик технических каналов утечки информации по различным физическим каналам. В пятой главе приведены методы выявления технических каналов утечки информации. Шестая глава дает основные сведения о методах и средствах защиты информации от утечки по различным техническим каналам. Седьмая глава посвящена анализу методов защиты компьютерной информации от несанкционированного доступа.

1.1. Концепция информационной безопасности

"*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ* - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств" (Закон РФ "Об участии в международном информационном обмене").

Что же такое информация? Понятие "информация" сегодня употребляется весьма широко и разносторонне. Вот некоторые ее признаки (характеристики, свойства).

1. Информация - это всеобщее свойство материи.
2. Любое взаимодействие в природе и обществе основано на информации.
3. Всякий процесс совершения работы есть процесс информационного взаимодействия.
4. Информация - продукт отражения действительности.
5. Действительность отражается в пространстве и времени.
6. Ничего не происходит из ничего.
7. Информация сохраняет свое значение в неизменном виде до тех пор, пока остается в неизменном виде носитель информации - ПАМЯТЬ.
8. Ничто не исчезает просто так.

На основе перечисленного можно дать следующее определений информации: “Информация (от латинского informatio - разъяснение, изложение) - с середины XX века общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке, от организма к организму; одно из основных понятий кибернетики”.

Существенные особенности информации:

- двойственность характера информации (материальное и нематериальное составляющие информации);
- распространение только копий с информации;
- информация имеет размерность;
- информация имеет стоимость и цену.

Таким образом, можно отметить, что *информация* - это субстанция, объединяющая в себе элементы идеального и материального, имеющая измеряемые определенными единицами физические параметры, стоимость и цену, обладающая специфическими свойствами дуализма и легкости копирования, которой можно владеть, ее использовать и ею распоряжаться.

Известно и такое определение информации: "*информация* - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления" (Закон РФ "Об информации, информатизации и защите информации").

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя - сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности - такие как персонал, материальные и финансовые средства и информацию.

1.1.1. Основные концептуальные положения системы защиты информации

Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

- хорошо развитый ассортимент технических средств защиты информации, производимых на промышленной основе;
- значительное число имеющих необходимые лицензии организаций, специализирующихся на решении вопросов защиты информации;
- достаточно четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта и др.

И, тем не менее, как свидетельствуют отечественные и зарубежные СМИ, число злоумышленных действий над информацией не только не уменьшается, но и имеет достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса. Опыт также показывает, что:

- обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;
- безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм - систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;
- никакая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту (рис. 1.1).

С учетом накопленного опыта можно определить систему защиты информации как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

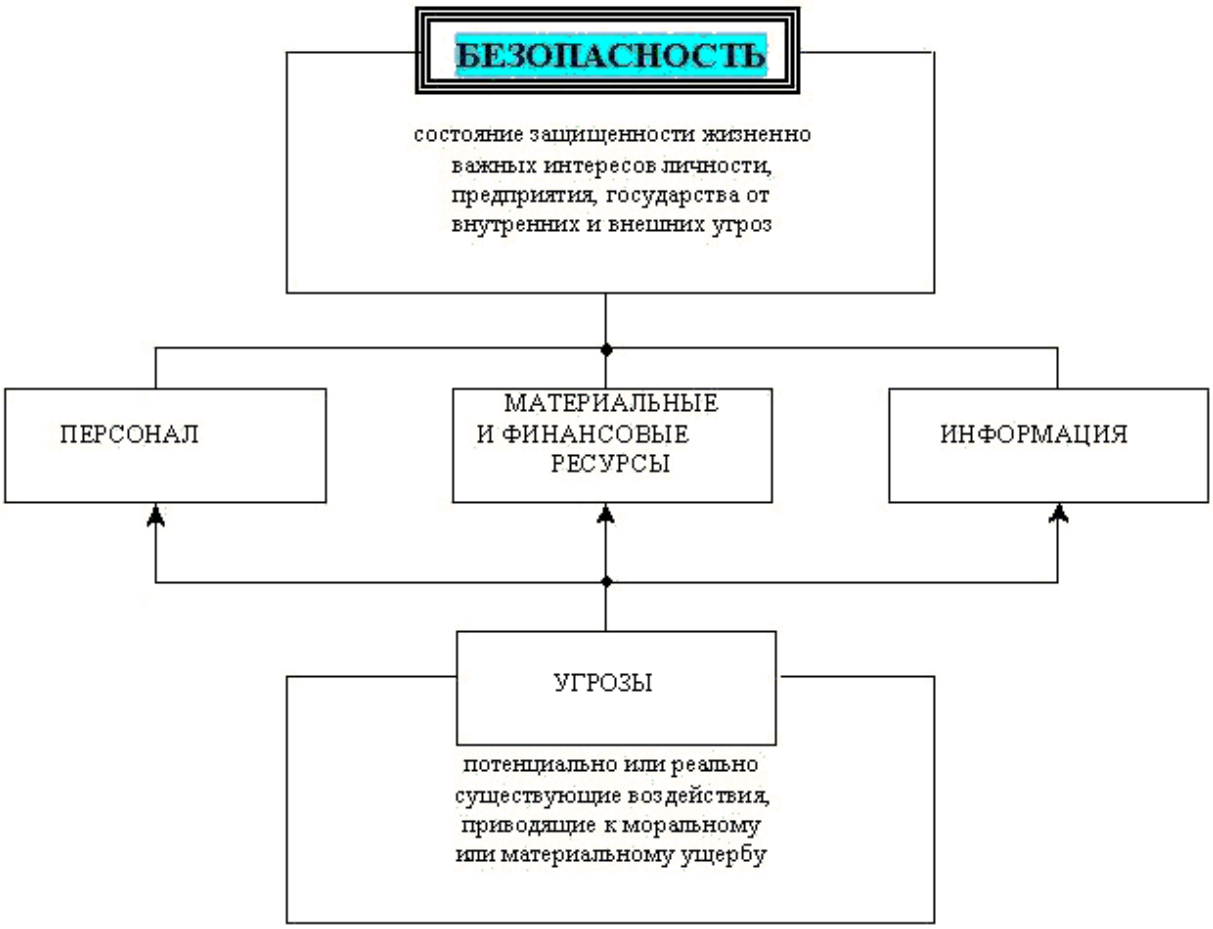


Рис. 1.1

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

- непрерывной. Это требование исходит из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;
- плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);
- целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
- конкретной. Защите подлежат конкретные данные, объективно нуждающиеся в охране, утрата которых может причинить организации определенный ущерб;
- активной. Защищать информацию необходимо с достаточной степенью настойчивости;
- надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
- универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
- комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита - это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств,

тенденций. Зарубежный и отечественный опыт показывают, что для обеспечения выполнения столь многогранных требований безопасности система защиты информации должна удовлетворять определенным условиям:

- охватывать весь технологический комплекс информационной деятельности;
- быть разнообразной по используемым средствам, многоуровневой с иерархической последовательностью доступа;
- быть открытой для изменения и дополнения мер обеспечения безопасности информации;
- быть нестандартной, разнообразной. При выборе средств защиты нельзя рассчитывать на неосведомленность злоумышленников относительно ее возможностей;
- быть простой для технического обслуживания и удобной для эксплуатации пользователями;
- быть надежной. Любые поломки технических средств являются причиной появления неконтролируемых каналов утечки информации;
- быть комплексной, обладать целостностью, означающей, что ни одна ее часть не может быть изъята без ущерба для всей системы.
- К системе безопасности информации предъявляются также определенные требования:
- четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;
- учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
- обеспечение оценки степени конфиденциальности информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.
- Система защиты информации, как любая другая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:
- правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действий;
- организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами - такими, как служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и др.;
- аппаратное обеспечение. Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно СЗИ;
- информационное обеспечение. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;
- программное обеспечение. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации;
- математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;
- лингвистическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Под *системой безопасности* будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз (рис. 1.2).

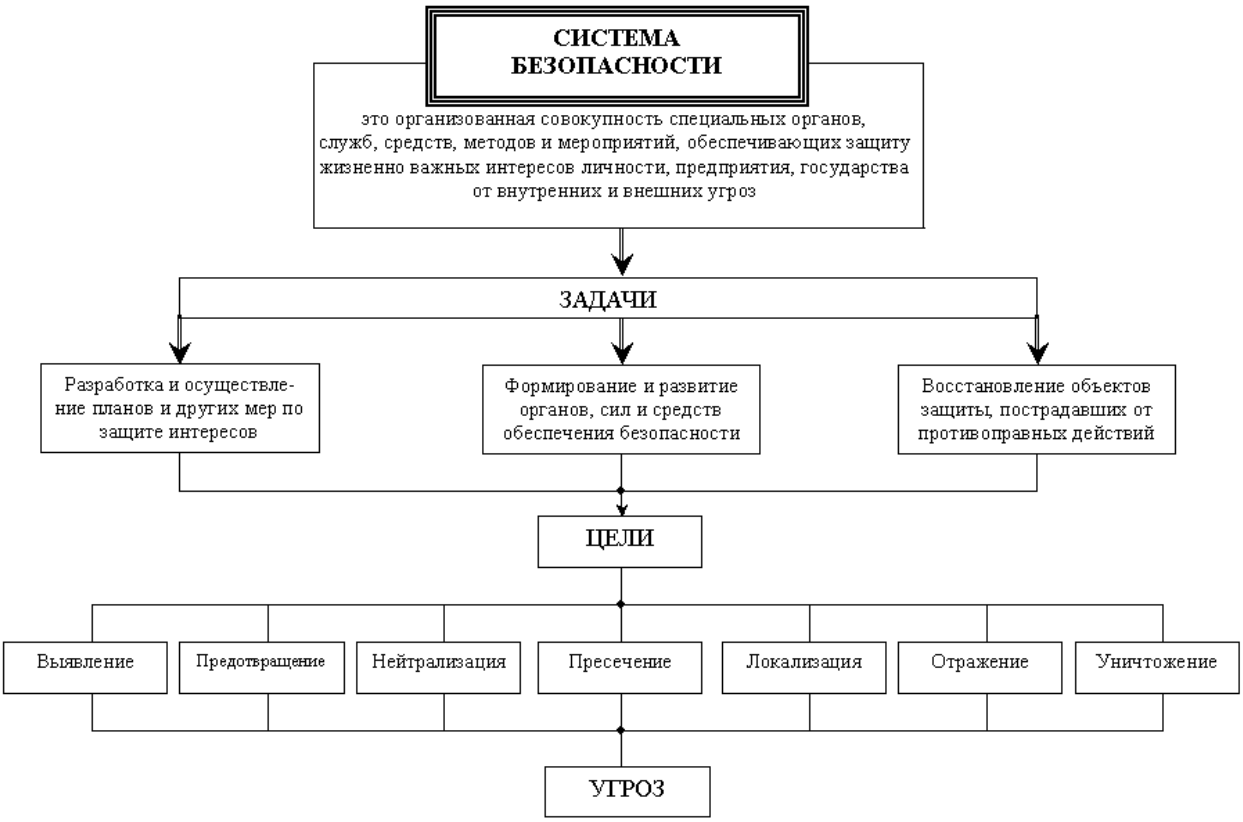


Рис. 1.2

Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

1.1.2. Концептуальная модель информационной безопасности

Понимая информационную безопасность как "состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, страны", правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность. При этом, естественно, следует рассматривать и меры защиты информации от неправомерных действий, приводящих к нанесению ущерба.

Практика показала, что для анализа такого значительного набора источников, объектов, действий целесообразно использовать методы имитационного моделирования, при которых формируется как бы "заместитель" реальных ситуаций. При этом следует учитывать, что модель не копирует оригинал, она проще. Модель должна быть достаточно общей, чтобы описывать реальные действия с учетом их сложности.

Можно предложить следующие компоненты модели информационной безопасности на первом уровне декомпозиции:

- объекты угроз;
- угрозы;
- источники угроз;
- цели угроз со стороны злоумышленников;
- источники информации;
- способы неправомерного овладения конфиденциальной информацией (способы доступа);
- направления защиты информации;
- способы защиты информации;
- средства защиты информации.

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы.

Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба (рис. 1.3)

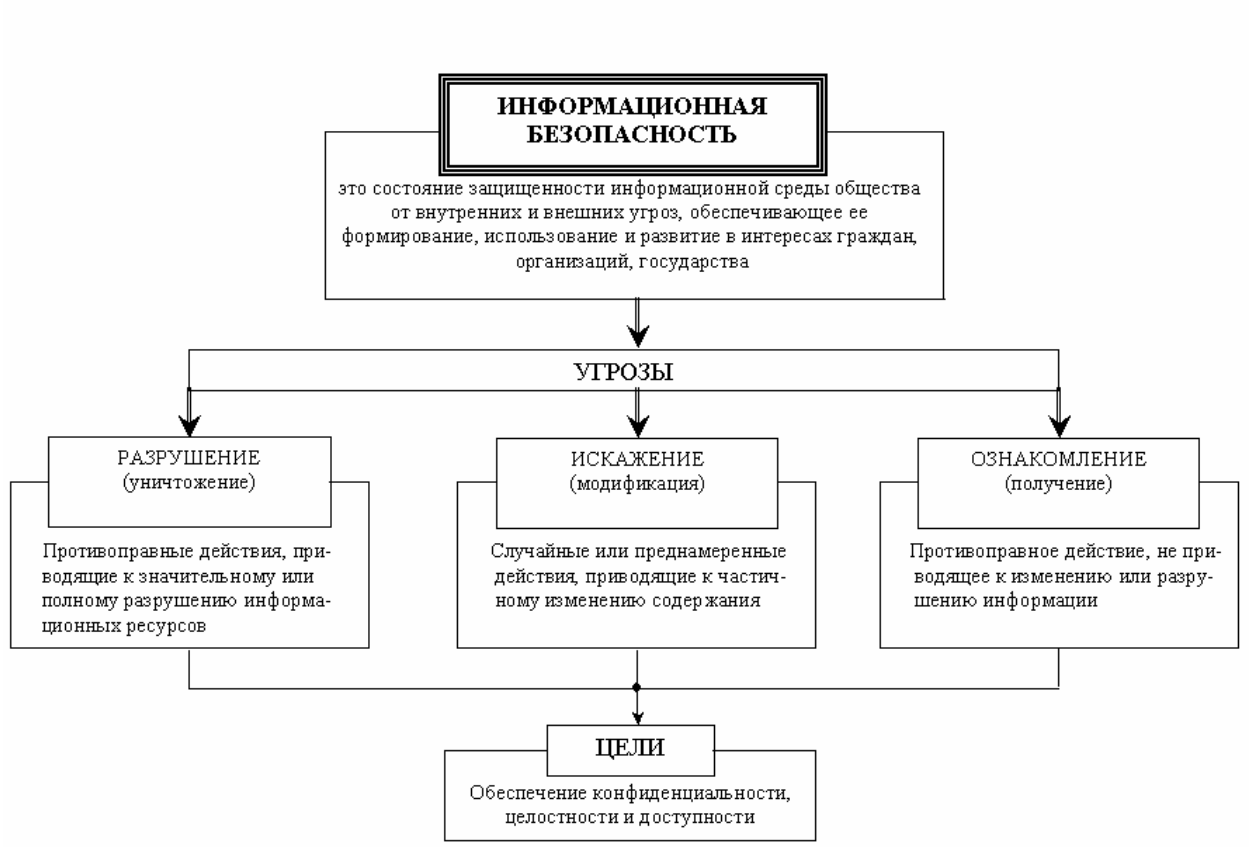


Рис. 1.3

Неправомерное овладение конфиденциальной информацией возможно за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкционированного доступа к охраняемым сведениям.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.

Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы. Последние могут быть реализованы как аппаратно, программно, так и так и смешанно - программно-аппаратными средствами.

В качестве *способов защиты* выступают всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу.

В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме (рис. 1.4).

Рис. 1.4

1.1.3. Угрозы конфиденциальной информации

Под *угрозами* конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями. Такими действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности (рис. 1.5), что, в свою очередь, приводит к нарушению как режима, управления, так и его качества в условиях ложной или неполной информации.

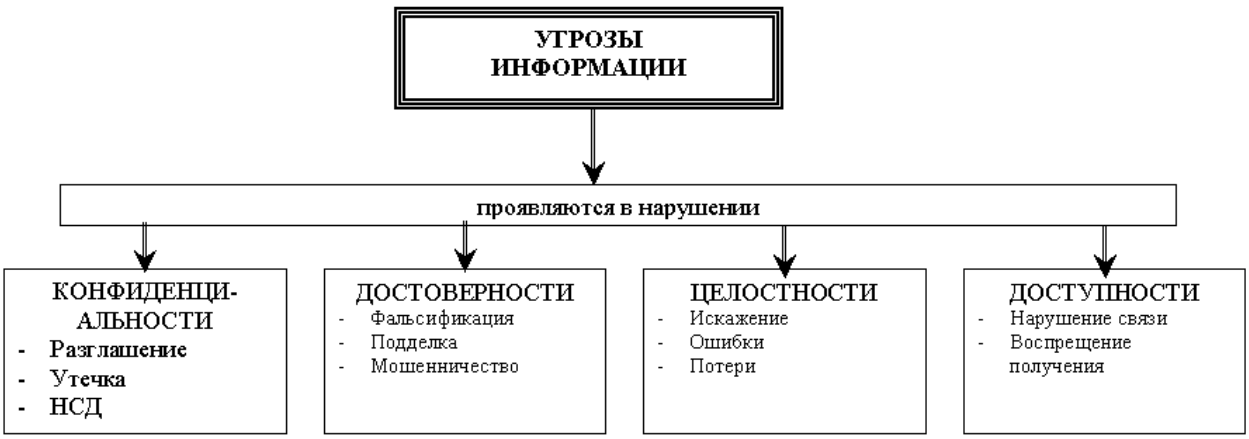


Рис.5

Каждая угроза влечет за собой определенный ущерб - моральный или материальный, а защита и противодействие угрозе призваны снизить ее величину хотя бы частично.

С учетом сказанного угрозы могут быть классифицированы следующим образом (рис. 1.6):

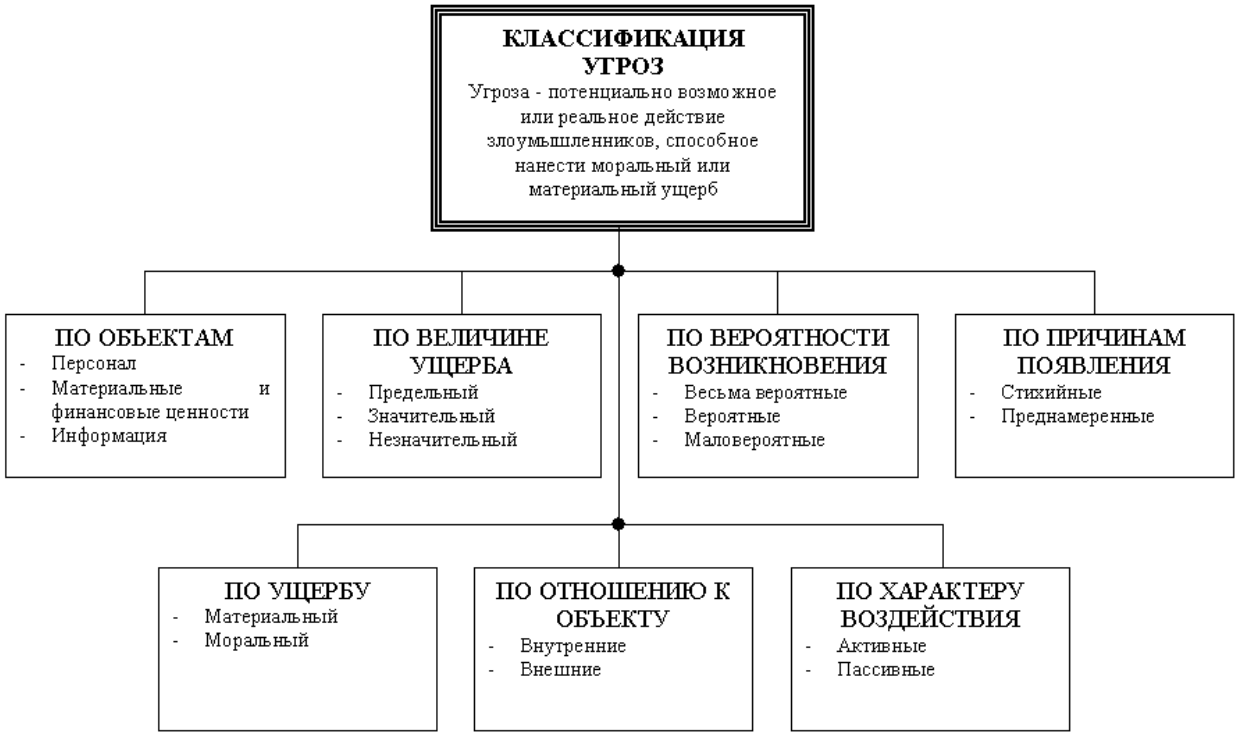


Рис. 1.6

По величине нанесенного ущерба:

- предельный, после которого фирма может стать банкротом;
- значительный, но не приводящий к банкротству;
- незначительный, который фирма за какое-то время может компенсировать и др.;

по вероятности возникновения:

- весьма вероятная угроза;
- вероятная угроза;
- маловероятная угроза;

по причинам появления:

- стихийные бедствия;
- преднамеренные действия;

по характеру нанесенного ущерба:

- материальный;
- моральный;

по характеру воздействия:

- активные;
- пассивные;

по отношению к объекту:

- внутренние;
- внешние.

Источниками внешних угроз являются:

- недобросовестные конкуренты;
- преступные группировки и формирования;
- отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:

- администрация предприятия;
- персонал;

- технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:

82 % угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;

17 % угроз совершается извне - внешние угрозы;

1 % угроз совершается случайными лицами.

1.1.4. Действия, приводящие к неправомерному овладению конфиденциальной информацией

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активности в действиях, приводящих к овладению конфиденциальными сведениями. В этом случае возможны такие ситуации:

- владелец (источник) не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;
- источник информации строго соблюдает меры информационной безопасности, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное, заходовое или беззаходовое;
- промежуточная ситуация - это утечка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

Факт получения охраняемых сведений злоумышленниками или конкурентами называют *утечкой*. Однако одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и несанкционированный доступ к конфиденциальной информации (рис. 1.7).

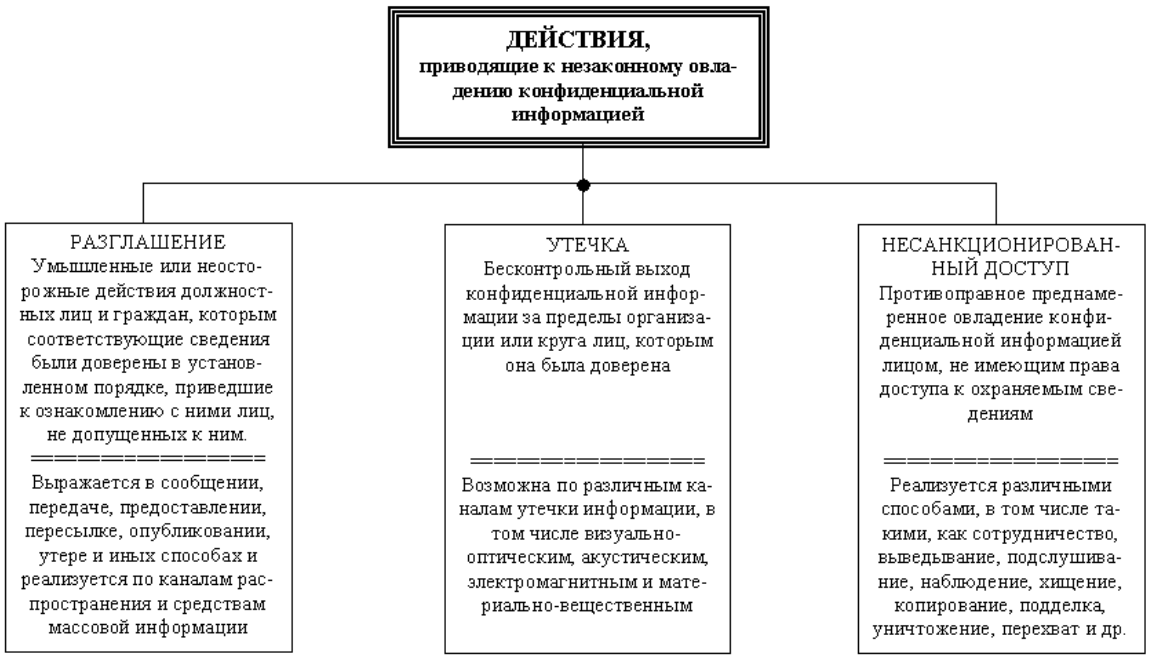


Рис. 1.7

1. *Разглашение* - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным

коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами средствами передачи официальной информации (почта, телефон, телеграф и др.). Неформальные коммуникации включают личное общение (встречи, переписка и др.), выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Здесь важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства (диктофоны, видеомониторинг).

2. Утечка - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации осуществляется по различным техническим каналам, Поскольку информация переносится или передается либо энергией, либо веществом, то это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под *каналом утечки информации* принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

3. *Несанкционированный доступ* - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении "продать" секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения - стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами.

Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников. Такой подход к классификации действий, способствующих неправомерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной информационной безопасности.

С учетом изложенного приведем условия, способствующие неправомерному овладению конфиденциальной информацией:

- разглашение (примитивная болтливость сотрудников) - 32 %;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок - 24 %;
- отсутствие на предприятии надлежащего контроля и жестких условий обеспечения информационной безопасности - 14 %;
- традиционный обмен производственным опытом - 12 %;
- бесконтрольное использование информационных систем - 10 %;
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций - 8 %.

Среди форм и методов недобросовестной конкуренции наибольшее распространение имеют следующие:

- экономическое подавление, выражающееся в срыве сделок и иных соглашений (48 %), блокировании деятельности предприятия (31 %), компрометации предприятия (11 %), шантаже руководителей предприятия (10 %);
- физическое подавление: ограбления и разбойные нападения на офисы, склады, грузы (73 %), угрозы физической расправы над руководителями предприятия и ведущими специалистами (22 %), убийства и захват заложников (5 %);
- информационное воздействие: подкуп сотрудников (43 %), копирование информации (24 %), проникновение в базы данных (18 %), продажа конфиденциальных документов (10 %), подслушивание телефонных переговоров и переговоров в помещениях (5 %), а также ограничение доступа к информации, дезинформация;
- финансовое подавление включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество;
- психическое давление может выражаться в виде хулиганских выходок, угрозы и шантажа, энергоинформационного воздействия.

Каждому из условий неправомерного овладения конфиденциальной информацией можно поставить в соответствие определенные каналы, определенные способы защитных действий и определенные классы средств защиты или противодействия. Совокупность определений, способов и средств представляется в виде следующей схемы (рис. 1.8).

Рис. 1.8

1.2. Направления обеспечения информационной безопасности

Направления обеспечения информационной безопасности - это нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз.

9. Если не уверен в безопасности, считай, что опасность существует реально.
10. Безопасности бесплатной не бывает.
11. Безопасности не бывает много.
12. Безопасность должна быть только комплексной.
13. Комплексная безопасность может быть обеспечена только системой безопасности.
14. Никакая система безопасности не обеспечивает требуемого уровня без надлежащей подготовки руководителей, сотрудников и клиентов.

Направления обеспечения безопасности рассматриваются как нормативно-правовые категории, определяющие комплексные меры защиты информации на государственном уровне, на уровне предприятия, на уровне отдельной личности (рис. 2.1.).

Рис. 2.1

С учетом сложившейся практики обеспечения информационной безопасности выделяют следующие направления защиты информации:

- *правовая защита* - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- *организационная защита* - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого либо ущерба исполнителям;
- *инженерно-техническая защита* - это использование различных технических средств, препятствующих нанесению ущерба производственной деятельности (рис. 2.1).

Кроме этого, защитные действия, ориентированные на обеспечение информационной безопасности, могут быть охарактеризованы целым рядом параметров, отражающих, помимо направлений, ориентацию на объекты защиты, характер угроз, способы действий, их распространенность, охват и масштабность (рис. 2.2).

Так, по характеру угроз защитные действия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа. По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение и восстановление ущерба или иных убытков. По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры. Масштабность защитных мероприятий характеризуется как объектовая, групповая или индивидуальная защита. Например, защита автономной ПЭВМ в режиме индивидуального пользования.

Правовая защита подробно будет рассмотрена в главе 2.3. Остановимся более детально на средствах и методах организационной и инженерно-технической защиты.

Рис2_2

1.2.1. Организационная защита

Организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- охрану, режим, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз производственной деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, т.к. возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

К основным организационным мероприятиям можно отнести:

организацию режима и охраны. Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и подержание надежного пропускного режима и контроля сотрудников и посетителей и др.;

организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

организацию работы с документами, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

организацию работ по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей (рис. 2.3).

Рис. 2.3

В каждом конкретном случае организационные мероприятия носят специфические для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Специфической областью организационных мер является организация защиты ПЭВМ, информационных систем и сетей, которая определяет порядок и схему функционирования основных ее подсистем, использование устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативно-правовыми требованиями и правилами. Защита информации на основе организационных мер играет большую роль в обеспечении надежности и эффективности, т.к. несанкционированный доступ и утечка информации чаще всего обусловлены злоумышленными действиями или небрежностью пользователей либо персонала. Эти факторы практически невозможно исключить или локализовать с помощью аппаратных и программных средств, криптографии и физических средств защиты. Поэтому совокупность организационных, организационно-правовых и организационно-технических мероприятий, применяемых совместно с техническими методами, имеют целью исключить, уменьшить или полностью устранить потери при действии различных нарушающих факторов.

Организационные средства защиты ПЭВМ и информационных сетей применяются:

- при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы, исключающих влияние стихийных бедствий, возможность недозволенного проникновения в помещения и др.;
- при подборе и подготовке персонала. В этом случае предусматриваются проверка принимаемых на работу, создание условий, при которых персонал был бы заинтересован в сохранности данных, обучение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.;
- при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.);
- при соблюдении надежного пропускного режима к техническим средствам, к ПЭВМ и информационным системам при сменной работе (выделение ответственных за защиту информации в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов);
- при внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требованиям защиты, документальное оформление изменений и др.);
- при подготовке и контроле работы пользователей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера.

Очевидно, что организационные мероприятия должны четко планироваться, направляться и осуществляться какой-то организационной структурой, каким-то специально созданным для этих целей структурным подразделением, укомплектованным соответствующими специалистами по безопасности производственной деятельности и защите информации. Зачастую таким структурным подразделением является служба безопасности предприятия, на которую возлагаются следующие общие функции:

- организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации;
- обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководство работами по правовому и организационному регулированию отношений по защите информации;
- участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разработка и осуществление совместно с другими подразделениями мероприятий по обеспечению работы с документами, содержащими конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований "Инструкции по защите конфиденциальной информации";
- изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и последующего противодействия любым попыткам нанесения ущерба, ведения учета и анализа нарушений режима безопасности, накопление и анализ данных о злоумышленных устремлениях конкурентных организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
- организация и проведение служебных расследований по фактам разглашения сведений, утрат документов, утечки конфиденциальной информации и других нарушений безопасности предприятия;
- разработка, ведение, обновление и пополнение "Перечня сведений конфиденциального характера" и других нормативных актов, регламентирующих порядок обеспечения безопасности и защиты информации;
- обеспечение строгого выполнения требований нормативных документов по защите производственных секретов предприятия;
- осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и другими структурами в части оговоренных в договорах условий по защите конфиденциальной информации;
- организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности;
- ведение учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам охраняемых секретов;
- обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз;
- поддержание контактов с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе и оказания взаимной помощи в кризисных ситуациях.

Служба безопасности является самостоятельной организационной единицей предприятия, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. Организационно служба безопасности состоит из следующих структурных единиц:

- подразделения режима и охраны;
- специального подразделения обработки документов конфиденциального характера;
- инженерно-технических подразделений;
- информационно-аналитических подразделений.

В таком составе службы безопасности способна обеспечить защиту конфиденциальной информации от любых угроз. К задачам службы безопасности предприятия относятся:

- определение круга лиц, которые в силу занимаемого служебного положения на предприятии прямо или косвенно имеют доступ к сведениям конфиденциального характера;
- определение участков сосредоточения конфиденциальных сведений;
- определение круга сторонних предприятий, связанных с данным предприятием кооперативными связями, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера;
- выявление круга лиц, не допущенных к конфиденциальной информации, но проявляющих повышенный интерес к таким сведениям;
- выявление круга предприятий, в том числе и иностранных, заинтересованных в овладении охраняемыми сведениями с целью нанесения экономического ущерба данному предприятию, устранения экономического конкурента либо его компрометации;
- разработка системы защиты документов, содержащих сведения конфиденциального характера;
- определение на предприятий участков, уязвимых в аварийном отношении, выход из строя которых может нанести материальный ущерб предприятию и сорвать поставки готовой продукции или комплектующих предприятиям, связанных с ним договорными обязательствами;
- определение на предприятии технологического оборудования, выход (или вывод) которого из строя может привести к большим экономическим потерям;
- определение уязвимых мест в технологии производственного цикла, несанкционированное изменение, в которой может привести к утрате качества выпускаемой продукции и нанести материальный или моральный ущерб предприятию;
- определение мест на предприятии, несанкционированное посещение которых может привести к изъятию (краже) готовой продукции или полуфабрикатов, заготовок и др., и организация их физической защиты и охраны;
- определение и обоснование мер правовой, организационной и инженерно-технической защиты предприятия, персонала, продукции и информации;
- разработка необходимых мероприятий, направленных на совершенствование системы экономической, социальной и информационной безопасности предприятия;
- внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической и информационной безопасности;
- организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями;
- изучение, анализ и оценка состояния обеспечения экономической и информационной безопасности предприятия и разработка предложений и рекомендаций для их совершенствования;
- разработка технико-экономических обоснований, направленных на приобретение технических средств, получение консультации у специалистов, разработку необходимой документации в целях совершенствования системы мер по обеспечению экономической и информационной безопасности.

1.2.2. Инженерно-техническая защита

Инженерно-техническая защита - это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты *конфиденциальной информации*. Поскольку совокупность целей, задач, объектов защиты и проводимых мероприятий очень разнородна и многообразна, необходимо систематизировать эту совокупность, введя классификацию средств по виду, ориентации и другим характеристикам (см. рис. 2.4).

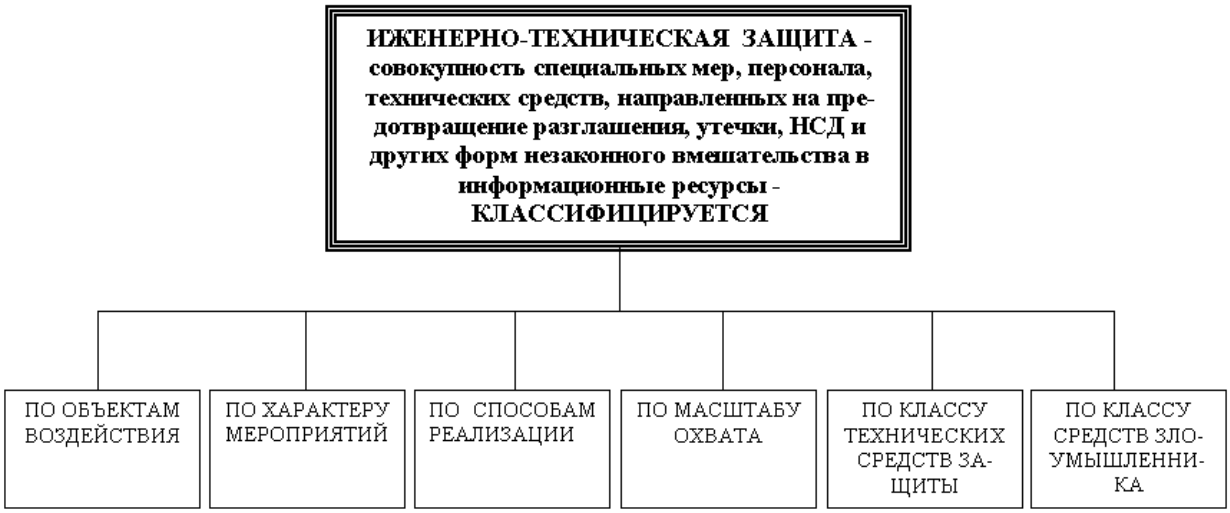


Рис. 2.4

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности. По функциональному назначению средства инженерно-технической защиты классифицируются на следующие группы:

- *физические средства*, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации (рис. 2.5) и осуществляющие защиту персонала, материальных средств и финансов и информации от противоправных воздействий;
- *аппаратные средства* - приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств - обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства, применяемые в производственной деятельности;
- *программные средства*, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
- *криптографические средства* - специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Аппаратные средства и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть используемы.

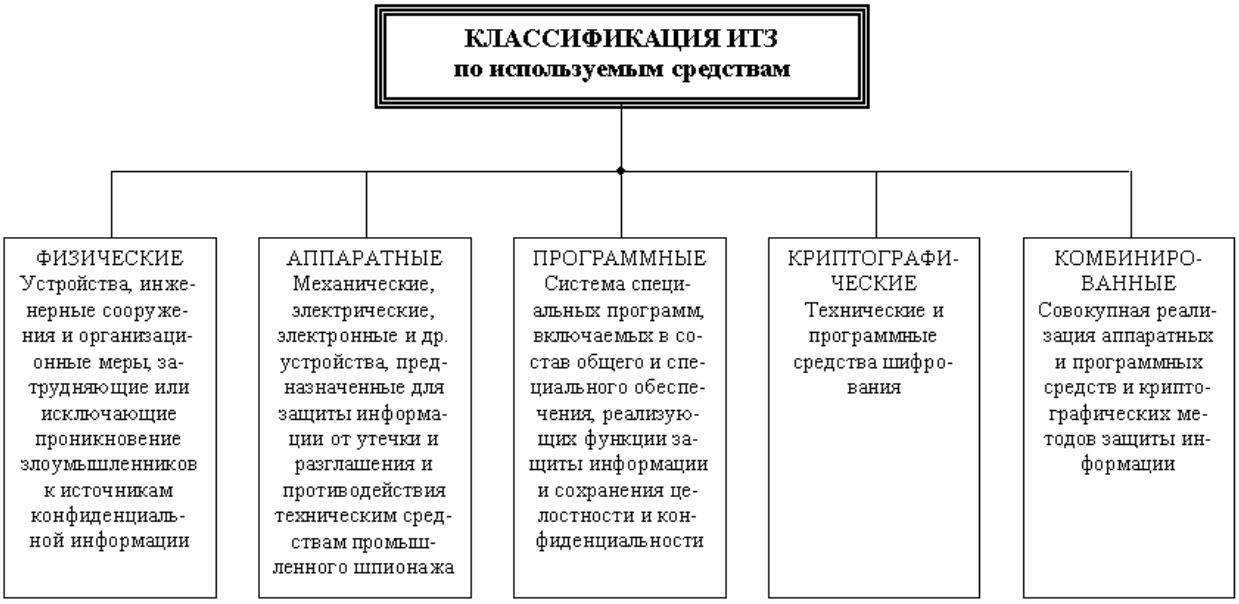


Рис. 2.5

Программные средства и методы защиты надежны, и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных.

Криптографические методы занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды.

Очевидно, что такое деление средств защиты информации достаточно условно, т.к. на практике очень часто они и взаимодействуют и реализуются в комплексе в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации. Аппаратные и программные средства и методы защиты будут рассмотрены в последующих главах. Остановимся на основных принципах криптографической защиты информации, а также дадим понятия физических средств защиты.

1.2.2.1. Физические средства защиты

Физические средства защиты - это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий реализации целей злоумышленников. К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий (рис. 2.6).

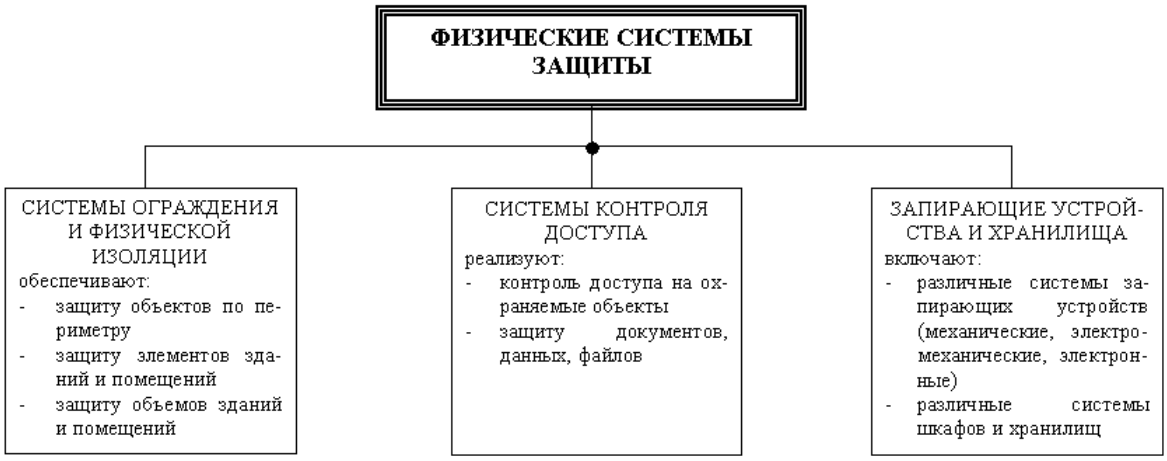


Рис. 2.6

Эти средства применяются для решения следующих задач:

1. охрана территории предприятия и наблюдение за ней;
2. охрана зданий, внутренних помещений и контроль за ними;
3. охрана оборудования, продукции, финансов и информации;
4. осуществление контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз. Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов - это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание взрывпакетов и др.). Средства пожаротушения относятся к системам ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства физической защиты.

Охранные системы

Охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения.

Важнейшими элементами охранных систем являются датчики, обнаруживающие появление угрозы. Характеристики и принципы работы датчиков определяют основные параметры и практические возможности охранных систем. Разработано и широко используется значительное количество самых разнообразных датчиков как по принципам обнаружения различных физических полей, так и по тактическому использованию.

Эффективность работы системы охраны и охранной сигнализации в основном определяется параметрами и принципом работы датчиков. В настоящее время известны датчики следующих типов: механические выключатели, проволока с выключателем, магнитный выключатель, ртутный выключатель, коврики давления, металлическая фольга, проволочная сетка, шифроволновой датчик, ультразвуковой датчик, инфракрасный датчик, фотоэлектрический датчик, акустический датчик, вибрационный датчик, индуктивный датчик, емкостный датчик и др.

Каждый тип датчика реализует определенный вид защиты: точечная защита, защита по линии, защита по площади или защита по объему. Механические датчики ориентированы на защиту линии, коврики давления - на точечное обнаружение, а инфракрасные находят широкое применение по площади и по объему.

Датчики с помощью различных каналов связи соединены с контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного оповещения. Каналами связи в системах охранной сигнализации могут быть специально проложенные проводные или кабельные линии, телефонные линии объекта, линии связи трансляции, системы освещения или радиоканалы. Выбор каналов определяется возможностями объекта. Важным объектом охранной системы являются средства тревожного оповещения: звонки, лампочки, сирены, подающие постоянные или прерываемые сигналы о появлении угрозы.

По тактическому назначению охранные системы подразделяются на системы охраны:

- периметров объектов;
- помещений и проходов в служебных и складских зданиях;
- сейфов, оборудования, основных и вспомогательных технических средств;
- автотранспорта;
- персонала, в том числе и личного состава охраны, и др.

К средствам физической защиты относятся:

- естественные и искусственные барьеры;
- особые конструкции периметров, проходов, оконных и дверных переплетов, помещений, сейфов, хранилищ и др.;
- зоны безопасности.

Естественные и искусственные барьеры служат для противодействия незаконному проникновению на территорию объекта. Однако основная защитная нагрузка ложится все-таки на искусственные барьеры - такие, как заборы и другие виды ограждений. Практика показывает, что ограждения сложной конфигурации способны задержать злоумышленника на достаточно большое время. На сегодня насчитывается значительный арсенал таких средств: от простых сетчатых до сложных комбинированных ограждений, оказывающих определенное отпугивающее воздействие на нарушителя.

Особые конструкции периметров, проходов, оконных переплетов, помещений, сейфов, хранилищ являются обязательными с точки зрения безопасности для любых организаций и предприятий. Эти конструкции должны противостоять любым способам физического воздействия со стороны криминальных элементов: механическим деформациям, разрушению сверлением, термическому и механическому резанию, взрыву и др.; несанкционированному доступу путем подделки ключей, угадыванию кода и др. Одним из главных технических средств защиты проходов, помещений, сейфов и хранилищ являются замки. Они бывают простыми (с ключами), кодовыми (в том числе и с временной задержкой на открывание) и с программными устройствами, открывающие двери и сейфы только в определенные часы.

Важнейшим средством физической защиты является планировка объекта, его зданий и помещений по зонам безопасности, которые учитывают степень важности различных частей объекта с точки зрения нанесения ущерба от различного вида угроз. Оптимальное расположение зон безопасности и размещение в них эффективных технических средств обнаружения, отражения и ликвидации последствий противоправных действий составляет основу концепции инженерно-технической защиты объекта.

Зоны безопасности должны располагаться на объекте последовательно, от забора вокруг территории объекта до хранилищ ценностей, создавая цепь чередующихся друг за другом препятствий (рубежей), которые придется преодолевать злоумышленнику. Чем сложнее и надежнее препятствие на его пути, тем больше времени потребуется на преодоление каждой зоны и тем больше вероятность того, что расположенные в каждой зоне средства обнаружения (охранные посты, охранная сигнализация и охранное телевидение) выявят наличие нарушителя и подадут сигнал тревоги. Основу планировки и оборудования зон безопасности объекта составляет принцип равнопрочности границ зон безопасности. Суммарная прочность зон безопасности будет оцениваться наименьшей из них.

Охранное телевидение

Одним из распространенных средств охраны является охранное телевидение. Привлекательной особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Через объектив изображение злоумышленника попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по специальному коаксиальному кабелю на монитор и при необходимости - на видеомагнитофон. Видеокамера является наиболее важным элементом системы охранного телевидения, т.к. от ее характеристик зависит эффективность и результативность всей системы контроля и наблюдения. В настоящее время разработаны и выпускаются самые разнообразные модели, различающиеся как по габаритам, так и по возможностям и по конструктивному исполнению.

Вторым по значимости элементом системы охранного телевидения является монитор. Он должен быть согласован по параметрам с видеокамерой. Часто используется один монитор с несколькими камерами, подсоединяемыми к нему поочередно средствами автоматического переключения по определенному регламенту. В некоторых системах телевизионного наблюдения предусматривается возможность автоматического подключения камеры, в зоне обзора которой произошло нарушение. Используется и более сложное оборудование, включающее средства

автоматизации, устройства одновременного вывода нескольких изображений, детекторы движения для подачи сигнала тревоги при выявлении каких-либо изменений в изображении.

Охранное освещение

Обязательной составной частью системы защиты любого объекта является охранное освещение. Различают два вида охранного освещения - дежурное и тревожное. Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри здания. Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и пр.). Сигнализация и дежурное освещение должны иметь резервное электропитание на случай аварии или выключения электросети.

Ограждения и физическая изоляция

В последние годы большое внимание уделяется созданию систем физической защиты, совмещенных с системами сигнализации. Так, известна электронная система сигнализации для использования в проволочном заграждении. Система состоит из электронных датчиков и микропроцессора, управляющего блоком обработки данных. Заграждение длиной до 100 м может устанавливаться на открытой местности или размещаться на стенах, чердаках и имеющихся оградах. Устойчивые к воздействию окружающей среды датчики монтируются на стойках, кронштейнах. Проволочное заграждение состоит из 32 горизонтально натянутых стальных нитей, в средней части каждой из которых крепится электромеханический датчик, преобразующий изменение натяжения нитей в электрический сигнал. Превышение пороговой величины напряжения, программируемое по амплитуде для каждого датчика отдельно, вызывает сигнал тревоги. Связь системы с центральным пунктом управления и контроля осуществляется с помощью мультиплексора. Микропроцессор автоматически через определенные интервалы времени проверяет работу компонентов аппаратуры и программных средств и - в случае установления отклонений - подает соответствующий сигнал. Подобные системы физической защиты могут использоваться для защиты объектов по периметру в целях обнаружения вторжения на территорию объекта.

Используются системы из сетки двух волоконно-оптических кабелей, по которым передаются кодированные сигналы инфракрасного диапазона. Если в сетке нет повреждений, то сигналы поступают на приемное устройство без искажений. Попытки повреждения сетки приводят к обрывам или деформации кабелей, что вызывает сигнал тревоги. Оптические системы отличаются низким уровнем ложных тревог, вызванных воздействию на нее мелких животных, птиц, изменением погодных условий и высокой вероятностью обнаружения попыток вторжения.

Следующим видом физической защиты является защита элементов зданий и помещений. Хорошую физическую защиту оконных проемов помещений обеспечивают традиционные металлические решетки, а также специальное остекление на основе пластмасс, армированных стальной проволокой. Двери и окна охраняемого помещения оборудуются датчиками, срабатывающими при разрушении стекол, дверей, но не реагирующими на их колебания, вызванные другими причинами. Срабатывание датчиков вызывает сигнал тревоги.

Среди средств физической защиты особо следует отметить средства защиты ПЭВМ от хищения и проникновения к их внутренним компонентам. Для этого используют металлические конструкции с клейкой подставкой, которая обеспечивает сцепление с поверхностью стола с силой в 2500 - 2700 кг/см^2. Это исключает изъятие или перемещение ПЭВМ без нарушения целостности поверхностного слоя. Перемещение ПЭВМ возможно только с использованием специальных ключей и инструментов.

Запирающие устройства

Запирающие устройства и специальные шкафы занимают особое место в системах ограничения доступа, поскольку они несут в себе признаки как систем физической защиты, так и устройств контроля доступа. Они отличаются большим разнообразием и предназначены для защиты документов, материалов, магнитных и фотоносителей и даже технических средств: ПЭВМ, калькуляторов, принтеров, ксероксов и пр.

Выпускаются специальные металлические шкафы для хранения ПЭВМ и другой техники. Такие шкафы снабжаются надежной двойной системой запирания: замком ключевого типа и трех-пятизначным комбинированным замком. Такие шкафы обладают прочностью и надежностью, достаточными для защиты от промышленного шпионажа. Выпускаются замки с программируемым временем открывания с помощью механических или электронных часов.

Системы контроля доступа

Регулирование доступа в помещения или здания осуществляется прежде всего посредством опознавания службой охраны или техническими средствами. Контролируемый доступ предполагает ограничение круга лиц, допускаемых в определенные защищаемые зоны, здания, помещения, и контроль за передвижение этих лиц внутри них. Основанием допуска служит определенный метод опознавания и сравнения с разрешительными параметрами системы. Имеется очень широкий спектр методов опознавания уполномоченных лиц на право их доступа в помещения, здания, зоны. На основе опознавания принимается решение о допуске лиц, имеющих на это право, или запрещение - для не имеющих его. Наибольшее распространение получили атрибутные и персональные методы опознавания. К атрибутным способам относятся средства подтверждения полномочий, такие, в частности, как документы (паспорт, удостоверение и др.), карты (фотокарточки, карты с магнитными, электрическими, механическими идентификаторами и пр.) и другие средства (ключи, сигнальные элементы и т.п.). Эти средства в значительной мере подвержены различного рода подделкам и мошенничеству.

Персональные методы - это методы определения лица по его независимым показателям: отпечаткам пальцев, геометрии рук, особенностям глаз и др. Персональные характеристики бывают статические и динамические. К последним относятся пульс, давление, кардиограммы, речь, почерк и пр. Персональные способы наиболее привлекательны. Во-первых, они полно описывают каждого отдельного человека. Во-вторых, невозможно или крайне трудно подделать индивидуальные характеристики.

Статические способы включают анализ физических характеристик - таких, как отпечатки пальцев, особенности геометрии рук и др. Они достаточно достоверны и обладают малой вероятностью ошибок. Динамические же способы используют изменяющиеся во времени опознавательные характеристики.

Характеристики, зависящие от привычек и навыков, являются не только наиболее простыми для подделок, но и наиболее дешевыми с точки зрения практической реализации. Способы опознавания, основанные на чем-либо запоминаемом (код, пароль и т.д.), могут применяться в случаях наиболее низких требований к безопасности, т.к. часто эта информация записывается пользователями на различных бумажках, в записных книжках и других носителях, что при их доступности другим может свести на нет все усилия по безопасности. Кроме того, имеется реальная возможность подсмотреть, подслушать или получить эту информацию другим путем (насилие, кража и др.)

Способ опознавания человеком (вахтер, часовой) не всегда надежен из-за так называемого "человеческого фактора", заключающегося в том, что человек подвержен влиянию многих внешних условий (усталость, плохое самочувствие, эмоциональный стресс, подкуп и пр.). В противовес этому находят широкое применение технические средства опознавания, такие как идентификационные карты, опознавание по голосу, почерку, пальцам и пр. Простейший и наиболее распространенный метод идентификации использует различные карты и карточки, на которых помещается кодированная или открытая информация о владельце, его полномочиях и т.д. Обычно это пластиковые карты типа пропусков или жетонов. Карты вводятся в читающее устройство каждый раз, когда требуется войти или выйти из охраняемого помещения или получить доступ к чему-нибудь (сейфу, камере, терминалу и т.п.). Существует много разновидностей устройств опознавания и идентификации личности, использующих подобные карты. Одни из них оптическим путем сличают фотографии и прочие идентификационные элементы, другие - магнитные поля и т.д. Рассмотрим ряд наиболее известных устройств (систем).

Системы опознавания по отпечаткам пальцев. В основу идентификации положено сравнение относительного положения окончаний и разветвлений линий отпечатка. Поисковая система ищет на текущем изображении контрольные элементы, определенные при исследовании эталонного образца. Для идентификации одного человека считается достаточным определение координат 12 точек. Эти системы, естественно, весьма сложны и рекомендуются к использованию на объектах, требующих надежной защиты.

Системы опознавания по голосу. Существует несколько способов выделения характерных признаков речи человека: анализ кратковременных сегментов, контрольный анализ, выделение статистических характеристик. Теоретически вопросы идентификации по голосу разработаны достаточно полно, но промышленное производство пока налажено слабо.

Системы опознавания по почерку считаются наиболее удобными для пользователя. Основным признаком идентификации по почерку является постоянство подписи каждого индивидуума, хотя абсолютного совпадения не бывает.

Система опознавания по геометрии рук. Для идентификации применяют анализ комбинации линий сгибов пальцев и ладони, линий складок, длины и толщины пальцев и др. Технически это реализуется путем наложения руки на матрицу фотоячеек. Рука освещается мощной лампой, производится регистрация сигналов с ячеек, несущих информацию о геометрии.

Все устройства идентификации человека могут работать как отдельно, так и в комплексе. Комплекс может быть узкоспециальным или многоцелевым, при котором система выполняет функции охраны, контроля, регистрации и сигнализации. Такие системы являются уже комплексными; они обеспечивают:

- допуск на территорию предприятия по карточке (пропуску), содержащей индивидуальный машинный код;
- блокирование прохода при попытках несанкционированного внедрения (проход без пропуска, проход в спецподразделения сотрудников, не имеющих допуска);
- возможность блокирования прохода для нарушителей графика работы (опоздание, преждевременный уход и т.п.);
- открытие зоны прохода для свободного выхода по команде вахтера;
- проверку кодов пропусков на задержание их предъявителей на КПП по указанию оператора системы;
- регистрацию времени пересечения проходной и сохранение его в базе данных персональной ЭВМ;
- обработку полученных данных и формирование различных документов (табель рабочего времени, суточный рапорт, ведомость нарушителей трудовой дисциплины и др.), что позволяет иметь оперативную информацию о нарушителях трудовой дисциплины, отработанном времени и пр.;
- оперативную корректировку информации базы данных с доступом по паролю;
- распечатку табелей рабочего времени по произвольной группе сотрудников (предприятие в целом, структурное подразделение, отдельно выбранные сотрудники);
- распечатку списков нарушителей графика рабочего времени с конкретными данными о нарушении;
- текущий и ретроспективный анализ посещения сотрудниками подразделений, передвижения сотрудников через КПП, выдачу списочного состава присутствовавших или отсутствовавших в подразделении или на предприятии для произвольно выбранного момента времени (при условии хранения баз данных за соответствующие периоды);
- получение оперативной информации абонентами локальной сети в случае сетевой реализации системы.

1.2.2.2. Криптографические средства защиты

Криптография представляет собой совокупность методов преобразования данных, ориентированных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблему конфиденциальности (путем лишения злоумышленника возможности извлечь информацию из канала связи) и проблему целостности (путем лишения злоумышленника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи).

Проблемы конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Обобщенная модель криптографической системы, обеспечивающей шифрование передаваемой информации, показана на рис. 2.7. Отправитель генерирует открытый текст исходного сообщения P, которое должно быть передано адресату по незащищенному каналу. За каналом следит перехватчик (злоумышленник) с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы перехватчик не смог узнать содержание сообщения P, отправитель шифрует его с помощью обратимого преобразования $E_к$ и получает шифртекст (криптограмму) $C=E_к(P)$, который отправляет адресату.

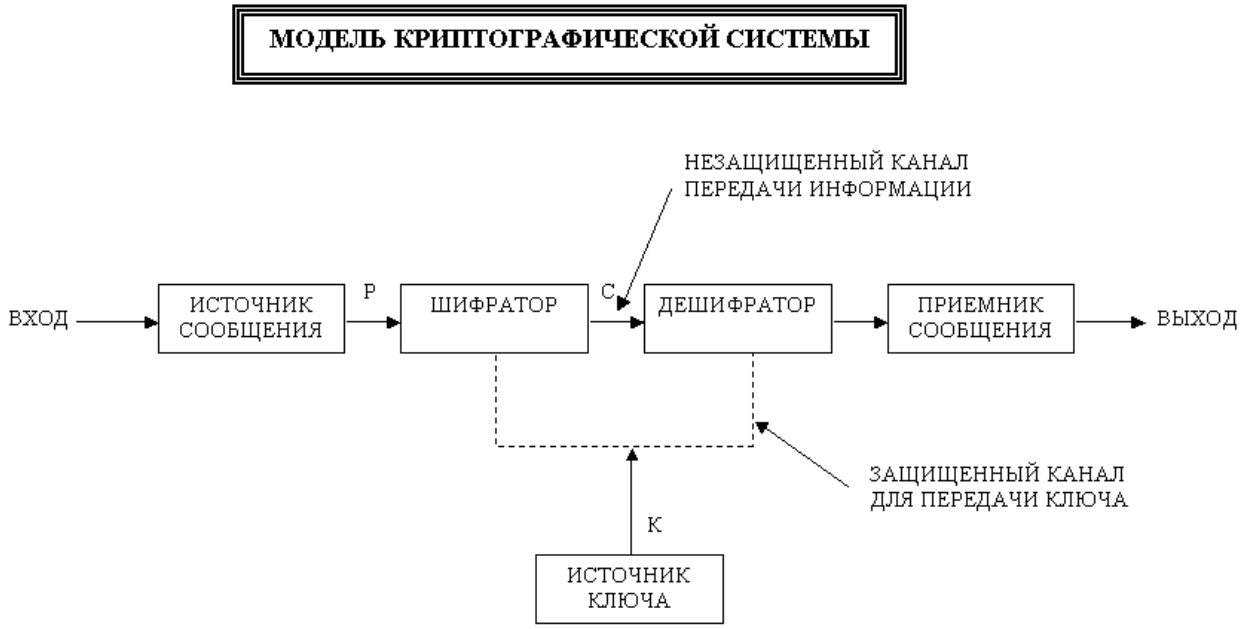


Рис. 2.7

Адресат, приняв шифртекст С, расшифровывает его с помощью обратного преобразования $Д=E_k^{-1}$ и получает исходное сообщение в виде открытого текста Р: $Д_к(C)= E_k^{-1}(E_к(P))=P$.

Преобразование $E_к$ выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим *ключом* К. Криптосистема имеет разные варианты реализации: набор инструкций, аппаратные средства, комплекс программ компьютера, которые позволяют зашифровать открытый текст и расшифровать шифртекст различными способами, один из которых выбирается с помощью конкретного ключа К.

Формализуя выше сказанное, криптографическая система - это однопараметрическое семейство $(E_K)_{K\in\overline{K}}$ обратимых преобразований $E_K : \overline{P} \to \overline{C}$ из пространства $\overline{P}$ сообщений открытого текста в пространство $\overline{C}$ шифрованных текстов. Параметр К (ключ) выбирается из конечного множества $\overline{K}$, называемого пространством ключей.

В общем случае преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Это важное свойство функции преобразования определяет два класса криптосистем:

- симметричные (одноключевые) криптосистемы;
- асимметричные (двуключевые) криптосистемы (с открытым ключом).

Схема симметричной криптосистемы с одним секретным ключом показана на рис. 2.7. В ней используются одинаковые секретные ключи в блоке шифрования и блоке расшифрования. В асимметричной криптосистеме с двумя разными ключами один из ключей является открытым, а другой - секретным.

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например, такому, как курьерская служба. На рис. 2.7 этот канал обозначен пунктирными линиями. Существуют и другие способы распределения секретных ключей. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют на месте его генерации.

Поскольку между шифратором и дешифратором передача информации осуществляется по незащищенному каналу, перехватчик может применить активные действия, заключающиеся не только в считывании всех шифртекстов, передаваемых по каналу, но и вз попытке изменения их по своему усмотрению. Любая попытка со стороны перехватчика расшифровать шифртекст С для получения открытого текста Р или зашифровать свой собственный текст М' для получения правдоподобного шифртекста С', не имея подлинного ключа, называется криптоаналитической атакой. Если предпринятые криптоаналитические атаки не достигают цели и криптоаналитик не

может, не имея подлинного ключа, вывести P из C или C' из M', то полагают, что такая криптосистема является криптостойкой.

Криптоанализ - это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу. Успешный анализ может раскрыть исходный текст или ключ. Он позволяет также обнаружить слабые места в криптосистеме, что, в конечном счете, ведет к тем же результатам. Фундаментальное правило криптоанализа, впервые сформулированное голландцем А.Керкхоффом еще в XIX веке, заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-нибудь такого, что невозможно быстро изменить в случае утечки секретной информации. Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств, тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа. Другое, почти общепринятое, допущение в криптоанализе состоит в том, что криптоаналитик имеет в своем распоряжении шифртексты сообщений.

Существует четыре основных типа криптоаналитических атак. Все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифртексты сообщений. Перечислим эти криптоаналитические атаки.

1. Криптоаналитическая атака при наличии только известного шифртекста. Криптоаналитик имеет только шифртексты $C_1, C_2,\ldots, C_в$ нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования $E_к$. Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты $P_1, P_2,\ldots, P_в$ по возможности большинства сообщений или, еще лучше, вычислить ключ К, использованный для шифрования этих сообщений, с тем, чтобы расшифровать и другие сообщения, зашифрованные этим ключом.
2. Криптоаналитическая атака при наличии известного открытого текста. Криптоаналитик имеет доступ не только к шифртекстам $C_1, C_2,\ldots, C_в$ нескольких сообщений, но также к открытым текстам $P_1, P_2,\ldots, P_в$ этих сообщений. Его работа заключается в нахождении ключа К, используемого при шифровании этих сообщений, или алгоритма расшифрования $Д_к$ любых новых сообщений, зашифрованных тем же самым ключом.
3. Криптоаналитическая атака при возможности выбора открытого текста. Криптоаналитик не только имеет доступ к шифртекстам $C_1, C_2,\ldots, C_в$ и связан с ними открытыми текстами $P_1, P_2,\ldots, P_в$ нескольких сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде. Такой криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоаналитик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Работа криптоаналитика состоит в поиске ключа К, использованного для шифрования сообщений, или алгоритма расшифрования $Д_к$ новых сообщений, зашифрованных тем же ключом.
4. Криптоаналитическая атака с адаптивным выбором открытого текста. Это- особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования. При криптоанализе с простым выбором открытого текста криптоаналитик обычно может выбирать несколько крупных блоков открытого текста для их шифрования; при криптоанализе с адаптивным выбором открытого текста сначала более мелкий пробный блок открытого текста, затем выбрать следующий блок в зависимости от результатов первого выбора и т.д. Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

Кроме перечисленных основных типов криптоаналитических атак, можно отметить, по крайней мере, еще два типа.

5. Криптографическая атака с использованием выбранного шифртекста. Криптоаналитик может выбирать для расшифрования различные шифртексты C1, C2,…, Cв и имеет доступ к расшифрованным открытыми текстами P1, P2,…, Pв.. Например, криптоаналитик

получил доступ к защищенному от несанкционированного вскрытия блоку, который выполняет автоматическое расшифрование. Работа криптоаналитика заключается в нахождении ключа. Этот тип криптоанализа представляет особый интерес для раскрытия алгоритмов с открытым ключом.

6. Криптоаналитическая атака методом полного перебора всех возможных ключей. Эта атака предполагает использование криптоаналитиком известного шифртекста и осуществляется посредством полного перебора всех возможных ключей с проверкой, является ли осмысленным получающийся открытый текст. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой. Существуют и другие, менее распространенные, криптоаналитические атаки.

Модуль 2. Правовая и техническая защита информации

2.3. Правовые основы информационной безопасности

2.3.1. Государственная политика информационной безопасности

Право - это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий и населения (отдельной личности).

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами (рис. 3.1).

Рис. 3.1

В нашей стране такими правилами (актами, нормами) являются Конституция, законы Российской Федерации, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Что касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, издаваемыми ведомствами, организациями и предприятиями, действующими в рамках определенных структур (рис. 3.2).

Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, его состава и содержания, соотнесения его со всей системой законов и правовых актов Российской Федерации.

Требования информационной безопасности должны органически включаться во все уровни законодательства, в том числе и в конституционное законодательство, основные общие законы, законы по организации государственной системы управления, специальные законы, ведомственные правовые акты и др. В литературе приводится такая структура правовых актов, ориентированных на правовую защиту информации.

Первый блок - конституционное законодательство. Нормы, касающиеся вопросов информатизации и защиты информации, входят в него как составные элементы.

Второй блок - общие законы, кодексы (о собственности, о недрах, о земле, о правах граждан, о гражданстве, о налогах, об антимонопольной деятельности и др.), которые включают нормы по вопросам информатизации и информационной безопасности.

Третий блок - законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы по вопросам защиты информации. Наряду с общими вопросами

информационного обеспечения и защиты информации конкретного органа эти нормы должны устанавливать его обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес.

Рис. 3.2

Четвертый блок - специальные законы, полностью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам. В их число, в частности, входит и Закон РФ "Об информации, информатизации и защите информации". Именно состав и содержание этого блока законов и создает специальное законодательство как основу правового обеспечения информационной безопасности.

Пятый блок - законодательство субъектов Российской Федерации, касающееся защиты информации.

Шестой блок - подзаконные нормативные акты по защите информации.

Седьмой блок - это правоохранительное законодательство России, содержащее нормы об ответственности за правонарушения в сфере информатизации.

Специальное законодательство в области безопасности информационной деятельности может быть представлено совокупностью законов. В их составе особое место принадлежит базовому Закону "Об информации, информатизации и защите информации", который закладывает основы правового определения всех важнейших компонентов информационной деятельности:

- информации и информационных систем;

- субъектов - участников информационных процессов;
- правоотношений производителей - потребителей информационной продукции;
- владельцев (обладателей, источников) информации - обработчиков и потребителей на основе отношений собственности при обеспечении гарантий интересов граждан и государства.

Этот закон определяет основы защиты информации в системах обработки и при ее использовании с учетом категорий доступа к открытой информации и к информации с ограниченным доступом. Этот закон содержит, кроме того, общие нормы по организации и ведению информационных систем, включая банки данных государственного назначения, порядка государственной регистрации, лицензирования, сертификации, экспертизы, а также общие принципы защиты и гарантий прав участников информационного процесса.

В дополнение к базовому закону в мае 1992 г. были приняты Законы "О правовой охране программ для электронно-вычислительных машин и баз данных" и "О правовой охране топологии интегральных микросхем". Оба закона устанавливают охрану соответствующих объектов с помощью норм авторского права, включая в перечень объектов авторского права наряду с традиционными базами данных топологии интегральных микросхем и программы для ЭВМ.

Вопросы правового режима информации с ограниченным доступом реализуются в двух самостоятельных законах о государственной и коммерческой тайнах. Кроме того, этот аспект раскрывается и в Гражданском кодексе РФ статьей 139 "Служебная и коммерческая тайна".

1. Информация составляет служебную или коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим кодексом и другими законами.

Вторая часть статьи 139 определяет правовые основы ответственности за несанкционированное получение информации или причинение ущерба: "Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору".

Указ Президента РФ от 6 марта 1997 г. № 188 определяет понятие и содержание конфиденциальной информации (см. таблицу).

Таким образом, правовая защита информации обеспечивается нормативно-законодательными актами, представляющими собой по уровню иерархическую систему от Конституции РФ до функциональных обязанностей и контракта отдельного конкретного исполнителя, определяющих перечень сведений, подлежащих охране, и меры ответственности за их разглашение.

Таблица

2.3.2. Органы обеспечения информационной безопасности

Для поддержания информационной безопасности на надлежащем уровне как в государственной, так и (с недавних пор) в коммерческой сферах необходима четкая система контроля. Причем, эта система контроля должна опираться на действующие силовые структуры, наделенные определенными правами в рамках действующего законодательства. Отметим следующие структуры, действующие в настоящее время.

Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России). Решения Гостехкомиссии России являются обязательными для исполнения всеми органами государственного управления, предприятиями, организациями и учреждениями независимо от их организационно-правовой формы и формы собственности, которые по роду своей деятельности обладают информацией, составляющей государственную или служебную тайну.

ФАПСИ – Федеральное агентство правительственной связи и информации. Является правопреемником трех технических управлений КГБ СССР.

Федеральная служба безопасности.

Служба внешней разведки.

Министерство обороны РФ.

Межведомственная комиссия по защите государственной тайны.

Контролирующие органы могут привлечь к ответственности за нарушения норм законодательства в области информационной безопасности по следующим статьям УК РФ – ст. ст. 137, 138, 139, 183, 272, 273, 274. Кроме того, вступивший в силу с 1 июля 2002 г. административный кодекс содержит статьи, в соответствии с которыми нарушители лицензионных и сертификационных норм в области информационной безопасности привлекаются к ответственности.

2.3.3. Лицензирование деятельности в области информационной безопасности

Лицензирование деятельности в области информационной безопасности регламентируется Законом РФ "О лицензировании отдельных видов деятельности" от 13.07.2001 г., а также Постановлениями Правительства РФ "О лицензировании отдельных видов деятельности" № 1418 от 24.12.98 г., "О лицензировании деятельности по технической защите конфиденциальной информации" № 290 от 30.04.2002 г., "Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации" № 348 от 27.05.2002 г. В этих документах определено, какие государственные

структуры и по каким направлением осуществляют лицензирование. Другими словами, определены следующие органы, уполномоченные на ведение лицензионной деятельности.

ФСБ РФ (на территории РФ) **и СВР** (за рубежом) – по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Гостехкомиссия, ФАПСИ, СВР, МО – на право проведения работ, связанных с созданием средств защиты информации (в пределах их компетенции).

ФСБ РФ, ФАПСИ, СВР, Гостехкомиссия – на право осуществления мероприятий и (или) оказания услуг в области государственной тайны.

Виды деятельности, лицензируемые **Гостехкомиссией**:

1. Сертификация и сертификационные испытания защищенных технических средств обработки информации.
2. Аттестование систем информатизации, систем связи и др., а также помещений, предназначенных для ведения переговоров, содержащих охраняемые сведения.
3. Разработка, изготовление, монтаж, наладка, установка, реализация, ремонт, сервисное обслуживание защищенных технических средств обработки информации.
4. Проведение специальных исследований на побочное электромагнитное излучение и наводки технических средств обработки информации.
5. Проектирование объектов в защищенном исполнении.
6. Виды деятельности, лицензируемые **ФАПСИ:**
7. Разработка, производство, проведение сертификационных испытаний, реализация шифровальных средств, а также предоставление услуг по шифрованию информации.
8. Эксплуатация негосударственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.
9. Разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка и ремонт систем телекоммуникаций высших органов государственной власти РФ.
10. Разработка, изготовление, монтаж, наладка, установка, реализация, ремонт, сервисное обслуживание специализированных защищенных технических средств обработки информации, предназначенных для использования в высших органах государственной власти РФ.
11. Проведение работ по выявлению электронных устройств перехвата информации в помещениях и технических средствах государственных структур на территории РФ.
12. Проведение специальных исследований на побочное электромагнитное излучение и наводки технических средств обработки информации, предназначенных для использования в высших органах государственной власти РФ.
13. Проектирование объектов в защищенном исполнении для использования в высших органах государственной власти РФ.

Кроме того, что для ведения деятельности в области защиты информации организация обязана иметь соответствующую лицензию, исполнители работ обязаны пользоваться только сертифицированными техническими средствами. Сертификация – это деятельность по подтверждению соответствия продукции установленным требованиям. Постановлением Правительства РФ от 26.06.1995 г. № 608 «О сертификации средств защиты информации» определены системы сертификации, которые создаются **Гостехкомиссией, ФАПСИ, ФСБ, СВР и МО РФ.**

2.4. Технические каналы утечки информации

2.4.1. Общая характеристика технического канала утечки информации

Технический канал утечки информации (ТКУИ) есть способ получения разведывательной информации об объекте с помощью технического средства разведки (ТСР). Иными словами, ТКУИ – совокупность объекта разведки, технического средства, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т.д. – любые виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

В зависимости от своей природы сигналы распространяются в определенных физических средах – газовых (воздушных), жидкостных (водных) и твердых.

Технические средства разведки служат для приема и измерения параметров сигналов.

Информация, получаемая об объекте разведки, может быть различна по своей природе (источнику). В зависимости от источника будем различать:

- информацию, обрабатываемую техническими средствами;
- информацию, передаваемую по каналам связи;
- акустическую (речевую) информацию;
- видовую информацию.

Под *видовой информацией* понимается информация о внешнем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений. Способами получения такой информации являются наблюдение, съемка и снятие копий документов. Защита видовой информации заключается уже не в закрытии технических каналов ее утечки, а в противодействии способам скрытого видеонаблюдения и съемки. Поэтому в дальнейшем будут рассматриваться каналы утечки информации первых трех видов.

2.4.2. Классификация технических каналов утечки информации, обрабатываемой техническими средствами передачи информации

Под *техническими средствами приема, обработки, хранения и передачи информации (ТСПИ)* понимают технические средства, непосредственно обрабатывающие информацию ограниченного доступа. К ним относятся вычислительная техника, режимные АТС, системы громкоговорящей и оперативной связи, звукозаписи, звукоусиления и т.д. ТСПИ в совокупности с помещением, в котором они размещены, составляют объект ТСПИ.

Наряду с ТСПИ в помещениях могут быть установлены технические средства и системы, непосредственно не участвующие в обработке информации ограниченного доступа, но находящиеся в зоне электромагнитных полей, создаваемых ТСПИ. Такие технические средства и системы называются *вспомогательными техническими средствами и системами (ВТСС)*. К ним относятся средства открытой связи (телефонной, громкоговорящей и т.д.), системы пожарной и охранной сигнализации, электроснабжения, радиотрансляции, часофикации, бытовые электрические приборы и т.д. В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы *контролируемой зоны (КЗ)*, т.е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, не относящиеся к ним, но проходящие через объекты ТСПИ, а также металлические трубы систем коммунального хозяйства и другие токопроводящие конструкции. Такие элементы называются посторонними проводниками.

В зависимости от физической природы возникновения информационных сигналов, среды их распространения и способов перехвата технические каналы утечки информации, обрабатываемой ТСПИ, подразделяются на электромагнитные, электрические и параметрический (табл. 4.1).

Таблица 4.1

Технические каналы утечки информации, обрабатываемой ТСПИ

Виды ТКУИ	Способы перехвата информации
Электромагнитные	Перехват ПЭМИ элементов ТСПИ
	Перехват ЭМИ на частотах работы ВЧ генераторов в ТСПИ и ВТСС
	Перехват ЭМИ на частотах самовозбуждения УНЧ ТСПИ и ВТСС
Электрические	Съем наводок ЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников
	Съем информационных сигналов с линий питания ТСПИ
	Съем информационных сигналов с цепей заземления ТСПИ и ВТСС
	Съем информации путем установки в ТСПИ аппаратных закладок
Параметрический	Перехват информации путем «высокочастотного облучения» ТСПИ

К **электромагнитным** относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ПЭМИ) ТСПИ.

ПЭМИ ТСПИ. В ТСПИ носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются в соответствии с изменениями информационного сигнала. При прохождении электрического тока по токоведущим элементам ТСПИ между различными точками его схемы образуются разности потенциалов, которые порождают магнитные и электрические поля, называемые ***побочными электромагнитными излучениями (ПЭМИ)***. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

ЭМИ на частотах работы высокочастотных генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы (задающие, тактовые, стирания и подмагничивания аппаратуры магнитной записи, гетеродины радиоприемных устройств и т.д.). В результате внешних воздействий информационного сигнала на элементах высокочастотных генераторов наводятся электрические сигналы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов. Эти промодулированные высокочастотные колебания излучаются в окружающее пространство.

ЭМИ на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Сигнал на частотах самовозбуждения может быть промодулирован информационным сигналом. Строго говоря, режим самовозбуждения является признаком неисправности (отказа) технического средства, поэтому возникновение ТКУИ за счет ЭМИ на частотах самовозбуждения возможно лишь при ненадлежащем исполнении техническим персоналом, обслуживающим ТСПИ, своих функциональных обязанностей (несвоевременное выявление неисправностей (отказов) и непринятие мер по их устранению).

Перехват ПЭМИ ТСПИ осуществляется средствами радиоразведки, размещенными вне контролируемой зоны. Зона, в которой возможен перехват ПЭМИ и последующая регистрация содержащейся в них информации с помощью средств радиоразведки (т.е. зона, в пределах которой отношение «информационный сигнал/помеха» превышает нормированное значение), называется зоной 2.

Причинами возникновения **электрических** каналов утечки информации могут быть:

- наводки ЭМИ ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивание информационных сигналов в цепи электропитания ТСПИ;
- просачивание информационных сигналов в цепи заземления ТСПИ.

Наводки ЭМИ ТСПИ возникают при излучении элементами ТСПИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСПИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов зависит от мощности излучаемых

сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСПИ и посторонних проводников.

Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется зоной 1.

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать ПЭМИ. Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство, например телефонный аппарат, приемник радиотрансляционной сети, датчик системы охранной или пожарной сигнализации. Распределенные случайные антенны – конструкции и коммуникационные линии, обладающие распределенными параметрами (кабели, провода, металлические трубы и другие токопроводящие коммуникации).

Просачивание информационных сигналов в цепи электропитания возможно при наличии магнитной связи между элементами обрабатывающих информацию узлов ТСПИ и элементами узлов вторичного электропитания (например, между выходным трансформатором УНЧ и трансформатором выпрямителя, формирующего напряжение питания УНЧ). Кроме того, информационный сигнал может проникнуть в цепи первичного электропитания в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения ТСПИ с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. Эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Съем информации с использованием аппаратных закладок. Электронные устройства перехвата информации, устанавливаемые в ТСПИ, называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в ТСПИ иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью аппаратных закладок информация или передается по радиоканалу в режиме реального времени, или записывается на запоминающее устройство, а уж затем по команде передается на запросивший ее объект.

Перехват информации по первым трем из электрических каналов возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через объекты ТСПИ, а также к их системам электропитания и заземления. Для этих целей используются средства радиоразведки и специальная измерительная аппаратура.

Перехват информации, обрабатываемой ТСПИ, возможен в результате их «высокочастотного облучения». При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит его переизлучение. Зачастую вторичное излучение оказывается промодулированным информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и переизлучающего сигналов используется их временн***а***я или частотная развязка.

При переизлучении параметры сигналов изменяются – поэтому данный ТКУИ называют **параметрическим.**

Для перехвата информации по параметрическому каналу используют специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства.

2.4.3. Классификация технических каналов утечки речевой информации

Информация, носителем которой является акустический сигнал, называется **акустической.** Если источник акустической информации – человеческая речь, то такая информация называется **речевой**.

Акустический сигнал – возмущения упругой среды различной формы и длительности (акустические колебания), распространяющиеся от источника в окружающее пространство.

Различают первичные и вторичные источники акустических колебаний. К первичным относятся непосредственные источники (например, органы речи человека), а к вторичным – различного рода преобразователи (пьезоэлементы, микрофоны, громкоговорители и т.п.).

В зависимости от формы колебаний различают простые (тональные) и сложные сигналы. *Тональный* – сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. *Сложный сигнал* содержит спектр гармонических составляющих. Речевой сигнал является сложным акустическим сигналом, составляющие которого лежат обычно в диапазоне 200 Гц – 6 кГц.

В таблице 4.2 приведена классификация технических каналов утечки акустической (речевой) информации в зависимости от природы возникновения, среды распространения и способов перехвата акустических сигналов.

В **воздушных** ТКУИ средой распространения акустических сигналов является воздух, и для их перехвата используются микрофоны – миниатюрные высокочувствительные или специальные узконаправленные. Микрофоны могут объединяться (соединяться) с устройствами записи речи (магнитофонами, диктофонами) или специальными миниатюрными передатчиками. Подобные комплексированные устройства называют закладными устройствами перехвата речевой информации, или акустическими закладками.

Перехваченная закладными устройствами речевая информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по сети электропитания, соединительным линиям ВТСС, посторонним проводникам.

Прием информации, передаваемой закладными устройствами, осуществляется специальными приемными устройствами соответствующего диапазона. Однако встречаются закладные устройства, прием информации с которых можно осуществлять с обычного телефонного аппарата. Подобное устройство конструктивно объединяет миниатюрный микрофон и специальный блок коммутации («телефонное ухо»). Блок коммутации подключает микрофон к телефонной линии («телефону – наблюдателю», установленному в контролируемом помещении) при дозвоне по определенной схеме или при подаче в линию специального сигнала.

Таблица 4.2

Технические каналы утечки акустической (речевой) информации

Виды ТКУИ	Способы перехвата информации
Воздушные	Перехват средствами записи
	Перехват направленными микрофонами
	Перехват радиомикрофонами
	Перехват с передачей по электрической сети
	Перехват с передачей в ИК-диапазоне
	Перехват с передачей по телефонной линии
	Перехват с передачей от «телефона-наблюдателя» на внешний телефон по сигналам вызова последнего
	Перехват с передачей по строительным конструкциям
Вибрационные	Перехват стетоскопами
	Перехват радиостетоскопами
	Перехват стетоскопами с передачей в ИК-диапазоне
	Перехват стетоскопами с передачей по строительным конструкциям
Электроакустические	Перехват через ВТСС, обладающие «микрофонным эффектом», с подключением к ним
	Перехват через ВТСС путем ВЧ-навязывания
Оптико-электронный (лазерный)	Перехват путем лазерного зондирования оконных стекол
Параметрические	Перехват путем приема ПЭМИ ВТСС (на частотах ВЧ-генераторов, модулированных акустическим сигналом)
	Перехват путем ВЧ-облучения специальных полуактивных закладных устройств

Микрофоны, объединенные с аппаратурой записи речи (диктофоны) позволяют получать информацию не в реальном масштабе времени, а с задержкой, поскольку для ее получения необходимо периодически заменять либо саму закладку, либо носитель, на который записывается речевой сигнал.

Использование закладных устройств требует проникновения на контролируемый объект. В том случае, когда это невозможно, могут быть использованы направленные микрофоны.

В вибрационных (структурных) ТКУИ средой распространения акустических сигналов являются конструкции зданий (стены, потолки, полы), трубы водоснабжения, канализации, отопления и другие твердые тела. Для перехвата акустических колебаний в этом случае используются электронные стетоскопы (контактные микрофоны).

Стетоскопы, как и микрофоны, обычно комплексируются с передатчиками информации различных диапазонов электромагнитных волн (чаще всего – радиоволн; в этом случае закладное устройство называют радиостетоскопом). Для перехвата информации используются специальные приемники, аналогичные тем, которые используются и для организации воздушных ТКУИ.

Электроакустические технические каналы утечки акустической (речевой) информации возникают за счет электроакустических преобразований акустических сигналов в электрические. Перехват речевой информации по электроакустическому каналу возможен через ВТСС, обладающие микрофонным эффектом, а также путем высокочастотного навязывания.

Некоторые элементы ВТСС (трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонковых устройств ТА, дроссели ламп дневного света и т.п.) обладают свойством изменять свои параметры под действием акустического поля. Изменение этих параметров приводит к тому, что в цепях этих элементов либо возникает ЭДС, значение которой зависит от изменяющейся величины звукового давления, либо происходит модуляция токов, протекающих в них. Эффект преобразования акустических колебаний в электроакустические называют микрофонным эффектом. Наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной и охранной сигнализации. Перехват акустических колебаний в данном канале осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей.

Канал утечки за счет высокочастотного навязывания образуется путем несанкционированного контактного введения токов ВЧ в цепи ВТСС, обладающие микрофонным эффектом, с целью повышения качества перехватываемого сигнала, а также для обеспечения бесконтактного перехвата излучаемого ВТСС модулированного ВЧ-сигнала (при помощи высокочувствительных приемников). Наиболее часто такой метод используют на телефонных линиях, имеющих выход за пределы контролируемой зоны.

Оптико-электронный (лазерный) канал утечки речевой информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (оконных стекол, зеркал, картинных стекол). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе в соответствии с колебаниями отражающей поверхности и принимается приемником оптического (лазерного) излучения. Лазер и лазерный приемник могут устанавливаться в одном или разных местах (помещениях).

Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, называемые «лазерными микрофонами».

Параметрические технические каналы утечки речевой информации – каналы, образуемые за счет высокочастотного облучения элементов ТСПИ и ВТСС или пассивных закладных устройств. Природа образования – такая же, как и в каналах высокочастотного навязывания.

2.4.4. Классификация технических каналов перехвата информации при ее передаче по каналам связи

Информация после обработки в ТСПИ может передаваться по каналам связи, где также возможен ее перехват.

В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. В зависимости от вида каналов связи технические каналы перехвата

информации можно разделить на **электромагнитные, электрические и индукционные** (табл. 4.3).

Таблица 4.3
Технические каналы перехвата информации, передаваемой по каналам связи

Виды каналов связи	Каналы перехвата	Способ перехвата
Каналы радио-, радиорелейной, тропосферной связи	**Электромагнитный**	Перехват ЭМИ на частотах работы передатчиков систем и средств связи
Кабельные линии связи	**Электрический**	Съем информации путем контактного подключения к линии
	Индукционный	Бесконтактный съем информации

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки.

Электромагнитный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ — это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения.

Поэтому средства разведки к линии связи подключаются или через согласующее устройство, несколько снижающее падение напряжения, или через специальные устройства компенсации падения напряжения. В последнем случае аппаратура разведки и устройство компенсации падения напряжения включаются в линию связи последовательно, что существенно затрудняет обнаружение факта несанкционированного подключения к ней.

Контактный способ используется в основном для снятия информации с коаксиальных и низкочастотных кабелей связи. Для кабелей, внутри которых поддерживается повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют **телефонными закладками**.

В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют **индуктивный** канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

Некоторые средства бесконтактного съема информации, передаваемой по каналам связи, могут комплексироваться с радиопередатчиками для ретрансляции в центр ее обработки.

2.5. Выявление (поиск) технических каналов утечки информации

2.5.1. Общие принципы и методы выявления технических каналов утечки информации

Выявление технических каналов утечки информации в общем случае осуществляется методами физического поиска и инструментального (технического) контроля. Инструментальный контроль проводится по отдельным физическим полям и включает в себя:

- подготовку исходных данных для контроля (ознакомление с объектом защиты; оценка его особенностей; уточнение видов и средств технической разведки, от которых осуществляется защита; подготовка и проверка контрольно-измерительной аппаратуры);
- определение допустимых нормируемых показателей в зависимости от вида технической разведки, от которого осуществляется защита;
- измерение (регистрация) нормируемых физических параметров по контролируемому физическому полю (специальные исследования);
- сравнение полученных данных специальных исследований с нормативными требованиями;
- поиск (специальная проверка) электронных средств перехвата информации (закладных и заносных устройств).

Общие методы выявления технических каналов утечки информации приведены в табл. 5.1. Способы ведения поиска по каждому методу могут быть самыми различными – в зависимости от глубины поиска, имеющихся поисковых технических средств, модели нарушителя и т.п.

Таблица 5.1.
Методы выявления технических каналов утечки информации

Вид информации	ТКУИ	Метод
Информация, обрабатываемая ТСПИ	Электромагнитные	Специальные исследования (СИ) ТСПИ на ПЭМИ в лабораторных условиях и на объекте; СИ ВТСС на объекте (I)
	Электрические	СИ на наводки от ТСПИ на случайные антенны (I)
		СИ на просачивание информационного сигнала в цепи питания и заземления ТСПИ (I)
		Специальная проверка (СП) ТСПИ и ВТСС, размещенных на объекте на отсутствие аппаратных закладок (II)
	Параметрический	Поиск источника узконаправленного ВЧ излучения на объекте (I)
Акустическая (речевая) информация	Воздушные, вибрационные	Поиск электронных средств перехвата информации (закладных устройств) на объекте (III)
		Проверка телеф. линий, соединительных линий ВТСС, линий питания аппаратуры на наличие ВЧ сигналов (I)
	Электроакустические	Проверка линий ВТСС на наличие микрофонного эффекта (III)
		Проверка линий ВТСС на наличие ВЧ сигналов (I)
	Параметрические	СИ ВТСС на объекте (I)
		Поиск источника узконаправленного ВЧ излучения на объекте (I)
Информация, передаваемая по кабельным линиям связи	Электрический	Специал. проверка линии связи (IV)

2.5.2. Классификация технических средств выявления каналов утечки информации

В соответствии с таблицей 5.1 технические средства выявления каналов утечки информации можно условно разделить на четыре группы:

- I – селективные микровольтметры, измерительные приемники, анализаторы спектра и специальные измерительные комплексы для проведения измерений уровней ЭМИ;
- II – специальные комплексы фотографирования в рентгеновских лучах для поиска аппаратных закладок, рентгеновские телевизионные комплексы;
- III – специальные технические средства поиска электронных закладных устройств (индикаторы поля, измерители частоты, интерсепторы, радиоприемные устройства, многофункциональные поисковые приборы, нелинейные локаторы, обнаружители диктофонов, аппаратно-программные комплексы радиомониторинга);
- IV – специальная аппаратура контроля проводных коммуникаций.

При осуществлении физического поиска также могут быть использованы технические средства – различного рода досмотровое оборудование, металлоискатели и т.п.

Технические средства I группы в основном представлены измерительными приборами, параметры которых (прежде всего частотный и динамический диапазоны) позволяют проводить измерения уровней ЭМИ в соответствии с утвержденными методиками. Подробно принципы работы, назначение и характеристики этих технических средств рассматриваются в рамках курсов «Радиоизмерения», «Радиоизмерительная техника». Следует только отметить, что в последнее время на рынке стали появляться специализированные комплексы, разработанные специально для решения задач поиска каналов утечки информации за счет ПЭМИН – «Навигатор», «Зарница», «Легенда», «Сигурд». Они позволяют производить автоматическое опознавание информационных сигналов, измерение их уровней, а также измерение наводок в сети питания, линиях и коммуникациях.

Технические средства II группы предназначены для поиска аппаратных закладок. Согласно действующим нормативно-методическим документам поиск аппаратных закладок производится при помощи фотографирования узлов, блоков, плат или всего аппарата в целом в рентгеновских лучах и последующего сравнения полученного изображения с эталонным. Визуальный осмотр проверяемого аппарата не позволяет сделать однозначное заключение о наличии или отсутствии в нем аппаратной закладки, поскольку последняя может быть внедрена на уровне кристаллов полупроводниковых элементов. Очевидно, что эффективность поиска будет зависеть в основном от полноты базы эталонных изображений.

Более подробно ниже будут рассмотрены специальные технические средства III и IV групп, предназначенные для поиска акустических и телефонных закладок.

2.5.3. Индикаторы поля, интерсепторы и измерители частоты

Индикаторы электромагнитного поля (индикаторы поля) предназначены для обнаружения активных (излучающих) во время проведения поиска акустических закладок. Позволяют обнаруживать закладки, использующие для передачи информации практически все виды сигналов, включая широкополосные шумоподобные и сигналы с псевдослучайной скачкообразной перестройкой несущей частоты. Характеристики некоторых индикаторов поля, отечественного и импортного производства, представлены в таблице 5.2.

Таблица 5.2
Характеристики индикаторов поля

Индекс (тип) прибора	Страна	Диапазон частот, МГц	Детектор	Чувствит., мВ	Динамический диапазон, дБ	Индикация	Питание
D 006	Россия	50-1000	AM	1,5…3	40	Св, З(о)	DC 9
ДИ-04		20-1000	AM			Св, З(о)	DC 9
ИП-3		50-1200	AM	1…3	55	Св, З	DC 7…9
РИЧ-2		50-1300	AM	1…3	40	ЖКИ	DC 7…9
ИПФ-Ч		30-1500	AM	0,5…1,5		Ст, З	DC 9
РТ 022		30-1500	AM	0,5…1,5		Ст, З	DC 9
ИПАР-01		50-1200	AM		26	Св, З	DC 9
D 008		50-1500	AM, FM	0,5…6	20	Св, З(о)	DC 9
СРМ-700	США	0,05-3000	AM, FM	-62 дБ		ЖКИ, З	DC 12
VL5000-P		2-1500	AM, FM	10 мкВ		ЖКИ, З	DC 2×9
Delta V/2	Англия	20-4200	AM, FM	-53 дБ	50	З	DC 5,8
HGS 4120	Германия	10-2000	AM, FM			Ст, З	DC 9
PROTECT-1203		10-3600	AM, FM			Св, З	DC 3,6
КОМАР	Россия	80-3000	AM, FM			Св	DC 12
ЛУЧ		40-2000	AM, FM			Св, З	220

Обозначения в столбце **«Индикация»:**

- **Св** – светодиодная;
- **Ст** – стрелочный индикатор;
- **З** – звуковая;
- **З(о)** – звуковая отключаемая;
- **ЖКИ** – отображение уровня на жидкокристаллическом индикаторе.

Принцип действия приборов основан на интегральном методе измерения уровня электромагнитного поля в точке их размещения и на этой основе – в определении точки абсолютного максимума уровня излучения в помещении. Наведенный в антенне и продетектированный сигнал усиливается, и в случае превышения им установленного порога срабатывает звуковая или световая сигнализация. Фактически индикаторы поля – это приемники с очень низкой чувствительностью, поэтому они обнаруживают излучения радиозакладок на предельно малых расстояниях (10 – 40 сантиметров), чем и обеспечивается селекция «нелегальных» излучений на фоне мощных «разрешенных» сигналов.

Некоторые индикаторы поля дополняются специальным блоком, включающим амплитудный детектор, усилитель низкой частоты и динамик. Этот блок позволяет не только прослушивать обнаруженные сигналы, но и реализует эффект акустической завязки (аналогичный режиму самовозбуждения, возникающему, например, в системах звукоусиления за счет положительной обратной связи, когда микрофон расположен вблизи от звуковых колонок). Если в динамике появляется характерный свист (за счет акустической завязки), оператор делает вывод, что объект поиска находится в непосредственной близости от антенны индикатора. Необходимо отметить, что у профессиональных радиозакладок с частотной модуляцией сигнала практически отсутствует паразитная амплитудная модуляция, и потому эффект акустической завязки не наблюдается.

В результате дальнейшего развития индикаторов поля созданы широкополосные радиоприемные устройства – ***интерсепторы***. Эти приборы автоматически настраиваются на частоту наиболее мощного радиосигнала и осуществляют его детектирование. Характеристики некоторых из них приведены в таблице 5.3.

Принцип захвата частоты радиосигнала с максимальным уровнем и последующим анализом его характеристик микропроцессором положен в основу работы **измерителей частоты (радиочастотомеров)**. Микропроцессор производит запись сигнала во внутреннюю память, цифровую фильтрацию, проверку на стабильность и когерентность сигнала, и измерение его

частоты с точностью от единиц Гц до 10 кГц. Значение частоты в цифровой форме отображается на жидкокристаллическом дисплее. Некоторые радиочастотомеры кроме частоты сигнала позволяют определить его относительный уровень. Характеристики измерителей частоты приведены в таблице 5.4.

Наиболее совершенным из всего вышеописанного семейства (индикаторы поля, интерсепторы, радиочастотомеры) является специальный приемник “Xplorer”. Он позволяет производить автоматический или ручной захват радиосигнала в диапазоне частот от 30 до 2000 МГц и осуществлять его детектирование и прослушивание через динамик. Дисплей показывает частоту обнаруженного сигнала, его относительный уровень и вид модуляции, а также широту и долготу места расположения прибора в системе GPS. Приемник имеет функции блокировки (пропуска) до 1000 частот и записи в память до 500 частот с дополнительной информацией о дате и времени записи.

Некоторые отечественные поисковые приборы, также как и частотомеры, позволяют определять частоту принимаемого сигнала (ИПФ-Ч, РИЧ-2). Точность измерения частоты сигнала составляет ± 2 кГц.

Таблица 5.3

Характеристики интерсепторов

Характеристика	Тип		
	OE R11	OE R20	“Xplorer”
Диапазон частот, МГц	3 … 2000	5 … 2500	30 … 2000
Чувствительность	100 мкВ	-20 дБ	100 мкВ
Тип детектора	FM	AM	FM
Девиация частоты сигнала	<100 кГц		< 100 кГц
Индикатор уровня сигнала		10 сегментов	50 сегментов
Время автонастройки, с	1	0,5	1
Питание, В	DC 7,2	DC 9	DC 7,2
Время работы, ч	5	3	5
Размеры, мм	108 x 63 x 32	107 x 71 x 23	140 x 76 x 41
Примечание	Индикация частоты по десяти поддиапазонам. Память Lockout на 1000 частот (частоты, исключаемые из просмотра)	Выход для подключения головных телефонов	Индикация частоты сигнала на 16 разрядном LCD дисплее. Запись в память до 500 частот с информацией о дате, времени записи, координат места записи. Порт подключения к ПЭВМ

Таблица 5.4
Характеристики радиочастотомеров

Характеристика	Тип		
	“Scout”	M-1	3000A+
Диапазон частот	10… 1400 МГц	20 Гц – 2,8 ГГц	20 Гц – 3 ГГц
Чувствительность	5 мВ	1 … 100 мВ (в зависимости от диапазона)	0,6 … 5 мВ (в зависимости от диапазона)
Период измерений	10 мс	10мкс … 10 с	200 нс
Тип дисплея	10 разрядный LCD		
Индикатор уровня сигнала	16 сегментный индикатор		
Питание, В	DC 6 (4 x AA) DC6;12(внешнее)	DC9 (аккумулятор)	DC9 (6 x AA) DC9 (внешнее)
Время работы, ч	8	5	6
Размеры, мм	94 x70 x30	120 x70 x34	135 x99 x36
Примечание	Цифровая фильтрация и автозахват сигнала. Запись в память до 400 частот. Интерфейс OptoScan для управления приемниками R7000, R7100, AR8000	Цифровая фильтрация сигнала, запись частот в память. Запись в ПЭВМ через интерфейс RS-232 частоты и времени записи (программа Optolog)	Два входа для подключения антенн. Цифровая фильтрация сигнала, запись частот в память. Запись в ПЭВМ через интерфейс RS-232 частоты и времени записи (программа Optolog)

2.5.4. Специальные сканирующие радиоприемники

Современные портативные сканирующие приемники широко используются для решения задач радиоразведки и радиоконтроля, а также поиска несанкционированных средств перехвата информации, использующих для передачи информации радиоканал (радиозакладок – акустических и телефонных).

Сканирующие приемники можно разделить на две группы: переносимые сканирующие приемники и перевозимые портативные сканирующие приемники. К переносимым относятся малогабаритные сканирующие приемники весом 150...350 г. (IC-R1, IC-R10, DJ-X1 D, AR-1500, AR-2700, AR-8000, MVT-700, MVT-7100, MVT-7200, PR-1300A, HSC-050 и т.д.). Они имеют автономные аккумуляторные источники питания и свободно умещаются во внутреннем кармане пиджака.

Несмотря на малые размеры и вес, подобные приемники позволяют вести разведку и контроль в диапазоне частот от 100...500 кГц до 1300 МГц, а некоторые типы приемников — до 1900 МГц (“AR-8000”) и даже — до 2060 МГц (“HSC-050”).

Они обеспечивают прием с амплитудной (AM), узкополосной (NFM) и широкополосной (WFM) частотной модуляцией. Приемники “AR-8000” и “HSC-050” кроме указанных типов принимают сигналы с амплитудной однополосной модуляцией (SSB) в режиме приема верхней боковой полосы (USB) и нижней боковой полосы (LSB), а также телеграфных сигналов (CW). При этом чувствительность приемников при отношении сигнал/шум, равном 10 дБ (относительно 1 мкВ), составляет: при приеме сигналов с NFM модуляцией — 0,35...1 мкВ, с WFM модуляцией — 1...6 мкВ. Избирательность на уровне минус 6 дБ составляет 12...15 и 150...180 кГц соответственно.

Портативные сканирующие приемники имеют от 100 до 1000 каналов памяти и обеспечивают скорость сканирования от 20 до 30 каналов за секунду при шаге перестройки от 50...500 Гц до 50...1000 кГц. Некоторые типы приемников, например, AR-2700, AR-8000, IC-R10 могут управляться компьютером.

Перевозимые сканирующие приемники (IC-R100, AR-3030, AR-3000A, AR-5000, IC-R72, IC-R7100, IC-R8500, IC-R9000, AX-700B, EB-100 и др.) отличаются от переносимых несколько

б*о*льшим весом (от 1,2 до 6,8 кг), габаритами и, конечно, б*о*льшими возможностями. Они, как правило, устанавливаются или в помещениях, или в автомашинах.

Почти все перевозимые сканирующие приемники имеют возможность управления с ПЭВМ.

Сканирующие приемники (как переносимые, так и перевозимые) могут работать в одном из следующих режимов:

- режим автоматического сканирования в заданном диапазоне частот;
- режим автоматического сканирования по фиксированным частотам;
- ручной режим работы.

Первый режим работы приемника является основным при выявлении частот работающих радиоэлектронных средств (при решении задач радиоразведки и радиоконтроля), а также при поиске излучений радиозакладок. При этом режиме устанавливаются начальная и конечная частоты сканирования, шаг перестройки по частоте и вид модуляции.

Как правило, имеются несколько программируемых частотных диапазонов, в которых осуществляется сканирование. Например, для AR-3000A их четыре, для IC-R1 — десять, а для AR-8000 — двадцать. Оперативное переключение между заданными частотными диапазонами осуществляется с помощью функциональных клавиш.

В данном режиме работы возможно осуществление сканирования диапазона с пропуском частот, хранящихся в специально выделенных для этой цели каналах памяти. Такие каналы часто называют маскированными. Функция пропуска частот включается при установке режима сканирования и используется для сокращения времени сканирования диапазона. В этом случае в блок памяти, как правило, записываются частоты постоянно работающих в данном районе радиостанций, которые с точки зрения разведки или контроля не представляют интереса (например, частоты, выделенные для телевизионных и радиовещательных станций).

Рис. 5.1. Стационарный сканирующий приемник

Можно использовать несколько режимов сканирования:

1. При обнаружении сигнала (превышении его уровня установленного порога) сканирование прекращается и возобновляется при нажатии оператором функциональной клавиши.
2. При обнаружении сигнала сканирование останавливается и возобновляется после пропадания сигнала.
3. При обнаружении аудиосигнала сканирование останавливается и возобновляется после пропадания сигнала.
4. При обнаружении сигнала сканирование останавливается для предварительного анализа сигнала оператором и возобновляется по истечении нескольких секунд. Например, для приемника AX-700E — через 5 с, а для приемника AR-3000A это время может изменяться в интервале от 0 до 9 с.

У некоторых приемников при проведении сканирования предусмотрена возможность автоматической записи в память частот обнаруженных сигналов. При этом запись в выделенные для этих целей каналы памяти осуществляется последовательно в порядке приема сигналов.

Например, у приемника AR-8000 для записи сигналов, обнаруженных в процессе сканирования, выделено 50 каналов в банке “j”.

Слуховой контроль обнаруженных сигналов может осуществляться оператором через головные телефоны или встроенный громкоговоритель. Выбором нужного вида детектора (NFM, WFM и т.д.) обеспечивается оптимальная демодуляция принимаемых сигналов.

Второй режим работы приемников используется при ведении радиоразведки и радиоконтроля, если известны и записаны в каналы памяти возможные частоты работы радиосредств.

Для каждого канала памяти вводится значение частоты, вид модуляции и ослабление входного аттенюатора (последнее - для некоторых видов приемников).

Информация, хранящаяся в каждой ячейке (канале) памяти, может легко вызываться на жидкокристаллический дисплей с помощью функциональных клавиш.

Сканирование каналов памяти осуществляется последовательно, при этом так же, как и при первом режиме работы, предусмотрены возможность сканирования с пропуском частот, записанных в маскированные каналы, и возможность автоматической записи в память частот обнаруженных сигналов.

У некоторых приемников предусмотрен режим сканирования памяти по заданному виду модуляции. При этом сканируются все каналы памяти, запрограммированные для выбранного вида модуляции. Например, если в канале памяти установлен вид модуляции АМ, а сканирование осуществляется по виду модуляции ЧМ (FM), то данный канал при сканировании пропускается.

Как правило, нулевые каналы каждого блока памяти являются приоритетными, что позволяет осуществлять приоритетный просмотр.

Третий режим работы приемников применяется для детального обследования всего или ряда частотных диапазонов и отличается от первого режима тем, что перестройка приемников осуществляется оператором с помощью ручки изменения частоты, при этом информация о частоте настройки, виде модуляции, уровне входного сигнала и т.п. выводится на жидкокристаллический дисплей.

Перестройка частоты осуществляется с выбранным шагом перестройки. Для более быстрого изменения частоты используется режим поразрядного набора, при котором частота изменяется последовательно по разрядам (например: 100 МГц, 10 МГц, 1 МГц, 100 кГц и т.д.). Данный режим работы позволяет довольно быстро и легко выйти в нужный частотный диапазон.

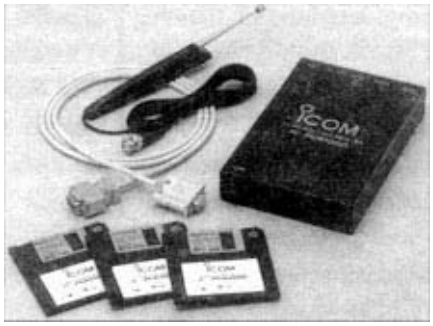


Рис. 5.2. Приемник IC-PCR1000

У ряда сканирующих приемников на дисплее, кроме информации о частоте настройки приемника и виде модуляции, отображается уровень принимаемого сигнала. Например, у приемников AR-3000A уровень входного сигнала отображается в виде 9-ти сегментной диаграммы. При этом используется следующая аппроксимация уровня сигнала: 1 — 1,0 мкВ; 7 — 30,0 мкВ; 9 — 300,0 мкВ.

Анализировать спектр сигналов можно с использованием специальной панорамной приставки SDU-5000.

Сканирующие приемники выпускаются как в обычном исполнении, так и в виде отдельных блоков, подключаемых к ПЭВМ, или в виде печатной платы, вставляемой в ПЭВМ. К таким приемникам относятся сканирующие приемники IC-PCR1000 и Winradio.

Приемник **IC-PCR1000** выполнен в виде отдельного блока и работает под управлением ПЭВМ через встроенный компьютерный интерфейс RS-232C. Сканер имеет шумоподавитель,

функцию автоматической подстройки частоты, функцию автоматической остановки сканирования на модулированных сигналах. В комплект входит управляющее специальное программное обеспечение для Windows.

Основные технические характеристики IC-PCR1000:

- рабочий диапазон частот: 0,01...1300 МГц;
- виды модуляции принимаемых сигналов: USB/LSB/CW и AM/FM/WFM;
- количество каналов памяти: неограниченное, размещается в банках частот на жестком диске ПЭВМ;
- минимальное разрешение по частоте: 1 Гц;
- режим настройки параметров приема при выборе частоты: автоматический.

Блок имеет размеры 127x30 x199 мм и весит 1 кг.

Универсальный сканирующий радиоприёмник **Winradio** выполнен в виде печатной платы ISA IBM (размеры: 294x121x20 мм). Работает под управлением ПЭВМ. Имеет режим автоматического сканирования по частоте в пределах всего диапазона 500 кГц...1300 МГц. Скорость сканирования 50 кан/с. Осуществляет приём в режимах WFM/NFM/ AM/SSB. Чувствительность — 0,5 мкВ. Имеет неограниченное количество каналов памяти, размещаемых в банках частот на жестком диске ПЭВМ. Позволяет отображать на экране дисплея ПЭВМ спектрограммы и осциллограммы принимаемых сигналов, давать данные об уровнях входных сигналов. Шаг перестройки по частоте может быть установлен в пределах от 1 кГц до 1 МГц. Панель управления отображается на экране монитора.

Для поиска радиозакладок наряду с обычными сканирующими приемниками используются и специально разработанные, например, **Scanlock ECM Plus**, **“Скорпион”** или **MRA- 3**.

Переносной комплекс Scanlock ECM Plus представляет собой специальное радиоприемное устройство, предназначенное для выявления, идентификации и определения местоположения закладных устройств, передающих информацию как по радиоканалу (в диапазоне частот от 10 кГц до 4 ГГц), так и по проводным линиям (в диапазоне частот от 8 кГц до 10 МГц), включая электросеть, телефонные кабели, линии селекторной связи, пожарной сигнализации и т.п. В комплект входит специальный интерфейс для подключения прибора к телефонной линии.

При отношении сигнал/шум 10 дБ чувствительность приемника в диапазоне 10 .. 1 100 МГц составляет - 85 дБм, в диапазоне свыше 1 100 МГц — 75 дБм, в диапазоне ниже 10 МГц — 90 дБм.

Главное преимущество Scanlock ECM Plus состоит в возможности быстрой автоматической перестройки в широком диапазоне частот. Сканирование по диапазону производится автоматически или вручную. В режиме автоматического сканирования перестройка может осуществляться с шагом от 1 до 99 кГц. Продолжительность анализа каждой дискретной частоты в автоматическом режиме составляет 0,7 сек. В ручном режиме шаг перестройки может выбираться из значений: 1, 2, 5, 10, 20, 50, 100 и 200 кГц.

Приемник имеет AM и FM детекторы.

Прибор позволяет осуществлять ускоренное автоматическое сканирование наиболее “сильных” сигналов, тем самым значительно сокращая время обнаружения излучений закладок. То есть, при включении режима сканирования приемник захватывает наиболее мощный сигнал и производит его анализ, затем последовательно производится анализ менее “сильных” сигналов.

Измерение частоты можно осуществить простым нажатием кнопки. Оператор идентифицирует обнаруженный сигнал, анализируя его частоту и прослушивая через головные телефоны или встроенный динамик. Идентификация обнаруженного сигнала может осуществляться также методом корреляции принимаемого сигнала с тестовым.

Комплекс питается как от встроенной аккумуляторной батареи, так и от сети 220/240 В. Аккумуляторная батарея обеспечивает 8-часовую работу приемника. Габаритные размеры приемника 310x240x80 мм, вес — 6,3 кг. Приемник с принадлежностями размещается а атташе-кейсе. Общий вес комплекса с кейсом — 15,2 кг.

Портативный комбинированный прибор “Скорпион” сочетает в себе функции обычного сканирующего приемника, радиочастотомера, интерсептора и постановщика помех.

Имея хорошую избирательность и чувствительность (не хуже 20 мкВ) в автоматическом режиме, как любой сканирующий приемник, он может осуществлять просмотр диапазона частот от 30 до 2000 МГц с полосой пропускания 200 кГц. При этом на двухстрочном 16-ти разрядном жидкокристаллическом индикаторе (ЖКИ) отображается информация о частоте, уровне входного

сигнала и других режимах работы прибора. Приемник имеет AM и FM детекторы и позволяет прослушивать принимаемые сигналы через встроенный динамик.

Рис. 5.3. Прибор радиомониторинга "СКОРПИОН"

Ошибка измерения частоты составляет ± 10 кГц. Относительный уровень принимаемого сигнала отображается на 16-ти сегментном индикаторе (ошибка измерения ± 3 дБ на один сегмент). При измерении уровня мощных сигналов может использовать аттенюатор, ослабляющий входной сигнал до 50 дБ.

Встроенный блок памяти позволяет запомнить и пропускать при сканировании (“вырезать”) до 128 частот известных сигналов (частоты радиовещательных и телевизионных станций и т.д.), вводимых оператором.

При регулировке чувствительности приемника с помощью входного аттенюатора и исключения из поиска частот известных сигналов, время сканирования всего диапазона от 30 до 2000 МГц не будет превышать 10 с. В этом случае прибор может использоваться для непрерывного радиоконтроля с постоянным сканированием заданного диапазона частот.

Отличительной особенностью прибора является то, что одновременно с функциями обнаружения сигналов закладных устройств, он также способен осуществлять их подавление постановкой прицельной помехи. Выходная мощность передатчика помех составляет 50 мВт в полосе частот 200 кГц.

Прибор “Скорпион” имеет небольшие размеры (166x90x29 мм без антенны) и вес. Питание прибора осуществляется от 8 батарей типа АА, информация о состоянии которых отражается на ЖКИ.

Разработка прибора «Скорпион» была завершена в 1998 году. Он занял достойное место среди портативных поисковых технических средств. Высокая оценка, данная специалистами прибору, подтвердила актуальность его создания. Анализ работы “Скорпиона” и требований потребителей, предъявляемых к работе такого рода устройств, послужил толчком к логическому развитию концепции и появлению приемника **“Скорпион 2”.**

“Скорпион 2” имеет более высокую чувствительность по всему диапазону частот. Улучшение схемотехнического решения привело к повышению надежности и качества работы прибора, что позволяет ему сохранять работоспособность в условиях сильных электромагнитных полей.

Прибор выполняет следующие основные функции:

- быстрого сканирования во всем диапазоне.
- радиотестера на частоте, установленной оператором; этот режим предназначен для проверки работоспособности радиоприемников, измерителей частоты и индикаторов радиоизлучений (поля), радиопеленгаторов, систем радиомониторинга;
- частотомера;
- локализации источников излучения в ближней зоне.

Прибор MRA — 3 также специально разработан для поиска радиозакладок в диапазоне частот от 42 до 2700 МГц и может использоваться как для периодического, так и для постоянного (непрерывного) радиоконтроля помещения.

Он имеет чувствительность 20 ... 60 мкВ в диапазоне частот от 50 до 1200 МГц и 60 ... 1000 мкВ — в диапазонах 42 ... 50 МГц и 1200... 2700 МГц. Полоса пропускания по промежуточной частоте (ПЧ) — 400 кГц.

Прибор позволяет детектировать сигналы с амплитудной (AM) и частотной (WFM, NFM) модуляцией и измерять их относительный уровень, который отражается на 40- разрядном линейном индикаторе. Прибор имеет 512 каналов “долговременной” памяти и 16 перезаписываемых каналов — для записи и последующего анализа “новых” сигналов, обнаруженных при сканировании. Прибор имеет защиту от несанкционированного доступа к каналам спектральной памяти.

Для первоначальной записи частотного спектра приемник осуществляет сканирование рабочего диапазона четыре раза подряд в течение 24 секунд (время сканирования спектрального диапазона составляет 6 секунд). Оператор имеет возможность произвести анализ записанных в память сигналов. В последующем приемник переводится в автоматический режим работы. При каждом сканировании производится сравнение обнаруженных и записанных в “долговременную” память сигналов. При выявлении нового сигнала срабатывает сигнализация, и этот сигнал записывается в блок памяти новых сигналов для последующей проверки. После анализа новых сигналов их можно записать в спектральную память в режиме обновления спектра (добавления новых сигналов).

Прибор MRA — 3 имеет размеры 136x49x137 мм и весит 620 г (вместе с аккумулятором).

2.5.5. Обнаружители диктофонов

Диктофон может быть использован как в качестве акустической закладки, так и для негласной записи конфиденциальных бесед какой-либо заинтересованной стороной. В первом случае его тайно устанавливают в контролируемом помещении и периодически меняют носитель информации, во втором – прячут в личных вещах или под одеждой.

Существуют два основных способа защиты от несанкционированной звукозаписи:

- предотвращение проноса звукозаписывающих устройств в контролируемые помещения;
- фиксация факта применения диктофона и принятие адекватных мер.

Первый способ является, по сути, поиском физического объекта, который (поиск) может осуществляться с использованием или без использования технических средств. Второй способ есть поиск радиоэлектронного устройства, и ниже будет рассмотрен подробно.

Сложность задачи обнаружения современных диктофонов заключается в том, что, с одной стороны, требуется регистрировать очень слабое электромагнитное излучение работающего диктофона. Для этого необходим чувствительный измеритель электромагнитного поля. С другой стороны, необходимо не реагировать на промышленные помехи и на излучение других приборов, которое может быть очень сильным. Причем частотный диапазон, характер и форма электромагнитных колебаний от диктофона и от мешающих источников одинаковы.

С точки зрения пользователя, обнаружитель современных диктофонов должен решать три задачи:

1. обеспечивать приемлемую дальность обнаружения для большинства диктофонов;
2. минимизировать вероятность пропуска сигнала;
3. минимизировать вероятность ложного срабатывания.

Для того чтобы оценить объем работ по созданию такого обнаружителя, необходимо рассмотреть все группы современных диктофонов на предмет создаваемого ими электромагнитного излучения, так как оно может явиться единственным демаскирующим признаком для записывающего диктофона.

По создаваемому электромагнитному излучению диктофоны могут быть разделены на две группы: имеющие в своей конструкции электродвигатель и имеющие микросхемы памяти для записи информации.

К первой группе относятся следующие аппараты:

1. построенные на классическом принципе записи электрических сигналов на магнитную ленту в аналоговом виде, имеющие простой лентопротяжный механизм и не имеющие генератора стирания и подмагничивания (ГСП);
2. то же, что п.1, но имеющие ГСП.
3. построенные на принципе записи электрических сигналов на магнитную ленту в цифровом виде на DAT-кассету и имеющие более сложный лентопротяжный механизм, аналогичный механизму видеомагнитофона;

4. построенные на принципе записи электрических сигналов на магнитный или оптический дисковый носитель в цифровом виде, например на минидиск, разработанный фирмой SONY (магнитный носитель), или на лазерный перезаписываемый диск (оптический носитель). Также имеют электродвигатель.

В дальнейшем эта группа диктофонов будет называться - "кинематические".

Характер создаваемого электромагнитного излучения этой группы диктофонов одинаков. Источником максимального излучения являются электродвигатель и генератор стирания – подмагничивания (ГСП) (только для подгруппы 2). Форма сигнала от электродвигателя носит импульсный характер с основной гармоникой в диапазоне от 80 до 300 Гц. С меньшими амплитудами в этот диапазон попадают другие гармонические составляющие этого сигнала. Излучение от ГСП приближено к синусоидальному и находится в пределах от 20 до 60 КГц.

Другая группа диктофонов построена на принципе записи электрических сигналов в кристалл микросхемы памяти в цифровом виде. Причем может использоваться энергонезависимая память (флэш-память) или (реже) динамическая или статическая память, требующая постоянно подключенного источника питания. В дальнейшем эта группа диктофонов будет называться - "цифровые".

Конструктивно "цифровые" диктофоны могут быть выполнены в двух вариантах:

1. функция диктофона является основной;
2. функция диктофона является дополнительной.

Ко второй подгруппе относятся устройства:

- некоторые модели сотовых телефонов;
- большинство "карманных" миникомпьютеров, например PocketPC;
- MP3-плейеры с возможностью записи.

Необходимо отметить, что теоретически понятием "цифровой" диктофон определено устройство, осуществляющее запись речевой информации на некоторый носитель в цифровом виде. Причем носителем может являться диск или лента. Такие устройства имеют кинематический механизм и относятся к "кинематическим" диктофонам.

По характеру излучения, "цифровые" диктофоны можно разделить на подгруппы:

1. имеющие импульсный преобразователь напряжения, например, если в качестве источника питания использована одна батарея напряжением 1,5 вольта;
2. имеющие съемную конструкцию флэш-памяти;
3. осуществляющие сжатие речевой информации посредством специализированного сигнального процессора;
4. имеющие жидкокристаллический дисплей;
5. имеющие различные подключенные аксессуары, такие, как выносной микрофон, пульт дистанционного управления и т.д.;
6. имеющие корпус, способный экранировать излучение диктофона.

Исследования показали, что максимальный уровень излучения "цифровых" диктофонов для всех подгрупп, как правило, лежит в диапазоне от 20 до 120 кГц. Для диктофонов с импульсным преобразователем напряжения наиболее сильный уровень наблюдается на частоте преобразования. Такие диктофоны могут обнаруживаться на максимальной дальности - более метра.

В диктофонах со съемной флэш-памятью неизбежно присутствует шлейф из нескольких десятков проводников, длиной несколько сантиметров. По нему передаются сигналы адреса и данных для записи в память. Эти сигналы цифровые, а значит, имеют крутые фронты и амплитуду, равную напряжению питания (обычно 3 вольта). Такое количество длинных проводников с такими сигналами дает шумоподобные всплески в некоторых частотных областях. Если использован сигнальный процессор, что характерно для техники западных производителей, спектральные всплески усиливаются, так как такой процессор потребляет более 50% энергии, необходимой для работы диктофона. Диктофоны этих двух подгрупп могут обнаруживаться на расстоянии от 50 см до 1 метра.

В диктофонах с жидкокристаллическим дисплеем последний тоже является источником образования электромагнитного поля. Причем энергия его растет с размерами дисплея, а также в случае, если он графический, и особенно цветной. Наличие таких дисплеев более характерно для приборов, у которых функция диктофона является дополнительной - сотовые телефоны, миникомпьютеры и т.д. Дальность обнаружения таких устройств может превысить 1 метр.

Для диктофонов с подключенным выносным микрофоном или пультом дистанционного управления, соединительный кабель является дополнительным относительно мощным источником излучения.

Для диктофонов в металлических корпусах дальность обнаружения резко падает, так как излучение экранируется корпусом и в зависимости от качества экранировки составляет от нескольких единиц до 30 см. Однако существует вероятность образования низкочастотных субгармоник, от излучения которых такая экранировка малоэффективна. В любом случае, диктофоны в металлических корпусах относятся к классу спецтехники и специально разрабатываются с целью минимизации излучения.

С точки зрения электротехники диктофон состоит из набора замкнутых электрических цепей, причем некоторые из них обладают значительной индуктивностью, что приводит к образованию вокруг работающего диктофона электромагнитного излучения с определенной диаграммой направленности и интенсивностью. Отсюда следует, что любой диктофон может быть обнаружен некоторым электронным устройством на определенном расстоянии.

Для выявления факта несанкционированной записи аудиосигнала используются **обнаружители (детекторы) диктофонов.** Обнаружители диктофонов, по сути, представляют собой детекторные приемники магнитного поля. Принцип их действия основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи. Электродвижущая сила (ЭДС), наводимая этим полем в датчике сигналов (магнитной антенне), усиливается и выделяется из шума специальным блоком обработки сигналов. При превышении уровня принятого сигнала некоторого установленного порога срабатывает световая или звуковая сигнализация. Технические характеристики некоторых обнаружителей приведены в таблице 5.5.

Таблица 5.5

Основные характеристики обнаружителей диктофонов

Характеристика	PTRD-016	PTRD-018	TRD-800	RM200	PK 645-S	PK 645-SS	BTRD-019	ST 0110
Изготовитель	Россия		США	Россия	Германия		Россия	Россия
Дальность обнаружения, м	До 0,7	До 1,5	До 0,5 (при наличии ГСП)	До 0,5	До 1,0	До 1,0	До 1,5	До 1,5
Количество датчиков	4	4/8/16	1	До 6	1	6	4/8/16	16/32
Питание, В	220	220			9	220	220	220
Примечание	Стационарный	Стационарный	Переносной	Стационарный	Переносной	Стационарный	Стационарный	Стационарный На базе PocketPC

Рассмотрим принцип работы обнаружителя диктофонов на основе обобщенной структурной схемы (рис. 5.4).

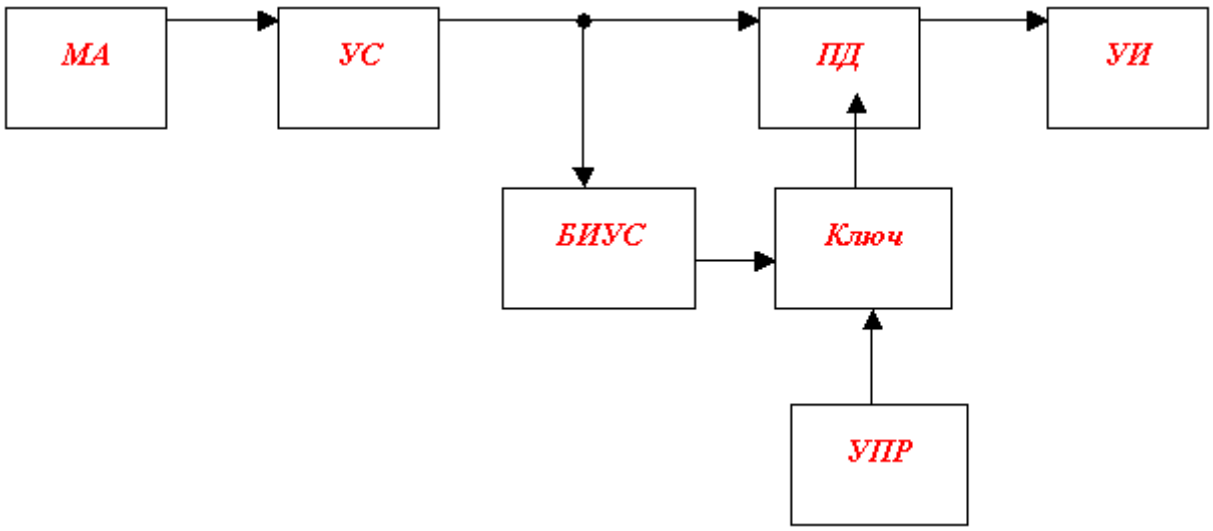


Рис. 5.4. Структурная схема обнаружителя диктофонов на базе широкополосного детектора

Магнитная антенна (МА) имеет амплитудно-частотную характеристику, которая выделяет необходимый частотный диапазон. Усилитель сигнала (УС) с антенны должен быть с минимальным собственным шумом, который и определяет чувствительность всей системы и, следовательно, дальность обнаружения. Теоретически уровень срабатывания порогового детектора (ПД) может быть установлен на значении максимального собственного шума усилителя. Соответственно превышение этого уровня покажет на устройстве индикации (УИ) наличие источника поля. Возможное расстояние до диктофона для такого обнаружителя определено собственным шумом и находится в пределах от десятков сантиметров до 2 метров, в зависимости от типа диктофона. В реальных условиях в некоторой точке пространства всегда присутствует определенный интегральный уровень электромагнитного излучения, созданный множеством других, близких и дальних источников. Этот уровень может значительно превысить собственный шум устройства обнаружения. Более того, некоторые источники (например, переменный ток в сети 220 В) создают очень большой уровень поля и фактически блокируют возможность измерения других полей. Эти условия приводят к необходимости использовать в качестве магнитной антенны (МА) не одну катушку, а две, разнесенные на некоторое расстояние и включенные дифференциально. Такая магнитная антенна становится градиентометром. При этом достигается значительное ослабление влияния удаленного источника, особенно при увеличении расстояния между катушками. К сожалению, уровень сигнала от ближнего источника (диктофона) тоже падает. Но это плата за саму возможность измерения поля ближнего источника. Учитывая действие "паразитных" электромагнитных полей, для регистрации излучения диктофона, необходим блок измерения уровня сигнала (БИУС), который выставит уровень порогового детектора (ПД) на измеренную величину при поступлении команды от управляющего устройства (УПР). Управляет этим оператор, проводящий обнаружение. Видно, что регистрация излучения диктофона в таком приборе возможна только, если это излучение больше уровня фона в данном месте. Соответственно реальная дальность обнаружения теперь сильно зависит от уровня фона и может упасть в несколько раз. Это физическое ограничение для широкополосных детекторов. По такому принципу построен канал обнаружения аудио и видеозаписывающей аппаратуры в приборе **ST 041** (в настоящее время модель снята с производства).

Для повышения эффективности этого прибора требуется решить, как минимум, две задачи: снизить собственный шум прибора и пытаться различить источники электромагнитного поля по частоте. Собственный шум устройства, рассмотренного выше, определялся шумовыми характеристиками микросхемы усилителя и шириной частотного диапазона измерения. Отсюда следует, что уменьшение частотной полосы приведет к уменьшению собственного шума обнаружителя. Эта задача решается путем использования группы полосовых фильтров, перекрывающих интересующий частотный диапазон. Увеличение числа фильтров приводит к улучшению соотношения сигнал/шум. Кроме того, эти же фильтры решают и вторую задачу - позволяют локализовать сигнал по частоте. В результате, у прибора появляется способность "видеть" очень слабые источники электромагнитного излучения на фоне очень сильных, что

абсолютно невозможно для широкополосного детектора. На этой основе построен другой прибор для обнаружения диктофонов - **ST 0110**. В каждом канале прибора используются две независимые магнитные антенны (МА НЧ и МА ВЧ), преобразующие магнитную составляющую электромагнитного поля в электрический сигнал, который поступает в усилитель сигнала. Полоса пропускания связки низкочастотной магнитной антенны и усилителя составляет 50-400 Гц, что достаточно для обнаружения "кинематических" диктофонов. В качестве магнитной антенны для этой частотной полосы использован градиентометр. Полоса пропускания связки высокочастотной магнитной антенны и усилителя составляет 20-120 КГц, что ориентировано на обнаружение "цифровых" диктофонов. Усиленные сигналы поступают на аналого-цифровой преобразователь (АЦП), переводятся в цифровую форму и все дальнейшие операции выполняются компьютером.

ST 0110 работает в комплекте с "карманным" миникомпьютером класса PocketPC или с любым IBM-совместимым настольным компьютером, в том числе ноутбуком. Максимальное число каналов (зон обнаружения) - 16, для настольного компьютера расширяется до 32 и более.

2.5.6. Универсальные поисковые приборы

Рассмотренные выше специальные технические средства узко специализированы. Так, индикаторы поля позволяют локализовать источник радиоизлучения в пространстве, сканирующие приемники – проводить радиомониторинг на объекте и т.д. Однако при проведении поиска приходится решать, как правило, несколько задач:

- проведение радиомониторинга;
- локализация (пеленгование) источника излучений;
- идентификация сигналов радиозакладок;
- контроль силовых, телефонных, радиотрансляционных и других линий;
- постановка прицельных помех и др.

На рынке специальных технических средств защиты информации представлено достаточно изделий как отечественного, так и зарубежного производства, в той или иной степени позволяющих решать эти задачи. Однако поиск средств негласного съема информации остается их основным предназначением. Решение задачи поиска обеспечивается наличием в составе комплексов следующих обязательных элементов:

- широкодиапазонного перестраиваемого по частоте приемника (сканера);
- блока распознавания закладок, осуществляющего идентификацию излучений радиозакладок на основе сравнения принятых продетектированных сигналов с естественным акустическим фоном помещения (пассивный способ) или тестовым акустическим сигналом (активный способ);
- блока акустической локации;
- процессора, осуществляющего обработку сигналов и управление приемником.

Ниже будут рассмотрены некоторые из универсальных поисковых приборов, конструктивно выполненные в виде единого устройства.

OSC-5000 (Oscor) (США)**.** Его название происходит от Omni Spectral Correlator и характеризует основное назначение прибора как спектрального коррелятора. OSC-5000 представляет собой функциональное сочетание нескольких приборов.

Во-первых, это панорамный приемник последовательно-параллельного типа (сканер), перекрывающий диапазон частот 10 кГц … 3ГГц с полосой пропускания 15 кГц. Широкий диапазон перестройки обеспечивается наличием нескольких входов (фактически нескольких приемников), к каждому из которых подключена своя антенна – рамочная, штыревая и дискоконусная. Анализ может производиться как во всем диапазоне, так и в заданных полосах, автоматически или в ручном режиме. Максимальная скорость перестройки по частоте составляет 93 МГц/сек при полосе пропускания 250 кГц. Чувствительность приемника соответствует значению 0,8 мкВ. Динамический диапазон составляет 90 дБ. Прибор оснащен набором детекторов, что позволяет принимать сигналы с различными видами модуляции. Кроме того, в составе прибора имеются инфракрасный детектор с областью спектральной чувствительности 0,85 – 1,07 мкм и специальный адаптер, позволяющий вести контроль излучений сетевых закладок в диапазоне частот 10 кГц … 5 МГц в проводных линиях с напряжением до 300 В.

Во-вторых, это осциллограф и анализатор спектра, позволяющий наблюдать амплитудно-временные развертки демодулированных сигналов и их спектры с разрешением по частоте не хуже 50 Гц.

В-третьих, это коррелятор, необходимый для идентификации сигналов закладных устройств.

Принцип работы коррелятора заключается в том, что демодулированный низкочастотный сигнал сравнивается с акустическим фоном помещения. На основе результатов этого сравнения рассчитывается коэффициент корреляции и в зависимости от полученного значения каждому сигналу присваивается один из пяти уровней тревоги. При превышении этим уровнем заданного оператором порогового значения срабатывает система оповещения – мигание сообщения на экране, звуковой сигнал, запись на диктофон или печать характеристик (по выбору). Прибор фиксирует частоту излучения, тип демодулятора, время обнаружения и сохраняет все эти сведения в базе данных или (и) выводит на встроенный термоплоттер. Прибор можно запрограммировать таким образом, что при обнаружении тревожного сигнала будет распечатан его спектр или произойдет запись передаваемой информации на встроенный диктофон.

В OSC-5000 предусмотрен режим загрузки в память частот, излучения на которых прибор будет считать «дружественными» (например, сигналы вещательных станций) и не затрачивать время на анализ в автоматическом режиме. Всего Oscor может хранить информацию о 7168 сигналах при штатной памяти 128 К или о 28672 при расширенном до 512 К объеме памяти. Эта информация может редактироваться оператором, протоколироваться самим прибором на термоплоттере или сбрасываться на ПЭВМ через COM-порт для дальнейшей обработки.

Дополнительными опциями для OSC-5000 являются:

- OVM-5000, предназначенная для анализа видеосигналов PAL/SECAM/NTSC при поиске видеопередатчиков;
- OTL-5000 – акустический локатор, предназначенный для определения положения активных радиозакладок;
- OPC-5000 – специальное программное обеспечение для работы с базами данных Oscor через COM-порт ПЭВМ, а также для организации дистанционного контроля работы комплекса через модем.

Комплекс смонтирован в кейсе (габариты 473 х368 х159 мм). Вес 12,7 кг. Питание 110/220 В и 12 В (встроенный аккумулятор).

Зонд-монитор СРМ-700 (США). Другое название – комплекс **«Акула».** Предназначен для:

1. обнаружения сигналов радиозакладок в диапазоне 50 кГц … 3 ГГц;
2. обнаружения закладных устройств, использующих токопроводящие линии для передачи информации (диапазон 15 кГц … 1 МГц);
3. выявления микрофонов с передачей информации по специально проложенным проводам;
4. определения степени опасности утечки информации за счет наличия «микрофонного эффекта» в телефонных, трансляционных и других низковольтных линиях;
5. обнаружения скрытых видеокамер и диктофонов;
6. выявления закладных устройств с инфракрасным каналом передачи информации;
7. обнаружения воздушных и структурных каналов утечки акустической информации.

Первые три задачи являются основными, поэтому в любой комплект СРМ-700 обязательно входят три соответствующих зонда.

1. Высокочастотный зонд с областью спектральной чувствительности 50 кГц … 3 ГГц. Это активный прибор с собственным коэффициентом усиления 20 дБ, обеспечивающий пороговую чувствительность приемника на уровне –85 дБ и динамический диапазон входных сигналов 100 дБ. Такие характеристики, например, позволяют обнаруживать источники радиосигналов мощностью 1 мкВт на расстоянии около 2 м.
2. Низкочастотный зонд для контроля токопроводящих линий. Диапазон рабочих частот лежит в пределах 15 кГц … 1 МГц, пороговая чувствительность – не хуже 60 дБ. Максимальный уровень постоянного напряжения в тестируемых линиях не должен превышать 300 В, переменного с частотой 60 Гц – 1500 В.
3. Усилитель низкой частоты (100 Гц … 15 кГц) для прослушивания электромагнитных сигналов звукового диапазона, возникающих вблизи токопроводящих линий.

Для решения 4 – 6 задач применяются дополнительные зонды:

4. Электромагнитный зонд MLP-700 для обнаружения скрытых видеокамер и диктофонов.

5. Инфракрасный зонд IRP-700 для обнаружения источников излучения в инфракрасном диапазоне.

6. Акустический зонд ALP-700 для обнаружения воздушных и структурных каналов утечки акустической информации.

Кроме вышеперечисленных основных функций комплекс обеспечивает:

- работу в дежурном режиме – отслеживает электромагнитную обстановку в контролируемом помещении и подает звуковой или световой сигнал при обнаружении неизвестного излучения («мониторинг опасности»);
- непрерывную запись всех принимаемых сигналов на любой стандартный диктофон.

ST 031 («Пиранья») (Россия). Комплекс предназначен для проведения оперативных мероприятий по обнаружению и локализации технических средств негласного получения конфиденциальной информации, а также контроля естественных и искусственно созданных ТКУИ.

Комплекс состоит из блока управления и индикации и комплекта преобразователей:

- высокочастотный детектор – частотомер;
- сканирующий анализатор проводных линий;
- детектор инфракрасных излучений;
- детектор низкочастотных магнитных полей;
- виброакустический приемник;
- акустический приемник;
- проводный акустический приемник.

Комплекс позволяет анализировать принимаемые сигналы как в режиме осциллографа, так и в режиме анализатора спектра с индикацией численных параметров. Переход в любой из режимов измерения осуществляется автоматически при подключении соответствующего преобразователя к блоку управления. Информация отображается на LCD-дисплее. Акустический контроль осуществляется через головные телефоны или встроенный динамик. Управление осуществляется с 16-и кнопочной пленочной клавиатуры. Габариты основного блока 180x97x47 мм, масса – 800 г. Источник питания прибора – 4 батареи AA.

2.5.7. Программно-аппаратные поисковые комплексы

Другая группа многофункциональных поисковых приборов представлена программно-аппаратными комплексами, сформированными на базе серийного сканера (сканеров), персонального компьютера (обычно notebook) и специального программного обеспечения.

Использование внешней ПЭВМ с программным обеспечением позволяет автоматизировать процесс поиска и обнаружения закладных устройств, проводить анализ радиоэлектронной обстановки по районам контроля, вести базу радиоэлектронных средств. Малый вес и габариты комплексов в сочетании с универсальным питанием позволяют работать с ними как в стационарных, так и в полевых условиях.

Состав и основные характеристики некоторых программно-аппаратных комплексов контроля приведены в таблицах 5.6 – 5.9.

Функциональное совмещение специальных приемников с ПЭВМ существенно повышает надежность и оперативность поиска закладных устройств, делает процедуру поиска более технологичной.

На компьютер при этом возлагается решение следующих задач:

- хранение априорной информации о радиоэлектронных средствах, работающих в контролируемой области пространства и выбранных диапазонах частот;
- получение программными методами временных и частотных характеристик принимаемых сигналов (вместо использования достаточно громоздких осциллографов и анализаторов спектра);
- тестирование принимаемых сигналов на принадлежность к излучению ЗУ.

Таблица 5.6

Программно-аппаратные комплексы контроля ЗАО НПЦ «Нелк»

Наименование характеристик	Индекс (тип)		
	Крона-4	Крона-5Н	Крона-6Н
Состав комплекса	Сканирующий приемник AOR 3000A. Пассивный акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook	Сканирующий приемник AOR 3000A (доработанный). Устройство спектральной обработки сигналов на основе процессора БПФ Пассивный акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook	Сканирующий приемник AOR 5000. Устройство спектральной обработки сигналов на основе процессора БПФ Пассивный акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook
Программное обеспечение	Специальное программное обеспечение семейства Sedif, Filin		
Диапазон частот, МГц	25 … 2000	25 … 2036	10 … 2600
Скорость просмотра диапазона, МГц/сек		4	4 …. 8
Вид модуляции обнаруживаемых сигналов	AM, NFM, WFM (в том числе с инверсией спектра)		
Методы идентификации сигнала	Корреляция сигнала (активный и пассивный тесты). Проверка на наличие гармоник		
Возможности документирования	Запись на жесткий диск спектрограмм, фонограмм, осциллограмм и корреляционных функций сигналов		
Дополнительные возможности	Определение координат радиозакладок. Проверка проводных линий. Поиск инфракрасных закладок. Возможность детального анализа сигналов в ручном режиме.		
Конструкционное оформление	Кейсовая укладка		

Таблица 5.7

Программно-аппаратные комплексы контроля ЗАО «Иркос»

Наименование характеристик	Индекс (тип)			
	АРК-Д1_5К	АРК-3Д	АРК-ПК_5К	АРК-ПК_3К
Состав комплекса	Сканирующий приемник AOR 5000. Устройство спектральной обработки сигналов на основе процессора БПФ. Акустический коррелятор. Устройство для проверки проводных линий. ПЭВМ Notebook	Сканирующий приемник AOR 3000A (доработанный). Устройство спектральной обработки сигналов на основе процессора БПФ Акустический коррелятор. Устройство для проверки проводных линий. ПЭВМ Notebook	Сканирующий приемник AOR 5000. Устройство спектральной обработки сигналов на основе процессора БПФ. Акустический коррелятор. Устройство для проверки проводных линий. ПЭВМ Notebook	Сканирующий приемник AOR 3000A (доработанный). Устройство спектральной обработки сигналов на основе процессора БПФ Акустический коррелятор. Устройство для проверки проводных линий. ПЭВМ Notebook
Программное обеспечение	СМО-Д5		Filin	Filin
Диапазон частот, МГц	1 … 2600	1 … 2000	1 … 2600	1 … 2000
Динамический диапазон, дБ	55 … 60			
Дискретность отсчета частоты	3 кГц			
Скорость просмотра диапазона, МГц/сек	28	40 … 70		
Скорость панорамного анализа, МГц/сек В полосе 2 МГц В полосе 80 МГц В полосе > 80 Мгц			 28 14 18	 40 … 70 30 40
Вид модуляции обнаруживаемых сигналов	AM, NFM, WFM (в том числе с инверсией спектра)			
Методы идентификации сигнала	Корреляция сигнала (активный и пассивный тесты). Проверка на наличие гармоник			
Возможности документирования	Запись на жесткий диск спектрограмм сигналов		Запись на жесткий диск спектрограмм сигналов, времени их обнаружения, речевых сигналов	
Дополнительные возможности	Определение координат радиозакладок. Проверка проводных линий, анализ видеосигналов			
Конструкционное оформление	Кейсовая укладка			

Таблица 5.8

Программно-аппаратные комплексы контроля фирмы «Радиосервис»

Наименование характеристик	Индекс (тип)			
	RS 1000/8	RS 1000/3	RS 1100	RS 1200
Состав комплекса	Сканирующий приемник фирмы AOR AR8000 (доработанный), соединительный кабель с интерфейсной схемой. Акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook	Сканирующий приемник фирмы AOR AR3000A, соединительный кабель с интерфейсной схемой. Акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook	Сканирующий приемник фирмы AOR AR5000. Микроконтроллер RS 1100/C. Антенные коммутаторы RS 1100/K Акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook	По выбору – AR3000A, AR5000, AR8000, AR8200, PCR1000, PCR100 Микроконтроллер RS 1100/C. Антенные коммутаторы RS 1100/K Акустический коррелятор. Конвертор для проверки проводных и оптических линий. ПЭВМ Notebook
Диапазон частот, МГц	30 … 1900	0,1 … 2030	0,1 … 2600	В зависимости от выбранного приемника
Скорость просмотра диапазона, динамический диапазон, дискретность отсчета частоты	Определяются возможностями базового приемника			
Вид модуляции обнаруживаемых сигналов	AM, NFM, WFM (в том числе с инверсией спектра)			
Методы идентификации сигнала	Корреляция сигнала (активный и пассивный тесты). Проверка на наличие гармоник			
Возможности документирования	Запись на жесткий диск спектрограмм сигналов			
Дополнительные возможности	Определение координат радиозакладок. Проверка проводных линий. Поиск инфракрасных закладок.			
Конструкционное оформление	Кейсовая укладка			

Таблица 5.9

Программно-аппаратный комплекс контроля КРК-1 ЗАО «Ново»

Наименование характеристик	Значение характеристик
Состав комплекса	Сканирующий приемник фирмы AOR AR5000. Устройство спектральной обработки сигналов на основе процессора БПФ. ПЭВМ не хуже Pentium 100/8/810. Звуковая плата SB Vibra 16S. Звуковые колонки. Блоки ВЧ и НЧ-коммутаторов. Токосъемник ТК-101.
Диапазон частот, МГц	0,01 … 2600
Скорость просмотра диапазона, МГц/сек, в режиме «Детальная панорама» «Общая панорама»	 200 30
Шаг перестройки в автоматическом режиме	20
Ширина полосы пропускания, кГц при сканировании при анализе сигнала	 44 3; 6; 15; 30; 110; 220
Динамический диапазон	65
Вид модуляции обнаруживаемых сигналов	Амплитудная, частотная (в т.ч. со скремблированием), дельта-модуляция, шумоподобные сигналы
Методы идентификации сигнала	Корреляция сигнала (активный и пассивный тесты). Проверка спектра сигнала на наличие паразитной модуляции. Сравнение уровней сигнала от внешней и внутренних (распределенных) антенн
Возможности документирования	Запись на жесткий диск спектрограмм, фонограмм, основных характеристик сигналов, амплитудно-частотной загрузки диапазона и протокола работы
Дополнительные возможности	Определение координат радиозакладок. Проверка проводных линий.
Конструкционное оформление	Единый корпус

В настоящее время известно большое количество программ, специально разработанных для ведения мониторинга. Наиболее распространенные среди них – это «СканАР», Sedif, Filin, RSPlus, «Крот-mini», Arcon, Radio-Search, а также некоторые другие. В качестве примера ниже будут рассмотрены возможности двух программ семейства «Sedif» - **«Sedif PRO»** и **«Sedif Scout»**.

Программное обеспечение **«Sedif PRO»** позволяет решать в автоматическом или автоматизированном режиме следующие задачи:

- выявление излучений радиозакладок и определение их местоположения;
- обнаружение и распознавание сигналов РЭС, выявление особенностей их работы;
- анализ индивидуальных особенностей спектров сигналов отдельных РЭС в интересах решения задачи их распознавания;
- выявление и анализ ПЭМИ, возникающих при работе ТСПИ;
- анализ данных по радиоэлектронной обстановке в точке приема, интенсивности использования фиксированных частот и работы отдельных РЭС;
- перехват и регистрацию сообщений, передаваемых по каналам радиосвязи.

В программе реализованы пять основных режимов работы: ПАНОРАМА, ЧАСТОТОГРАММА, ПРИЕМНИК, ФОНОТЕКА и ОСЦИЛЛОГРАФ.

В режиме ПАНОРАМА управляющая программа выполняет перестройку приемника с выбранным шагом и полосой пропускания в пределах заданной полосы обзора относительно заданной центральной частоты и представляет результаты измерений уровней принимаемых сигналов на каждом шаге в форме панорамы частот в координатах «уровень – частота». Обеспечивается возможность слухового контроля, записи информации на жесткий диск, формирования до 100 режекторных фильтров, быстрого изменения масштабов амплитудно-частотного окна, накопления значений уровня сигнала за несколько измерений на каждом шаге.

Режим ПАНОРАМА необходим для первичного анализа спектра шумов и сигналов в заданных частотных диапазонах, выбора оптимального порога, оценки загруженности диапазонов, а также анализа амплитудно-частотных характеристик отдельных сигналов. Для гарантированного

обнаружения новых сигналов при большой загруженности частотных диапазонов предусмотрен режим вычитания текущей панорамы из сохраненной ранее. Любая панорама может быть сохранена в архиве с соответствующими комментариями, вызвана на экран и распечатана на принтере.

Режим ЧАСТОТОГРАММА предназначен для временного анализа загруженности сетки частот с возможностью регистрации всех сеансов работы РЭС (по критерию превышения уровня сигнала заданного порога). Для каждой частоты устанавливается свой порог, полоса пропускания, вид модуляции (детектор) и ослабление (аттенюатор).

В каждой ЧАСТОТОГРАММЕ возможны сканирование и отображение сигналов на 24 номиналах частот в течение времени до 36 часов, быстрое включение и исключение из списка отдельных частот, их сортировка по определенным критериям, остановка на любой частоте для звукового контроля, анализ интенсивности работы РЭС. Оператор может создать библиотеку частотограмм и включать их в задание в нужной последовательности. Таким образом, число контролируемых частот не ограничивается количеством банков и ячеек памяти приемника.

Режим ПРИЕМНИК предназначен для сканирования в широком участке частотного диапазона с отображением обнаруженных сигналов. Это позволяет, например, отобразить на экране монитора диапазон частот шириной 1000 МГц и разрешением по частоте 10 кГц. Все сигналы, обнаруженные в процессе работы в режимах ПАНОРАМА и ЧАСТОТОГРАММА, при переходе в режим ПРИЕМНИК будут также отображены на мониторе. Имеющаяся в данном режиме функция «лупы» позволяет увеличивать в 10 раз выбранный участок обзора для точной настройки на отдельный сигнал.

В режиме ФОНОТЕКА осуществляется регистрация на жесткий диск ПЭВМ принимаемой звуковой информации или модулирующей функции радиосигналов, а также учет и обработка звуковых файлов. Предусмотрен осциллографический анализ звуковых сигналов. Встроенный конвертор аудиофайлов позволяет использовать аппаратные и программные средства обработки фонограмм других производителей.

Режим ОСЦИЛЛОГРАФ позволяет проводить визуальное исследование модулирующей функции радиотехнических сигналов в непрерывном или запоминающем режимах с частотой дискретизации до 40 кГц. Предусмотрено создание архива осциллограмм, сжатие/растяжение по горизонтали и вертикали, различные варианты запуска.

Процесс контроля может быть полностью автоматизирован путем создания и запуска на исполнение комплексных заданий. Задание представляет собой совокупность заполненных диапазонов, панорам и фиксированных частот, сканирование и измерения в которых будут выполняться так же, как в режимах ПРИЕМНИК и ПАНОРАМА, но без вмешательства оператора. Перед выполнением каждого пункта задания может быть включен режим ожидания. По результатам выполнения задания формируется отчет, который может быть отредактирован оператором и выведен на печать.

Программное обеспечение **«Sedif Scout»** предназначено прежде всего для обнаружения излучений акустических и телефонных закладных устройств и их локализации. Для работы с программой необходима ПЭВМ, имеющая в своем составе звуковую карту CREATIVE SB-16.

Программа позволяет оператору с помощью сканирующего приемника (AR-2700, AR-8000, AR-3000A, AR-5000, IC-R10, IC-R7100, IC-R8500, IC-R9000) проводить автоматический анализ загрузки выбранного участка диапазона, выявлять в нем новые сигналы, осуществлять их проверку на принадлежность к классу закладных систем, определять координаты местоположения закладок.

В программе реализованы следующие алгоритмы работы:

- установка динамического порога обнаружения;
- проверка наличия гармоник у выявленного закладного устройства;
- возможность использования для выявления новых излучений заранее отснятых спектрограмм загрузки диапазона;
- отслеживание сигналов источников с нестабильным по частоте излучением и др.

Программа полностью автоматизирует процесс поиска и принятия решения об обнаружении закладных устройств, что дает возможность использовать ее даже неподготовленному оператору. В списке сигналов, классифицированных программой как сигналы закладных устройств, против каждого номинала частоты указываются признаки, по которым принято данное решение: акустическая корреляция с тестовым сигналом, наличие гармоник основного излучения с превышением порога или и то и другое.

В программе сохранены все режимы и функции программы **«Sedif PRO»**, что дает возможность оператору самому детально исследовать параметры сигналов, отнесенных программой к разряду вероятных сигналов закладных устройств.

Определение местоположения обнаруженной закладки осуществляется программой с участием оператора. Полученные координаты программа наглядно отображает на экране монитора.

2.5.8. Нелинейные локаторы

Нелинейный локатор предназначен для обнаружения дистанционно-управляемых и (или) включающихся по голосовому сигналу закладных устройств, а также обнаружения скрытно установленных записывающих устройств. Обычно специальная техника для их обнаружения имеет очень небольшой радиус действия и эффективна для обнаружения только активной техники. Иначе говоря, нелинейный локатор может быть использован для обнаружения активных и неиспользуемых, работающих и неработающих радиомикрофонов и телефонных микропередатчиков, сожженных радиомикрофонов, тайно установленных диктофонов, усилителей, микрофонов с усилителями и т.п.

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

Нелинейные локаторы отечественного и зарубежного производства можно разделить на две группы: импульсного и непрерывного излучения. Первые посылают более мощный сигнал короткими импульсами, последние производят обнаружение за счет повышенной чувствительности. Экспериментально доказано, что локаторы с импульсным излучением обладают большей глубиной обнаружения.

Наличие в локаторе анализа 2-ой и 3-ей гармоник позволяет производить детектирование микросхем закладных устройств и диктофонов с большей точностью: некоторые органические предметы могут проявлять нелинейность также, как и электронные компоненты. Результаты сравнения отражения по обеим гармоникам свидетельствуют с большей точностью о наличии подобной "псевдонелинейности". Это сравнение дает возможность отличить отраженный сигнал электронных компонентов и органических объектов. Превышение уровня сигнала на 3-ей гармонике над уровнем на 2-ой свидетельствует об обнаружении помехового объекта с контактными нелинейностями (коррозионный эффект). Такой функцией обладает, например, локатор NR-900E. Также немаловажно наличие функции прослушивания модулированных сигналов локатора, отраженных от обнаруженных полупроводниковых элементов закладок.

Работа с нелинейными локаторами требует некоторых навыков. При обследовании оператор двигается по помещению вдоль стен и предметов интерьера, антенна локатора медленно перемещается на расстоянии не более 20 см от обследуемых предметов со скоростью не более 30 см/сек. Об обнаружении предмета, содержащего полупроводниковые компоненты, свидетельствует наличие сигнализации отражения сигнала по второй или по второй и третьей гармоникам; при этом при понижении уровня чувствительности локатора уровень сигнала по 3-ей гармонике значительно сокращается или исчезает. В наушниках при этом прослушивается устойчивый сигнал, причем, если обнаружена активная радиозакладка, через наушники можно прослушать тестовый сигнал, создаваемый на время обследования в помещении. Напротив, неустойчивый сигнал в наушниках, потрескивание, неустойчивая световая сигнализация свидетельствуют о коррозионном эффекте. В этом случае простое постукивание по обследуемому объекту может привести к изменению характеристик сигнала.

Таблица 5.10

Характеристики нелинейных локаторов

Тип, страна изготовит.	Режим излуч.	Мощ. перед. Вт. мин./макс.	Коэф. усиления антенны, Дб	Частота излучения, МГц	Частота приёма, МГц	Чувств. dB/Вт	Напряж. питания В
“BROOM CM” (Великоб.)	Непр.	0.02/0.3	-	915	1830	-120	220/12
“SUPER BROOM” (Великоб.)	Непр.	0.03/0.3	-	915	1830 2745	-120	220/12
“Энвис” (Россия)	Непр.	0.04/0.8	3	910	1820 2730	-145	220/12
“AT623” (Россия)	Непр.	0.03/0.3	0	915	1830 2745	-150	12
“Онега 3” (Россия)	Имп.	-/100	3	910	1820 2730	-120	220/12
“Обь” (Россия)	Непр.	-/0.25	3	1000	2000	-145	220/12
“Люкс” (Россия)	Имп.	3/14	3	435	970	-120	220
“Лотос” (Россия)	Имп.	30/300	3	890	1780	-110	220
“Циклон_М” (Россия)	Имп.	50/300	3	680	1360	-110	220/12
“Октава М” (Россия)	Имп.	50/300	3	890	1780	-110	220/12
NR 900M (Россия)	Имп.	40/150	8 - 9	900	1800	-115	220/12
NR 900E (Россия)	Имп.	40/150	8 – 9	900	1800 2700	-115	220/12
NR 900EM (Россия)	Имп.	0,1 (средняя)	8 - 9	900	1800 2700	-115	220/12
ORION (США)	Имп.	1,4 (пиковая)		850 -1020 с шагом 200 кГц	1700-2040 2550-3060	-129	7,2

В табл. 5.10 приведены основные технические характеристики нелинейных локаторов (НЛ) зарубежного и отечественного производства, представленные на рынке России.

Наиболее существенным классификационным признаком является мощность излучаемого зондирующего сигнала. Анализ таблицы показывает, что все НЛ можно разделить на две большие группы:

- "мощные", как правило, импульсные НЛ с выходной мощностью > 100 Вт;
- "маломощные", как правило, непрерывные НЛ с выходной мощностью ~ 1 Вт.

В свою очередь, НЛ той и другой группы подразделяются на одночастотные и двухчастотные. Последние обеспечивают возможность сравнительного анализа 2 и 3-й гармоник зондирующего сигнала, что существенно расширяет возможности оператора в части идентификации электронных объектов поиска на фоне коррозионных нелинейностей.

Рис. 5.5. Нелинейный локатор NR-900E

Рис. 5.6. Нелинейный локатор «ORION»

Как следует из таблицы 5.10, мощность передатчиков импульсных локаторов в 1000 раз выше, чем у непрерывных; в то же время чувствительность приемников непрерывных локаторов в 1000 раз лучше, чем у приемников импульсных НЛ.

С учетом указанных пропорций из соотношений ближней нелинейной локации следует, что при прочих равных условиях, в частности, идентичных направленных свойствах антенных систем, соотношение сигнал/шум на входе приемника импульсного локатора примерно на 3 порядка выше, нежели у непрерывного. Это означает, что дальность обнаружения объекта, обеспечиваемая импульсным НЛ, в 3 раза больше, чем у непрерывных.

Сфера применения маломощных, как непрерывных, так и импульсных НЛ, ограничивается поиском в поверхностном слое строительных конструкций, а также в простейших элементах интерьера. Маломощные НЛ способны гарантировать обнаружение только простейших объектов поиска, не оснащенных серьезной экранировкой и специальными фильтрами, снижающими нелинейную эффективную поверхность рассеивания искомого объекта.

Мощные импульсные локаторы обеспечивают гораздо большую производительность и эффективность поисковых мероприятий. Они практически не требуют двухстороннего

обследования массивных элементов интерьера, обязательного вскрытия подвесных потолков, а также обеспечивают уверенный поиск в толще строительных конструкций.

Вопросы электромагнитной совместимости мощных локаторов положительно решены в последней модификации локаторов серии NR900 за счет высокоэффективной антенной системы, имеющей узкую диаграмму направленности (60 дБ по половинной мощности), а также за счет введения режима прослушивания, обеспечивающего контроль загрузки диапазона до включения передатчика.

Совместно с нелинейным локатором целесообразно использовать металлодетекторы, так как некоторые закладные устройства выполняются в экранированном корпусе.

2.5.9. Технические средства контроля двухпроводных линий

Технические средства данной группы предназначены для выявления электрических каналов утечки информации, передаваемой по двухпроводным линиям. Как правило, такими линиями являются линии телефонной связи на участке «Абонент – ГАТС», т.е. речь будет идти о выявлении негласных гальванических подключений к телефонной линии для их последующей нейтрализации.

Методы **контроля телефонных линий** в основном основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: амплитуд напряжения и тока в линии, а также значений емкости, индуктивности, активного и реактивного сопротивления линии. В зависимости от способа подключения устройства перехвата информации к телефонной линии (последовательного, в разрыв одного из проводов телефонного кабеля, или параллельного) степень его влияния на изменение параметров линии будет различной.

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 входное сопротивление, которое может составлять от сотен Ом до нескольких МОм.

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: 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 в линию от АТС поступает сигнал, преобразуемый в телефонной трубке в длинный гудок, а напряжение в линии уменьшается до 10 – 12 В.

Большинство устройств защиты производят автоматическое измерение напряжения в линии и отображают его значение на цифровом индикаторе.

Если к линии будет подключено закладное устройство, то эти параметры изменятся (напряжение будет отличаться от типового для данного телефонного аппарата).

В табл. 5.11 приведены экспериментально полученные значения падения напряжения на линии для некоторых телефонных закладок.

Однако падение напряжения в линии (при положенной и поднятой трубке) не дает однозначного ответа – установлена в линии закладка или нет, так как 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 устройства перехвата информации необходим постоянный контроль ее параметров.

При подключении к телефонной линии устройства перехвата информации 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.

Таблица 5.11

Экспериментально полученные значения падения напряжения на линии, при подключении некоторых телефонных радиозакладок

Тип радиозакладки	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 = 140 МГц)	63.2	- 0.5	- 0.78	9.9	- 0.5	- 4.81
С последовательным включением, кварцевая стабилизация частоты (f = 140 МГц)	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
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	-	-	-

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 имеют невысокое входное сопротивление (несколько кОм) и практически не потребляют энергию из телефонной линии, но значительно увеличивают ее емкость.

Производя измерение тока в линии при снятии телефонной трубки и сравнивая его с типовым, можно выявить факт подключения закладных устройств с током потребления более 500 – 800 мкА.

Определение техническими средствами контроля закладных устройств с малым током потребления из линии ограничено собственными шумами линии, вызванными нестабильностью 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.

В настоящее время рынок изделий специальной техники представлен широким выбором приборов, позволяющих с той или иной степенью достоверности обнаруживать наличие прослушивающих устройств, установленных на телефонной линии.

По принципу действия приборы обнаружения подслушивающих устройств можно условно разделить на следующие группы:

- устройства контроля напряжения линии;
- устройства контроля окружающей радиообстановки;
- устройства контроля сигналов на телефонной линии;
- устройства анализа неоднородности телефонной линии;
- устройства анализа несимметрии линии;
- устройства анализа нелинейности параметров линии

Устройства контроля напряжения линии образуют наиболее многочисленную группу приборов обнаружения. Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения. При настройке оператор фиксирует значение напряжения, соответствующее нормальному состоянию линии (когда к линии не подключены посторонние устройства), и порог тревоги. При уменьшении напряжения в линии более установленного порога устройством подается световой или звуковой сигнал тревоги.

На принципах измерения напряжения в линии построены и устройства, сигнализирующие о размыкании телефонной линии, которое возникает при последовательном подключении закладного устройства.

Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет "микрофонного эффекта" в элементах телефонного аппарата и высокочастотного "навязывания".

Приборы данной группы регистрируют изменение напряжения линии с помощью компараторов или вольтметров. При этом если напряжение на линии изменяется на достаточную величину, то делается вывод о гальваническом подключении к линии. Основным недостатком всех приборов данной группы является то, что они должны быть установлены на «чистую» линию, т.е. выявляются только новые гальванические подключения к линии. Например, все приборы данной группы успешно выявляют «поднятие» трубки параллельного телефона в момент проведения переговоров по линии или подключение к линии «новых» телефонных закладок с питанием от линии (последовательных с сопротивлением более 0,5 кОм, параллельных с сопротивлением менее 10 кОм). При измерении напряжения линии с помощью вольтметров или компараторов следует учитывать «естественные» колебания напряжения линии в пределах до 1В, зависимость параметров линии от температуры, влажности, состояния оборудования АТС, сопротивления переходных колодок и других факторов. На рынке спецтехники широко представлены недорогие анализаторы напряжения линии на основе компараторов: **АЛ-2, АТЛ-2, АТЛ-3, АТ-21, СКАТ-3, СКАТ-4** и др. Часто анализаторы напряжения линии встраивают как составные части в более сложные приборы защиты переговоров по телефонной линии (например, в генераторы помех). К таким приборам можно отнести: **TRTD-061, TSU-3000, SI-2002, АТОЛЛ, АТ-23, БАРЬЕР-3, КЗОТ-06, ПРОКРУСТ, ПРОТОН, SI-2020, УЗТ-01.** В любом из перечисленных приборов контроля напряжения линии чувствительность невысока и ограничена нестабильностью параметров телефонной линии. Замена телефонного аппарата требует перенастройки прибора, а при первом подключении необходима проверка линии на «чистоту» другими техническими средствами.

Устройства контроля окружающей радиообстановки позволяют проводить поиск активных радиомикрофонов (радиозакладок) в помещении, обследовать телефонную линию, электросеть и другие линии связи для выявления работающих закладок с радиоканалом, побочных излучений, радиооблучения и много другого. К данному типу устройств относятся сканирующие приемники, индикаторы поля, специальные частотомеры и анализаторы спектра, спектральные корреляторы, комплексы радиоконтроля и т.д. – все те технические средства, которые достаточно подробно рассмотрены в разделах 2.5.3, 2.5.4, 2.5.6 и 2.5.7. Основным достоинством этой группы приборов является достоверность полученной информации о наличии прослушивающих устройств с радиоканалом, возможность отыскания радиопередающего устройства. К недостаткам способа относятся малая дальность обнаружения «жучков», обязательная активизация прослушивающих устройств при их поиске, значительное время контроля эфира, что затрудняет оперативный

контроль телефонной линии. Следует заметить, что в данной группе приборов наиболее предпочтительными и эффективными являются сложные комплексы радиоконтроля (**OSCOR-5000, КРОНА** и подобные).

Принцип действия **устройств контроля сигналов на телефонной линии** основан на частотном анализе сигналов, имеющихся на проводной линии (электросеть, телефонная лини, кабельные линии сигнализации и т.д.). Как правило, приборы этой группы работают в диапазоне частот 40 Гц ...10 МГц, имеют высокую чувствительность (на уровне 20 мкВ), различают модуляцию принимаемого сигнала, имеют возможность контроля принимаемой информации. С помощью данных приборов можно легко установить факт передачи информации по линии связи, «ВЧ-навязывание» и др. К таким приборам можно отнести **TRTD-061, TSU-3000, SI-2002, SCANNER-3, SELSP-31/C, ТСМ-03, ПСЧ-4, РТО-30** и др. Основным недостатком приборов данной группы применительно к телефонной линии является обнаружение узкого класса устройств прослушивания. Контроль сигналов на телефонной линии часто выполняют более сложные многофункциональные приборы (например, **OSCOR-5000, СРМ-700** и др.).

Устройства анализа неоднородности телефонной линии определяют сосредоточенные резистивные или реактивные проводимости, подключенные к линии. Производится это путем измерения параметров сигнала (чаще всего мощности), отраженного от неоднородности линии. Периодически появляющиеся на рынке опытные образцы приборов, реализующие этот принцип (например, **БОР-1**), позволяют определить расстояние до неоднородности. Это, несомненно, является преимуществом данного способа. Однако небольшая дальность обнаружения (реально до 500 м), низкая достоверность (чаще всего за неоднородность принимаются контактные соединения в линии) полученных результатов измерений делают приборы этой группы эффективными только для регистрации «новых» подключений к линии при небольших измеряемых расстояниях. Высокая цена и сложность реализации данного способа обнаружения, ограниченные функциональные и технические возможности опытных образцов приборов препятствуют их распространению на рынке.

Устройства анализа несимметрии линии. Принцип действия прибора основан на определении разности сопротивлений проводов линии по переменному току и определении утечки по постоянному току между проводами линии. Измерения проводятся относительно нулевого провода электросети. Прибор не требует «чистой» линии при работе. Чувствительность его довольно высока для обнаружения практически любых закладок, контактно подключенных к линии. Прибор обнаруживает последовательно включенные прослушивающие устройства с внутренним сопротивлением более 100 Ом, параллельные с током потребления более 0,5 мА. Прибор имеет и ряд недостатков. При изначальной несимметрии линии (например, за счет продолжительной и разветвленной проводки внутри здания, наличия скруток, отводов, контактных соединений и т.п.) приборы данной группы ошибочно указывают на наличие последовательно подключенного прослушивающего устройства. Изменение параметров линии из-за смены климатических условий, «неидеальность» телефонной линии, утечки за счет устаревшего оборудования АТС и т.д. приводят к ошибочному «определению» параллельно подключенного прослушивающего устройства. И, наконец, использование в качестве «третьего» провода нулевой шины электросети при неисправности в приборе может привести к выходу из строя оборудования АТС, телефонной линии. Наиболее распространенными приборами этого класса являются **ТПУ-5** и его современная модификация **ТПУ-7.**

В последние несколько лет на отечественном рынке спецтехники появились **устройства анализа нелинейности параметров линии**, принцип действия которых основан на анализе нелинейности импеданса телефонной линии. В свою очередь в этой группе приборов существуют две подгруппы. Это приборы, определяющие нелинейность двухпроводной обесточенной линии, и приборы, работающие на реальной телефонной линии. Приборы, определяющие нелинейность двухпроводной обесточенной линии **(АТ-2, ВИЗИР** и др.), обладают высокой чувствительностью и позволяют определять практически любые нелинейные устройства съема информации, подключенные к линии. Существенным недостатком таких приборов применительно к телефонной линии является небольшая дальность обнаружения, ограниченная физической доступностью к проводам линии и необходимостью отключения телефонной линии от АТС на время проверки. Эти особенности эксплуатации не позволяют производить оперативный контроль телефонной линии и ограничивают область их применения. Приборы наиболее пригодны для периодических проверок обесточенных отрезков линий (телефонные, электросеть, сигнализация) внутри здания.

Приборы, работающие на реальной телефонной линии **(SELSP-18/T, КТЛ-400)**, обладают меньшей чувствительностью по сравнению с приборами предыдущей подгруппы. Происходит это из-за того, что помехи, специальные сигналы АТС, наводки промышленной частоты, присутствующие на линии, реально не позволяют получить такую же чувствительность. Однако их чувствительность вполне достаточна для обнаружения практически всех известных прослушивающих устройств с питанием от телефонной линии, имеющих нелинейный характер импеданса. С другой стороны, возможность работы на реальной телефонной линии, оперативность проведения контроля (не более 5 минут) без нарушения нормального функционирования линии, максимально возможная дальность обнаружения прослушивающих устройств (от абонентского ТА до АТС), необязательность «чистой» линии на момент подключения прибора, отсутствие зависимости результатов проверки линии от реактивных неоднородностей, некачественных контактов (скруток), утечек тока, делают приборы второй подгруппы наиболее привлекательными при эксплуатации.

К несомненным достоинствам приборов следует отнести их многофункциональность. Анализатор **SELSP-18/T** выполнен как поисковый прибор с автономным питанием и в качестве дополнительных функций определяет «ВЧ-навязывание» и наличие аудиосигналов на линии. В отличие от **SELSP-18/T** контроллеры **КТЛ-3, КТЛ-400** кроме функции поиска выполняют функцию защиты переговоров по линии от утечки информации. Например, **КТЛ-400** полностью автоматизирован, имеет цифровой генератор шума с автоматически перестраиваемым спектром. Прибор оказывает эффективное противодействие параллельным ТА, телефонным закладкам с питанием от линии или внешним питанием, диктофонам, подключенным к линии через контактные или индуктивные съемники, микрофонам и радиомикрофонам с питанием от линии. Кроме этого прибор защищает ТА от аппаратуры «ВЧ-навязывания» и обнаруживает и отключает аппаратуру типа «телефонного уха». **В КТЛ-400** также реализован новый эффективный способ защиты - компенсация постоянного напряжения линии при разговоре, что позволяет полностью отключить параллельные прослушивающие устройства с питанием от линии. Прибор может эксплуатироваться как на городских, так и на местных линиях (с мини АТС). И, наконец, прибор можно использовать для проверки любых двухпроводных обесточенных линий (электросеть, сигнализация и т.д.).

Современные контроллеры телефонных линий, как правило, кроме средств обнаружения подключения к линии устройств несанкционированного съема информации, оборудованы и средствами их подавления. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии. Более подробно об энергетической защите телефонных линий говорится в разделе 3.6.

Таким образом, можно сказать, что на сегодняшний день, несмотря на развитие рынка спецтехники для проверки телефонной линии, не существует универсальной аппаратуры, позволяющей определить подключение к телефонной линии. Более того, индуктивные и емкостные съемники без радиоканала не определяются ни одним прибором из перечисленных групп. Следует учитывать, что наибольшее распространение (до 95%) получили контактно подключенные устройства прослушивания переговоров с радиоканалом и питанием от линии и устройства типа «телефонное ухо». Распространено прослушивание с помощью параллельных ТА, АОНов и автоответчиков. Значительно более сложным организационно, дорогостоящим и, следовательно, менее вероятным следует считать бесконтактное подключение к линии устройств без радиоканала, контактное подключение устройств с высоким входным сопротивлением и внешним питанием без радиоканала, использование аппаратуры «ВЧ-навязывания». Что касается выбора из всех выше перечисленных приборов для проверки телефонной линии, то в каждом конкретном случае пользователь должен исходить из того, какие типы устройств наиболее вероятно могут быть подключены к линии. Следует учитывать место, где они могут быть установлены, и ориентировочную продолжительность их работы.

Модуль 3. Защита информации от утечки по техническим каналам

3.6. Методы и средства защиты информации от утечки по техническим каналам

3.6.1. Основные методы, используемые при создании системы защиты информации от утечки по техническим каналам

Защита информации достигается:

- проектно-архитектурными решениями;
- проведением организационных и технических мероприятий;
- выявлением закладных устройств.

Организационное мероприятие – это мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств. К ним относятся:

- привлечение к проведению работ лицензированных предприятий;
- категорирование и аттестация объектов ТСПИ и ***выделенных помещений***;
- использование на объекте сертифицированных ТСПИ и ВТСС;
- установление контролируемой зоны вокруг объекта;
- организация контроля и ограничение доступа на объекты ТСПИ и в выделенные помещения;
- отключение на период проведения закрытых мероприятий ТС, выполняющих роль электроакустических преобразователей, от проводных линий.

Техническое мероприятие – это мероприятие, предусматривающее применение специальных активных и пассивных технических средств и реализацию технических решений.

К ***техническим мероприятиям с использованием пассивных средств*** относятся:

- контроль и ограничение доступа путем установки ТС и систем ограничения контроля доступа;
- локализация излучений (экранирование ТСПИ и соединительных линий, заземление ТСПИ и экранов соединительных линий, звукоизоляция выделенных помещений);
- развязывание информационных сигналов (установка средств защиты типа «Гранит» в ВТСС, обладающие микрофонным эффектом и имеющие выход за пределы КЗ; установка диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющие выход за пределы КЗ; установка автономных или стабилизированных источников питания ТСПИ; установка в цепях питания помехоподавляющих фильтров).

К техническим мероприятиям с использованием активных средств относятся:

- *пространственное зашумление* (электромагнитное – с помощью генераторов шума или генераторов прицельной помехи; акустическое и виброакустическое; подавление диктофонов в режиме записи);
- *линейное зашумление* (линий электропитания и соединительных линий ВТСС, имеющих выход за пределы КЗ);
- *уничтожение закладных устройств*.

Выявление закладных устройств осуществляется проведением специальных обследований и специальных проверок.

Специальные обследования объектов ТСПИ и выделенных помещений проводятся путем визуального осмотра без применения ТС (или с применением досмотрового оборудования).

Специальная проверка проводится с применением ТС и осуществляется путем:

- *выявления закладных устройств с применением пассивных средств* (установка ТС обнаружения лазерного облучения; установка стационарных обнаружителей диктофонов; поиск закладных устройств с использованием индикаторов поля, интерсепторов, частотомеров, сканерных радиоприемников, программно-аппаратных комплексов контроля; организация контроля ПЭМИН и радиодиапазона – постоянно или периодически, во время проведения конфиденциальных мероприятий);
- *выявления закладных устройств с применением активных средств* (СП выделенных помещений с использованием нелинейных локаторов; СП выделенных помещений, ТСПИ и ВТСС с использованием рентгеновских комплексов).

Рассмотрим основные активные и пассивные технические методы защиты информации.

3.6.2. Методы и средства защиты информации, обрабатываемой ТСПИ

Пассивные методы защиты информации, обрабатываемой ТСПИ, направлены на:

- ослабление информационных ПЭМИ ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средствами разведки на фоне естественных шумов; осуществляется путем **экранирования** и **заземления** ТСПИ и их соединительных линий;
- ослабление наводок ПЭМИ ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средствами разведки на фоне естественных шумов; осуществляется также путем экранирования и заземления ТСПИ и их соединительных линий;
- исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средствами разведки на фоне естественных шумов; достигается путем **фильтрации** информационных сигналов.

Активные методы защиты направлены на:

- создание маскирующих пространственных электромагнитных помех с целью уменьшения соотношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средствами разведки на фоне естественных шумов; достигается применением **систем пространственного зашумления**;
- создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения соотношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средствами разведки на фоне естественных шумов; достигается применением **систем линейного зашумления.**

Экранирование технических средств

Узлы и элементы электронной аппаратуры создают в ближней зоне электромагнитные поля с преобладанием электрической или магнитной составляющей (в зависимости от соотношения величин протекающих в них токов и действующих напряжений) (ПЭМИ). ПЭМИ создаются также в пространстве, окружающем соединительные линии ТСПИ.

ПЭМИ ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки информации, а также возникновения наводок информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня ПЭМИ уделяется большое внимание.

Эффективным методом снижения уровня ПЭМИ является экранирование их источников. Различают электростатическое, магнитостатическое и электромагнитное экранирование, причем на высоких частотах (свыше 100 кГц) применяется исключительно электромагнитное экранирование. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экрана вихревым токам) полем обратного направления.

Экранирование помещений применяется в случаях, когда контролируемая зона от ОТСС превышает размеры контролируемой зоны объекта. Наиболее приемлемым материалом для изготовления экрана всего объема помещения является сталь листовая.

Толщина металлического листа, обеспечивающего необходимую эффективность экранирования, определяется расчетом. Конструкция швов экрана должна обеспечивать надежный электрический контакт с низким переходным сопротивлением высокочастотным токам по периметру соединяемых деталей экрана. Для обеспечения этого требования соединение листов экрана должно производиться герметичным швом электродуговой сварки в среде защитного газа.

Выполнение экранировки требует значительных экономических затрат и большого расхода материалов, весьма трудоемко, сложно в изготовлении входов в помещения вентиляции и вводов коммуникаций. Для выполнения работ по экранировке требуется высокая квалификация исполнителей. При использовании металлических сеток эффективность экранирования значительно меньше.

Кабельные экраны выполняются в форме цилиндра из сплошных оболочек, в виде спирально намотанной на кабель плоской ленты или в виде оплетки из тонкой проволоки. Наиболее экономичным способом экранирования информационных линий связи между устройствами ТСПИ считается групповое размещение их информационных кабелей в экранирующий распределительный короб.

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, то их необходимо скрутить, образовав бифиляр (витую пару).

Наилучшую защиту как от электрического, так и от магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, один из которых используется в качестве экрана), триаксиального кабеля (изолированного коаксиального кабеля, помещенного в электрический экран), экранированного плоского кабеля.

Заземление технических средств

Необходимо отметить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении.

Наиболее часто для заземления используются схемы:

- одноточечные (рис. 6.1 и 6.2);
- многоточечные (рис. 6.3);
- гибридные.

Наиболее проста одноточечная последовательная схема заземления. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях.

Ошибка!

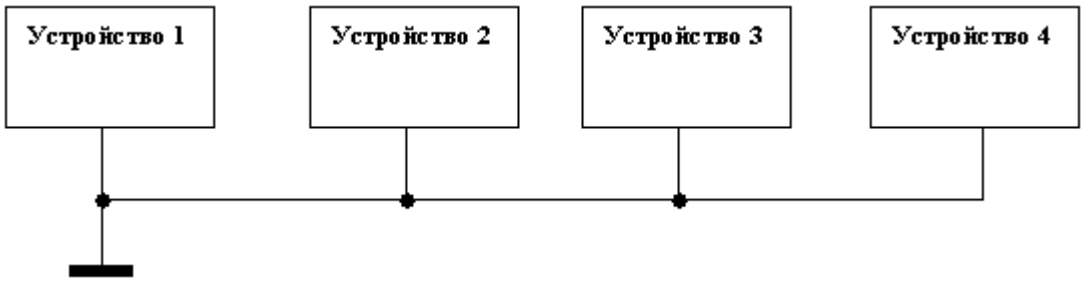


Рис. 6.1. Одноточечная последовательная схема заземления

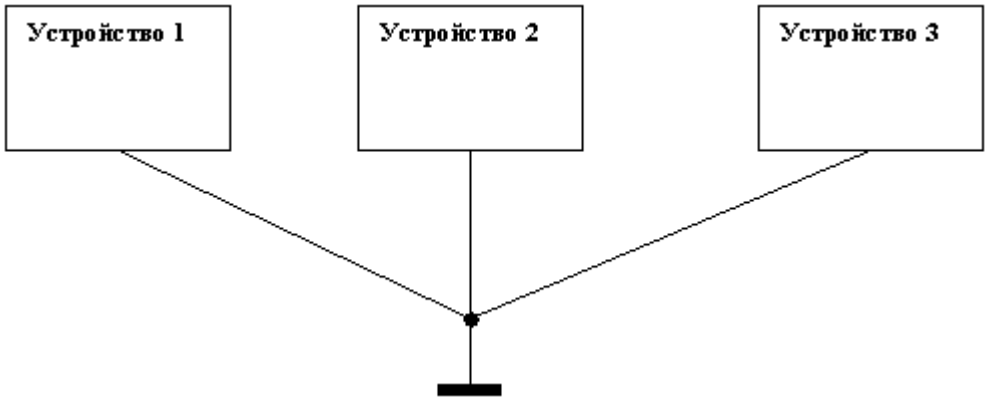


Рис. 6.2. Одноточечная параллельная схема заземления

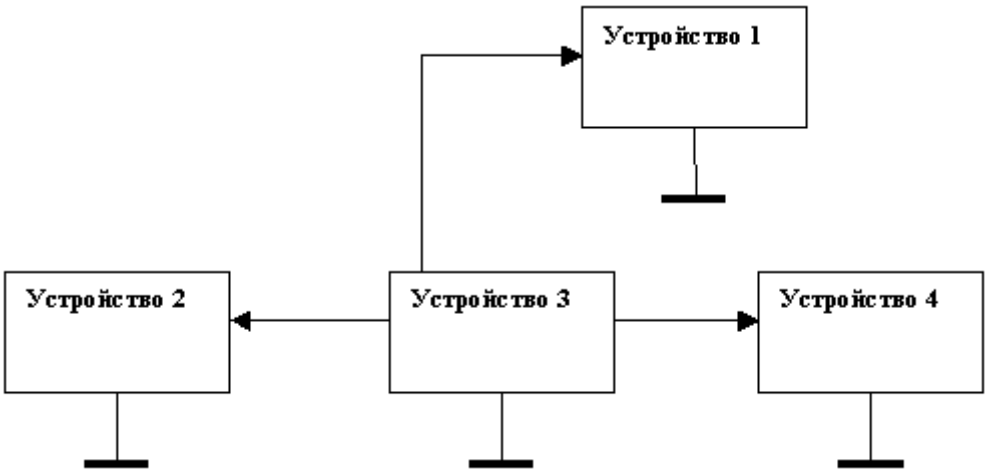


Рис. 6.3. Многоточечная схема заземления

Одноточечная параллельная схема заземления свободна от этого недостатка. Но эта схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи.

Многоточечная схема, в которой все отдельные устройства индивидуально заземлены, является наиболее приемлемой по качеству заземления, но ее реализация требует значительных затрат.

Фильтрация информационных сигналов

Для фильтрации сигналов в цепях питания ТСПИ используются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Такое проникновение возможно из-за наличия нежелательных резистивных и емкостных цепей связи между обмотками.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с минимальным сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (порядка 10 МОм) и незначительной емкости между обмотками. Эти особенности отличают разделительные трансформаторы от обычных.

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ.

Помехоподавляющие фильтры предназначены для ослабления нежелательных сигналов в разных участках частотного диапазона. Различают фильтры верхних и нижних частот, полосовые и заграждающие фильтры.

Основные требования, предъявляемые к помехоподавляющим фильтрам:

- величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
- величина ослабления нежелательных сигналов должна быть не менее требуемой;
- ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

- затухание, вносимое фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая может быть достаточно широкой (до 10 ГГц);

- сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;
- ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими.

В настоящее время промышленностью выпускаются несколько серий защитных фильтров. Их основные характеристики представлены в таблицах 6.1 – 6.2.

Таблица 6.1

Основные характеристики фильтров серии ФП

Наименование характеристик	Тип фильтра					
	ФП-1	ФП-6	ФП-7	ФП-10	ФП-11	ФП-15
Количество проводов	2	2	2	2	2	4
Номинальный ток, А	2,5	20,0	1,0	10,0	16,0	70,0
Номинальное напряжение, В						
- постоянного тока	500	500	250	500	1000	500
- переменного 50 Гц	220	220	110	220	380	220
- переменного 400 Гц	110	110	60	110	110	110
Вносимое затухание	60	60	80	80	100	100

Таблица 6.2

Основные характеристики фильтров серии ФСПК

Наименование характеристик	Тип фильтра	
	ФСПК-100	ФСПК-200
Число фильтруемых проводных линий	2	
Номинальный ток, А	100	200
Напряжение питающей сети 50 Гц, В	220/380	
Частотный диапазон подавления помех, МГц	0,02 … 1000	
Вносимое затухание, дБ	Не менее 60	
Падение напряжения на фильтре при номинальном токе	Не более 5	

Пространственное и линейное зашумление

Реализация пассивных методов защиты, основанных на экранировании и фильтрации, приводит к ослаблению уровней ПЭМИН ТСПИ и тем самым – к уменьшению отношения опасный сигнал/шум (с/ш). Однако возможны ситуации, когда, несмотря на применение пассивных методов и мер защиты, отношение с/ш на границе контролируемой зоны будет превышать допустимое значение. В таких случаях применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

Для исключения перехвата ПЭМИ по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС – линейное зашумление.

К системам пространственного зашумления предъявляются следующие требования:

- система должна создавать электромагнитные помехи в диапазоне частот возможных ПЭМИ ТСПИ;
- создаваемые помехи не должны иметь регулярной структуры;
- уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных ПЭМИ ТСПИ;
- система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией;
- на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать норм по электромагнитной совместимости.

В системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазной помехи».

Системы, реализующие метод «синфазной помехи», применяются в основном для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного

сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру ПЭМИ ПЭВМ.

Системы зашумления типа «белого шума» излучают широкополосный шумовой сигнал (как правило, с равномерно распределенной во всем диапазоне частот энергией), существенно превышающий уровень ПЭМИ. Спектр применения таких систем достаточно широк. Они применяются для защиты ЭВТ, систем звукоусиления, внутреннего телевидения и т.д.

Генераторы шума выполняются или в виде отдельного блока с питанием от сети 220 В, или в виде отдельной платы, вставляемой в свободный слот системного блока ПЭВМ.

Таблица 6.3

Основные характеристики систем пространственного зашумления

Тип (модель)	Наименование характеристик			
	Диапазон частот, МГц	Спектральная плотность мощности шума, дБ	Вид антенны	Конструкция
ГШ-1000М	0,1 … 1000	40 … 75	Рамочная жесткая	Переносной
ГШ-К-1000М	0,1 … 1000	40 … 75	Рамочная мягкая	Бескорпусной
СМОГ	0,00005 … 1000	55 … 80	Подставки под принтер	Бескорпусной
ГНОМ-3	0,01 … 1000	45 … 75	Рамочная гибкая	Стационарный

Таблица 6.4

Основные характеристики систем пространственного и линейного зашумления

Наименование характеристик	Тип (модель)	
	ГРОМ-ЗИ-4	ГНОМ-2С
Диапазон частот, МГц	20 … 1000	0,01 … 1000
Спектральная плотность мощности шума, дБ	40 … 90	50 … 80
Вид антенны	Телескопическая	Рамочная
Конструкция	Переносной	Стационарный

Учитывая вышеизложенное, рекомендуется использовать комплексный метод защиты информации - пассивный и активный одновременно. Такое сочетание методов защиты позволяет максимально использовать возможности каждого из технических средств и, как следствие, минимизировать затраты на их приобретение и монтаж при выполнении предъявленных требований к защите информации от утечки.

3.6.3. Методы и средства защиты речевой информации в помещении

В разделе 2.4.3 дана классификация технических каналов утечки речевой информации: воздушные, структурные и электроакустические каналы. В настоящем разделе рассматриваются методы и средства защиты речевой информации от утечки по воздушным и структурным ТКУИ. Электроакустические каналы возникают в линиях ВТСС (в основном – телефонных) и поэтому требуют специфических методов и средств защиты, которые будут рассмотрены в разделе "Методы и средства защиты телефонных линий".

Пассивные методы защиты акустической (речевой) информации в помещениях направлены на ослабление акустических сигналов на границах контролируемой зоны до величин, обеспечивающих невозможность их выделения средствами разведки на фоне естественных шумов.

Активные методы защиты речевой информации направлены на:

- создание маскирующих акустических (вибрационных) помех с целью уменьшения соотношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного сигнала средствами разведки;
- электромагнитное и ультразвуковое подавление диктофонов в режиме записи;
- создание прицельных радиопомех акустическим радиозакладкам (в том числе - средствам мобильной радиосвязи, используемым в качестве радиомикрофона) с целью уменьшения соотношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного сигнала средствами разведки.

Основой пассивных методов защиты речевой информации является звукоизоляция помещений, активных – использование различного типа генераторов помех и другой специальной техники.

Звукоизоляция помещений

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них и проводится с целью исключения перехвата акустической (речевой) информации по прямому акустическому (через щели, окна, двери, технологические проемы, вентиляционные каналы и т.д.) и вибрационному (через ограждающие конструкции, трубы и т.д.) каналам.

Звукоизоляция оценивается величиной ослабления акустического сигнала, которое для сплошных однослойных или однородных ограждений (строительных конструкций) приближенно рассчитывается по формуле:

$$K \approx 20\lg(c*g_n*f)-47{,}5, \text{ дБ},$$

где

g_n – масса 1 м^3 ограждения, кг;

f - частота звука, Гц;

c – коэффициент пропорциональности, 1/(кг*Гц).

Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов. Одним из наиболее слабых звукоизолирующих элементов являются двери и окна.

Двери имеют существенно меньшие по сравнению со стенами и межэтажными перекрытиями поверхностные плотности и трудноуплотняемые зазоры и щели. Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой дверей специальными материалами. В особо режимных помещениях используются двери с тамбуром, а также специальные двери с повышенной звукоизоляцией (см. таблицу 6.5).

Таблица 6.5

Звукоизоляция специальных дверей

Конструкция двери	Звукоизоляция (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Дверь звукоизолирующая облегченная	18	30	39	42	45	43
Дверь звукоизолирующая облегченная с зазором более 200 мм	25	42	55	58	60	60
Дверь звукоизолирующая тяжелая	24	36	45	51	50	49
Дверь звукоизолирующая тяжелая, двойная с зазором более 300 мм	34	46	60	60	65	65
Дверь звукоизолирующая тяжелая, двойная с облицовкой тамбура	45	58	65	70	70	70

Звукопоглощающая способность окон, так же как и дверей, зависит, главным образом, от поверхностной плотности стекла и степени прижатия притворов. В таблице 6.6 приведены данные по звукоизоляции наиболее распространенных вариантов остекления помещений.

Таблица 6.6

Звукоизоляция окон

Схема остекления	Звукоизоляция (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарное 3 мм	17	17	22	28	31	32
Одинарное 4 мм	18	23	26	31	32	32
Одинарное 6 мм	22	22	26	30	27	25
Двойное 3 мм с промежутком 57 мм	15	20	32	41	49	46
Двойное 3 мм с промежутком 90 мм	21	29	38	44	50	48
Двойное 4 мм с промежутком 57 мм	21	31	38	46	49	35
Двойное 3 мм с промежутком 90 мм	25	33	41	47	48	36

Как видно из таблицы, увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резонансных явлений в воздушных промежутках и эффекта волнового совпадения.

Для повышения звукоизоляции в помещениях применяют **акустические экраны**, устанавливаемые на пути распространения звука на наиболее опасных (с точки зрения разведки) направлениях.

Действие акустических экранов основано на отражении звуковых волн и образовании за экраном звуковых теней. С учетом дифракции эффективность экрана повышается с увеличением соотношения размеров экрана и длины акустической волны. Размеры эффективных экранов превышают более чем в 2 – 3 раза длину волны. Реально достигаемая эффективность акустического экранирования составляет 8 … 10 дБ.

Применение акустического экранирования целесообразно при временном использовании помещения для защиты акустической информации. Наиболее часто применяют складные акустические экраны, используемые для дополнительной звукоизоляции дверей, окон, технологических проемов и других элементов ограждающих конструкций, имеющих звукоизоляцию, не удовлетворяющую действующим нормам.

Широко используются для звукоизоляции помещений **звукопоглощающие материалы.**

Звукопоглощение обеспечивается путем преобразования кинетической энергии акустической волны в тепловую энергию в звукопоглощающем материале. Звукопоглощающие свойства материалов оцениваются коэффициентом звукопоглощения, определяемым отношением энергии звуковых волн, поглощенной в материале, к падающей на поверхность и проникающей в звукопоглощающий материал.

Звукопоглощающие материалы могут быть сплошными и пористыми. Пористые материалы малоэффективны на низких частотах.

Для ведения конфиденциальных переговоров разработаны специальные звукоизолирующие кабины. В зависимости от требований к звукоизоляции они подразделяются на четыре класса (см. таблицу 6.7).

Таблица 6.7.

Характеристики звукопоглощающих кабин

Класс кабины	Звукопоглощение на частотах, дБ	
	Низких (65 Гц)	Высоких (4000 Гц)
I	25	50
II	15	49
III	15	39
IV	15	29

Виброакустическое зашумление

В случае, если используемые пассивные средства защиты помещений не обеспечивают требуемых норм по звукоизоляции, необходимо использовать активные меры защиты. Они заключаются в создании маскирующих акустических помех средствам разведки. Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброакустическому и оптико-электронному каналам утечки информации.

Для формирования акустических помех применяются специальные генераторы, к выходам которых подключены звуковые колонки (громкоговорители), или вибрационные излучатели (вибродатчики). Громкоговорители систем зашумления устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки, а вибродатчики крепятся на рамах, стеклах, коробах, стенах, межэтажных перекрытиях и т.д.

В настоящее время создано большое количество систем активной виброакустической маскировки (в таблице 6.8 приведены характеристики некоторых из них). В состав типовой системы входят шумогенератор и от 6 до 25 вибродатчиков (пьезокерамических или электромагнитных). Дополнительно в состав системы могут включаться звуковые колонки.

Таблица 6.8.
Основные характеристики систем виброакустического зашумления

Наименование характеристик	Модель		
	VNG-006DM	ANG-2000	«Заслон-2М»
Полоса частот эффективной защиты на перекрытии толщиной 0,25 м, кГц	0,25 … 5	0,25 … 5	0,1 … 5
Максимальное количество вибродатчиков, шт	12	18	25
Тип и принцип действия вибродатчиков	КВП-2,КВП-6, КВП-7 пьезокерамические	TRN-2000 электромагнитные	электромагнитные
Эффективный радиус подавления вибродатчика на перекрытии толщиной 0,25 м, м	4	5	1,5
Габариты вибродатчика, мм	40x30, 50x39, 33x8	100x338	46x65x53
Примечания	Подключение спикера	Подключение спикера	Акустопуск. Адаптация к акустическому фону

В комплекс «Барон», кроме обычного генератора шума, включены три радиоприемника, независимо настраиваемые на различные радиовещательные станции. Смешанные сигналы этих станций используются в качестве помехового сигнала, что значительно повышает эффективность помехи.

В ряде систем виброакустической маскировки возможна регулировка уровня помехового сигнала. Например, в системах «Кабинет» и ANG-2000 осуществляется ручная плавная регулировка уровня помехового сигнала, а в системе «Заслон-2М» - автоматическая (в зависимости от уровня маскируемого речевого сигнала). В комплексе «Барон» возможна независимая регулировка уровня помехового сигнала в трех частотных диапазонах с центральными частотами 250, 1000 и 4000 Гц.

Для защиты временно используемых для ведения конфиденциальных переговоров помещений используются мобильные системы виброакустической маскировки. К таким системам относится изделие «Фон-В». В его состав входят: генератор ANG-2000, вибродатчики TRN-2000 и TRN-2000M и металлические штанги для крепления датчиков к строительным конструкциям. Система обеспечивает защиту помещения площадью до 25 м^2. Монтаж и демонтаж системы осуществляется тремя специалистами за 30 минут без повреждения строительных конструкций и элементов отделки интерьера.

Для создания акустических помех в небольших помещениях или в салоне автомобиля могут использоваться малогабаритные акустические генераторы, например, WNG-023. Генератор имеет размеры 111x70x22 мм и создает помеховый акустический сигнал типа «белый шум» в диапазоне частот от 100 до 12000 Гц мощностью 1 Вт. Питание генератора осуществляется от элементов типа «Крона» или сети 220 В.

При организации акустической маскировки необходимо помнить, что акустический шум создает дополнительный мешающий фактор для сотрудников и раздражающе воздействует на нервную систему человека. Степень влияния мешающих помех определяется санитарными нормативами на величину акустического шума.

Методы и средства подавления диктофонов

Рассмотренные в разделе 2.5.5 обнаружители диктофонов сами по себе не решают проблему противодействия несанкционированной звукозаписи, а только позволяют установить факт ее ведения и локализовать в пространстве устройство записи. Кроме того, системы обнаружения диктофонов, как правило, монтируются стационарно и потому неприменимы в тех случаях, когда переговоры ведутся на «чужой» или «нейтральной» территории. Поэтому на практике наряду с системами обнаружения диктофонов эффективно применяются и средства их подавления – электромагнитного или ультразвукового.

Принцип действия **устройств электромагнитного подавления** основан на генерации в дециметровом диапазоне частот (около 900 МГц) мощных шумовых сигналов. Излучаемые

направленными антеннами помеховые сигналы, воздействуя на элементы электронной схемы диктофона (усилитель низкой частоты и усилитель записи), вызывают в них наводки шумовых сигналов. Вследствие этого одновременно с информационным сигналом (речью) осуществляется запись и детектированного шумового сигнала, что приводит к значительным искажениям первого.

Конструктивно подавители диктофонов состоят из генератора, источника питания и антенны. Электромагнитную помеху они излучают направленно: обычно это конус 60-70 градусов, направленный в одну сторону (задний лепесток излучения практически отсутствует). Именно в этой зоне и происходит подавление диктофонов. Направленный сигнал позволяет существенно увеличить напряженность электромагнитного поля в зоне подавления и снизить помехи, наводимые на радиоэлектронную аппаратуру, находящуюся вне зоны подавления (офисная оргтехника, компьютеры, телевизоры и т.д.). Поскольку шумовой сигнал наводится непосредственно во входных цепях, то одинаково хорошо подавляется и другая подслушивающая аппаратура, имеющая в своем составе микрофоны.

Как и для обнаружителей диктофонов, важную роль играет степень экранировки диктофона или другого подслушивающего устройства. Поэтому если диктофоны в пластмассовых корпусах подавляются на расстоянии до 5-6 метров, то в металлических - 2,5-3,5 метра. Применяются в основном два варианта исполнения электромагнитных подавителей: переносной, смонтированный в обычном кейсе, и стационарный, размещаемый в месте переговоров под столом или в ближайшем шкафу. Переносной вариант обязательно оснащен источником автономного питания, которого хватает на 30-60 минут работы. Практически все модели имеют пульт дистанционного включения, некоторые оснащены малогабаритными индикаторами включения подавителя, т.к. внешних проявлений его работы практически нет. Сравнительно недавно появился совсем небольшой прибор - "Шумотрон-4". Его габариты: 200x150x50 вместе с автономным питанием. Прибор можно поместить в барсетку, но работает он всего 15-20 минут, и зона подавления в 1,5-2 раза меньше, чем у традиционных.

Для стационарного варианта используют ту же самую аппаратуру. Ее размещают под столом, а антенну чаще всего крепят к крышке стола снизу, либо ставят непосредственно на стол, что обеспечивает оптимальную зону. Еще одна неприятность - излучение от одной антенны не обеспечивает зону подавления, перекрывающую обычный стол переговоров длиной около 3 м. Для расширения зоны подавления устанавливают вторую антенну ("Шумотрон", "Шторм", "РаМЗес-дубль") либо даже 4 антенны ("Шумотрон"). Двухантенные системы позволяют обеспечить зону подавления вдоль одной, широкой стороны стола переговоров.

Характеристики некоторых систем электромагнитного подавления приведены в таблице 6.9. В графе «Дальность подавления» в числителе – значение для диктофонов в пластмассовом корпусе, в знаменателе – для диктофонов в металлическом корпусе.

Таблица 6.9

Характеристики подавителей диктофонов

Наименование характеристик	Модель					
	Рубеж-1	РаМЗес-Авто	РаМЗес-Дубль	Буран-2	Буран-3	УПД-2
Дальность подавления, м	>1,5/-	>1,5/<1,5	>2/<2	>1,5/-	>3/2	<6/<4
Зона подавления	60^0	60^0	70^0	45^0x45^0	45^0x45^0	80^0
Излучаемая мощность, Вт		5 (AC220) 4 (DC12B)	8	<10	<10	
Питание,	AC220	AC220 DC12	AC220	AC220 DC12	AC220 DC12	AC220 DC12
Время непрерывной работы, час	<1	<1	<1	<2 (AC) <1 (DC)	<2 (AC) <1 (DC)	<1,5 (DC)
Примечания	Стационарный	Стационарный, автомобильный	Стационарный.	В дипломате	В дипломате	В дипломате

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания частотой около 20 кГц, воздействующие непосредственно на микрофоны диктофонов. Это воздействие приводит к перегрузке усилителя низкой частоты

(усилитель начинает работать в нелинейном режиме) и, тем самым, – к значительным искажениям записываемых сигналов.

В отличие от систем электромагнитного подавления подобные системы обеспечивают подавление в гораздо большем секторе. Например, комплекс «Завеса» при использовании двух ультразвуковых излучателей подавляет диктофоны (и акустические закладки) в помещении объемом 27 м^3.

Однако системы ультразвукового подавления имеют два существенных недостатка:

- их эффективность резко снижается, если микрофон прикрыть фильтром из специального материала или на входе усилителя низкой частоты установить фильтр низких частот;
- интенсивность ультразвукового сигнала оказывается выше всех допустимых медицинских норм воздействия на человека. При снижении интенсивности ультразвука невозможно надежно подавить записывающую аппаратуру.

Из-за этих недостатков системы ультразвукового подавления не нашли широкого практического применения.

Методы и средства подавления акустических закладок

Если при проведении радиоконтроля обнаружена передача информации радиозакладкой, а физический поиск ее по тем или иным причинам невозможен, то для предотвращения утечки информации может быть организована постановка прицельных помех на частоте передачи закладки. Для этих целей могут быть использованы устройства АРК-СП или рассмотренные ранее «Скорпион» и «Скорпион-2».

В состав устройства АРК-СП входят широкополосная антенна, перестраиваемый передатчик помех и программное обеспечение. Управляющая программа позволяет с высокой скоростью настраивать передатчик на предварительно заданные частоты в диапазоне 65 … 1000 МГц. Передатчик создает прицельную по частоте помеху с узкополосной и широкополосной модуляцией несущей частоты специальными сигналами: речевая фраза или тональный сигнал. Мощность помехи – 150 …200 мВт. Аппаратура функционирует под управлением ПЭВМ автономно или в составе программно-аппаратных комплексов контроля типа АРК (см. раздел 2.5.7).

Для подавления радиозакладок также могут использоваться системы пространственного электромагнитного зашумления, применяемые для маскировки побочных электромагнитных излучений ТСПИ (таблица 6.3). Однако необходимо помнить, что ввиду относительно низкой спектральной мощности излучаемой помехи, эти системы эффективны для подавления только маломощных (с мощностью излучения до 10 мВт) радиозакладок.

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

Помехоподавляющие фильтры устанавливаются в линии питания розеточной и осветительной сетей в местах их выхода из защищаемого помещения. Учитывая, что сетевые закладки используют для передачи информации частоты свыше 40 … 50 кГц, для защиты информации необходимо использовать фильтры низких частот с граничной частотой не более 40 кГц. К таким фильтрам относятся, например, фильтры ФСПК, граничная частота которых составляет 20 кГц (см. таблицу 6.2).

Системы линейного зашумления подробно рассматриваются в разделе, посвященном методам и средствам защиты телефонных и слаботочных линий.

В качестве радиозакладки могут быть использованы средства мобильной связи, прежде всего – абонентские аппараты систем сотовой телефонной связи. Микрофонная система сотового телефона с приемлемым качеством принимает речевые сигналы в радиусе 3 … 5 м, а передача их может осуществляться на заранее оговоренный стационарный или мобильный телефонный номер, на котором производится их регистрация.

Для предотвращения утечки информации по подобным образом организованному каналу служат так называемые **блокираторы сотовых телефонов**.

Блокиратор представляет собой генератор радиочастот с антенной системой. Излучение производится в диапазоне работы определенных систем мобильной связи, мощность излучения в других диапазонах незначительна. Мобильные телефоны во время работы блокиратора остаются фиксируемыми системой связи, но не обнаруживают сигнала базовой станции, и связь не может быть установлена. Радиус эффективного действия блокиратора зависит от расстояния до ближайшей базовой станции (чем больше расстояние, тем больше радиус действия).

В таблице 6.10 в качестве примера приведены характеристики блокиратора GAMMA, а в таблице 6.11 – краткие описания некоторых моделей современных блокираторов.

Таблица 6.10

Технические характеристики устройства локального блокирования абонентских терминалов радиотелефонной связи GAMMA

Наименование характеристики, параметра	Значение
Диапазон рабочих частот	840-960, 1680-1820 МГц (стандарты GSM,CDMA, AMPS, DAMPS)
Мощность излучения	Не более 200 мВт/диапазон
Радиус действия	3 – 20 м
Питание изделия	AC 220 В, DC 12 В
Потребляемая мощность	Не более 8 ВА
Продолжительность работы от аккумулятора	Не менее 1 часа

Таблица 6.11

Блокираторы абонентских аппаратов систем мобильной радиосвязи

Название	Краткое описание
СКАТ	Для блокирования работы телефонов систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, проведения совещаний.
RS-minijam	Блокиратор сотовой связи с адаптацией к режиму скачков по частоте (Frequency Hopping).
DLW-2000	Для блокирования работы телефонов систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, проведения совещаний. Используется в целях предотвращения утечки информации за пределы выделенного помещения при использовании подслушивающих устройств, работающих с применением каналов систем мобильной связи (сотовых – GSM, AMPS, DAMPS), при использовании для передачи информации включенных телефонов названных стандартов, а также для обеспечения рабочей обстановки во время проведения переговоров, совещания.
МОСКИТ	Миниатюрные устройства обнаружения и подавления сотовых телефонов стандарта GSM 900/1800
HAMMER	Система “Hammer” позволяет обнаруживать включенные сотовые телефоны и блокировать их работу в стандарте сотовой связи GSM 900/1800

3.6.4. Методы и средства защиты телефонных линий

В разделах 2.4.3 и 2.4.4 были рассмотрены каналы утечки речевой информации по различного рода и назначения двухпроводным линиям. Наибольшая угроза для безопасности информации исходит от линий телефонной связи, поэтому ниже основной акцент будет сделан на рассмотрение методов и средств защиты именно телефонных линий. Некоторые из этих методов и средств применимы для защиты иных двухпроводных линий, по которым возможна утечка информации (линий радиотрансляции, охранной и пожарной сигнализации и т.п.).

При организации защиты телефонных линий необходимо учитывать несколько аспектов:

- телефонные аппараты (даже при положенной трубке) могут быть использованы для прослушивания разговоров, ведущихся в помещениях, где они установлены;
- телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания электронных устройств перехвата речевой (акустической) информации, установленных в этих помещениях, а также для передачи перехваченной ими информации;
- возможно прослушивание телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии электронных устройств перехвата речевой информации;
- возможно несанкционированное использование телефонной линии для ведения телефонных разговоров.

Следовательно, методы и средства защиты телефонных линий должны быть направлены на исключение:

- использования телефонных линий для прослушивания разговоров, ведущихся в помещениях, через которые проходят эти линии;
- прослушивания телефонных разговоров, ведущихся по данным телефонным линиям;
- несанкционированного использования телефонных линий для ведения телефонных разговоров.

В разделе 2.4.3 уже упоминалось, что прослушивание разговоров, ведущихся в помещениях, возможно за счет электроакустических преобразований, возникающих в ВТСС. К ним относятся и элементы телефонного аппарата: звонковая цепь, телефонный, микрофонный капсюли и т.д. Сейчас физика образования опасных сигналов в них будет рассмотрена несколько подробнее.

При положенной трубке телефонный и микрофонный капсюли гальванически отключены от телефонной линии, и информационные сигналы возникают в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

Перехват возникающих в элементах звонковой цепи информационных сигналов возможен путем гальванического подключении к телефонной линии специальных высокочувствительных низкочастотных усилителей (рис. 6.4). Однако вследствие малой амплитуды сигналов, дальность перехвата информации, как правило, не превышаем нескольких десятков метров.

Для повышения дальности перехвата информации низкочастотный усилитель подключают к линии через устройство анализа состояния телефонной линии, включаемое в разрыв телефонной линии (рис. 6.5). Данное устройство при положенной трубке телефонного аппарата отключает линию от АТС (сопротивление развязки составляет более 20 МОм), подключает специальный низкочастотный усилитель и переходит в режим анализа поднятия телефонной трубки и наличия сигналов вызова. При получении сигналов вызова или поднятии телефонной трубки устройство отключает специальный низкочастотный усилитель и подключает телефонный аппарат к линии АТС.

Рис. 6.4 Схема подключения специальных низкочастотных усилителей к телефонной линии через адаптер

Вследствие отключения телефонного аппарата от линии в момент съема информации значительно уменьшается уровень шумов в линии и, следовательно, повышается дальность перехвата информации.

Рис. 6.5 Схема подключения низкочастотного усилителя к телефонной линии через специальное устройство анализа состояния телефонной линии

Второй способ повышения дальности перехвата информации заключается в использовании метода “высокочастотного навязывания”, который может быть осуществлен путем контактного введения токов высокой частоты от генератора, подключенного в телефонную линию. Частота сигнала “навязывания” может составлять от 30 кГц до 10 МГц и более. Благодаря высокой частоте сигнал “навязывания” проходит не только в звонковую, но и в микрофонную и телефонную цепи и модулируется информационным сигналом, возникающим вследствие акустоэлектрических преобразований. В силу того, что нелинейные или параметрические элементы телефонного аппарата для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный речевым сигналом высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии. Отраженный высокочастотный сигнал принимается и обрабатывается специальным приемным устройством, также подключаемым к телефонной линии (рис. 6.6). Устройство анализа состояния телефонной линии выполняет функции, рассмотренные выше.

Дальность перехвата информации при использовании метода "высокочастотного навязывания" может составлять несколько сот метров.

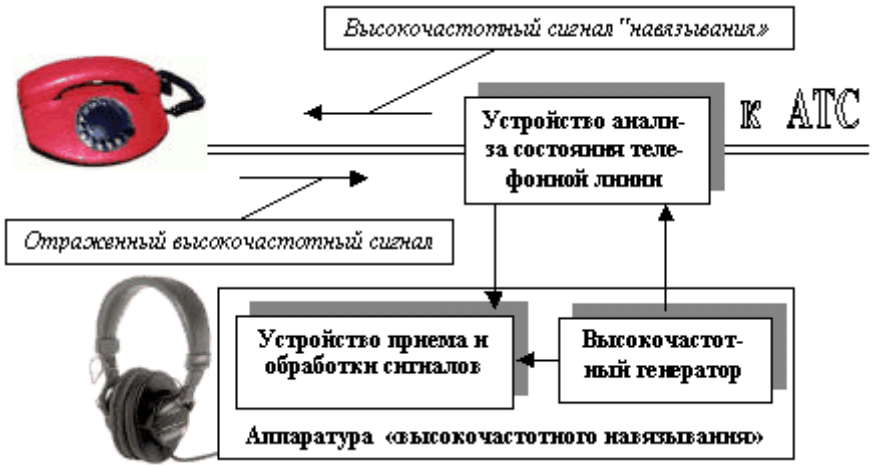


Рис.6.6 Схема реализации метода “высокочастотного навязывая”

Для защиты телефонного аппарата от утечки речевой информации по электроакустическому каналу используются как пассивные, так и активные методы и средства.

К наиболее широко применяемым **пассивным методам защиты** относятся:

- ограничение опасных сигналов;
- фильтрация опасных сигналов;
- отключение источников (преобразователей) опасных сигналов.

Возможность **ограничения опасных сигналов** основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используются два встречновключенных диода, имеющих вольтамперную характеристику (зависимость значения протекающего по диоду электрического тока от приложенного к нему напряжения), показанную на рис. 6.7. Такие диоды имеют большое сопротивление (сотни кОм) для токов малой амплитуды и единицы Ом и менее – для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияния на прохождение через диоды полезных сигналов.

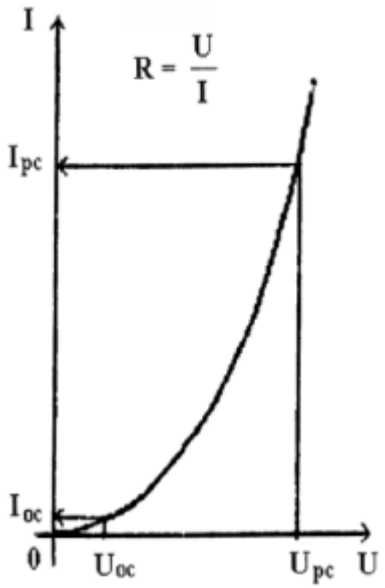


Рис. 6. 7. Вольтамперная характеристика диода VD

Диодные ограничители включаются последовательно в линию звонка (рис. 6.8, б) или непосредственно в каждую из телефонных линий (рис. 6.8, а).

Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от "высокочастотного навязывания".

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов (рис. 5). Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного “навязывания” и не оказывать существенного влияния на полезные сигналы. Обычно для установки в звонковую цепь используются конденсаторы, емкостью 1 мкФ, а для установки в микрофонную цепь - 0,01 мкФ. Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах.

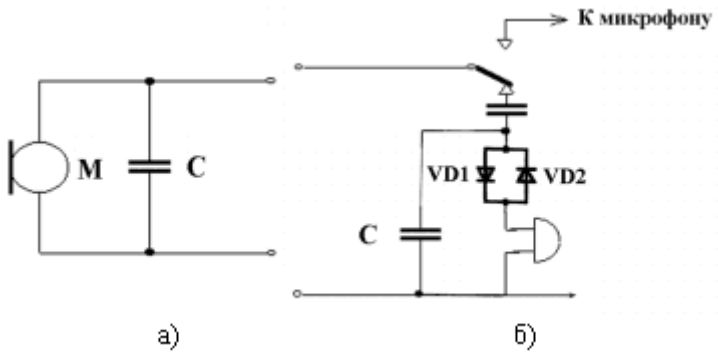


Рис. 6.8. Схемы защиты микрофона (а) и звонковой цепи (б) телефонного аппарата

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель. К ним относятся устройства типа "Экран", "Гранит-8", "Грань-300" и др. (рис. 6.9). Эти устройства обеспечивают подавление информационного низкочастотного сигнала

более чем на 80 дБ и вносят затухание для высокочастотных сигналов в полосе частот от 30 кГц до 30 МГц более 70 дБ.

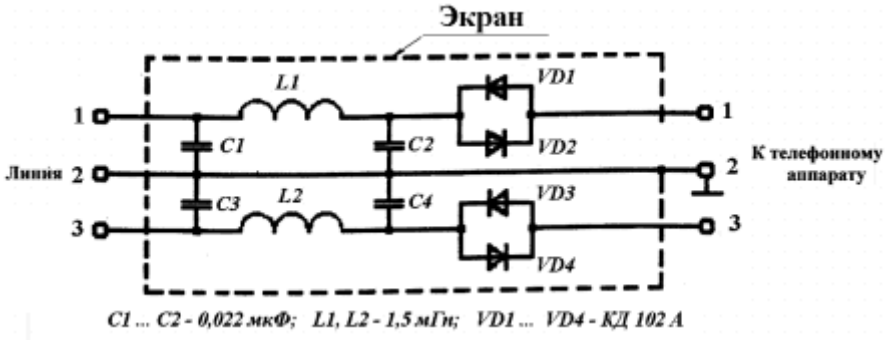


Рис. 6.9. Схема устройства защиты телефонных аппаратов типа "Гранит-8"

Отключение телефонных аппаратов от линии при ведении в помещении конфиденциальных разговоров является наиболее эффективным методом защиты информации. Самый простой способ реализации этого метода защиты заключается в установке в корпусе телефонного аппарата или телефонной линии специального выключателя, включаемого и выключаемого вручную. Более удобным в эксплуатации является установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке.

К типовым устройствам, реализующим данный метод защиты, относится изделие "Барьер-М1". Устройство имеет следующие режимы работы: дежурный режим, режим передачи сигналов вызова и рабочий режим.

В дежурном режиме (при положенной телефонной трубке) телефонный аппарат отключен от линии и устройство находится в режиме анализа поднятия телефонной трубки и наличия сигналов вызова. При этом сопротивление развязки между телефонным аппаратом и линией АТС составляет не менее 20 МОм.

При получении сигналов вызова устройство переходит в режим передачи сигналов вызова, при котором через электронный коммутатор телефонный аппарат подключается к линии. Подключение осуществляется только на время действия сигналов вызова.

При поднятии телефонной трубки устройство переходит в рабочий режим и телефонный аппарат подключается к линии.

Изделие устанавливается в разрыв телефонной линии, как правило, при выходе ее из выделенного (защищаемого) помещения или в распределительном щитке (кроссе), находящемся в пределах контролируемой зоны.

Использование средств защиты типа “Барьер-М1” наряду с защитой информации от утечки по электроакустическому каналу является практически единственным методом борьбы с электронными устройствами перехвата речевой информации, использующим телефонную линию в качестве источника питания.

Активные методы защиты телефонных аппаратов от утечки информации по электроакустическому каналу заключаются в подаче в телефонную линию при положенной телефонной трубке маскирующего низкочастотного (диапазон частот от 100 Гц до 10 кГц) шумового сигнала (**метод низкочастотной маскирующей помехи**).

Устройства защиты, реализующие метод низкочастотной маскирующей помехи, часто называют средствами линейного зашумления. Они подключаются в разрыв телефонной линии, как правило, непосредственно у корпуса телефонного аппарата (рис.6.10). Шумовой сигнал подается в линию в режиме, когда телефонный аппарат не используется (трубка положена). При снятии трубки телефонного аппарата подача в линию шумового сигнала прекращается.

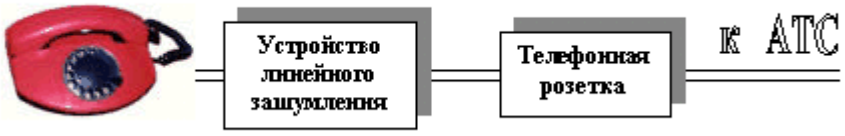


Рис. 6.10. Схема подключения средств линейного зашумления

К сертифицированным средствам линейного зашумления относятся устройства типа МП-1А (защита аналоговых телефонных аппаратов) и МП-1Ц (защита цифровых телефонных аппаратов) и др.

Наряду с электроакустическими каналами утечки информации для прослушивания разговоров в помещениях могут использоваться электронные устройства перехвата речевой (акустической) информации, использующие телефонную линию в качестве канала передачи информации. При этом передача информации может осуществляться как на низких (в речевом диапазоне частот), так и на высоких частотах (от 40 кГц до 10 МГц и более).

Для передачи информации по телефонной линии на низких частотах используются микрофонные проводные системы и устройства типа “телефонное ухо”.

Типовое электронное устройство перехвата информации включает: микрофон, микрофонный усилитель, электронный коммутатор и устройство анализа состояния телефонной линии (рис. 6.11).

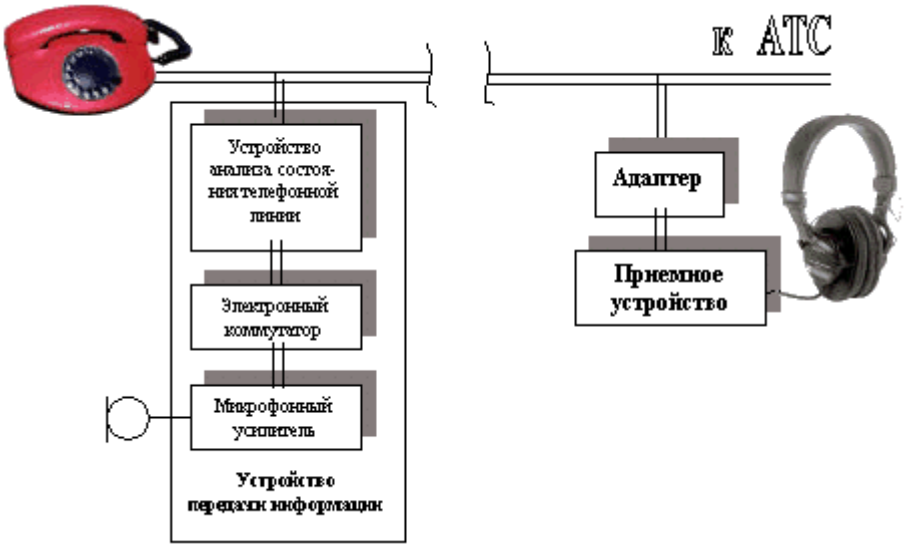


Рис. 6.11. Схема микрофонной проводной системы, использующей для передачи информации телефонную линию

Электронный коммутатор и устройство анализа состояния телефонной линии используются для исключения возможности обнаружения факта подключения закладного устройства к телефонной линии по наличию в ней посторонних сигналов при ведении телефонных разговоров. Устройство анализа контролирует состояние телефонной линии и при положенной телефонной трубке через электронный коммутатор подключает выход микрофонного усилителя к телефонной линии. При поднятии телефонной трубки микрофонный усилитель от телефонной линии отключается. В качестве приемного устройства в системе могут использоваться низкочастотный усилитель или портативное устройство регистрации речевой информации (магнитофон, диктофон, устройства записи на основе использования цифровых методов звукозаписи), подключаемые к линии с помощью специального адаптера.

Дальность передачи информации при использовании проводных микрофонных систем составлять несколько километров.

Схема перехвата информации с использованием устройств типа “телефонное ухо” показана на рис. 6.12.

В данной системе в качестве устройства дистанционного управления используется обычный телефонный аппарат (возможно использование аппаратов сотовой связи).

Принцип работы устройства передачи информации заключается в следующем. После набора номера “телефона-наблюдателя”, к линии которого подключено устройство, абонент переключает телефонный аппарат в тональный режим и осуществляет набор кодового числа. При отсутствии у телефонного аппарата режима тонового набора, для трансляции в линию кодированного звукового (тонального) сигнала используется специальное кодовое устройство (это устройство часто называют “бипером”). В момент передачи кодированного сигнала “бипер” подносится к микрофону телефонной трубки. Устройство анализа состояния линии закладки при приеме кодированного сигнала подавляет сигналы вызова, что обеспечивает скрытность работы устройства. При совпадении принятого кодового сигнала с записанным в память дешифратора, электронный коммутатор шунтирует телефонную линию сопротивлением 600 Ом. При этом АТС переключает “телефон-наблюдатель” на прием-передачу информации и в линию подается сигнал с выхода микрофонного усилителя, что обеспечивает звонящему абоненту возможность прослушивания разговоров, ведущихся в комнате, где установлено устройство.

При поднятии трубки “телефона-наблюдателя” микрофонный усилитель от телефонной линии отключается.

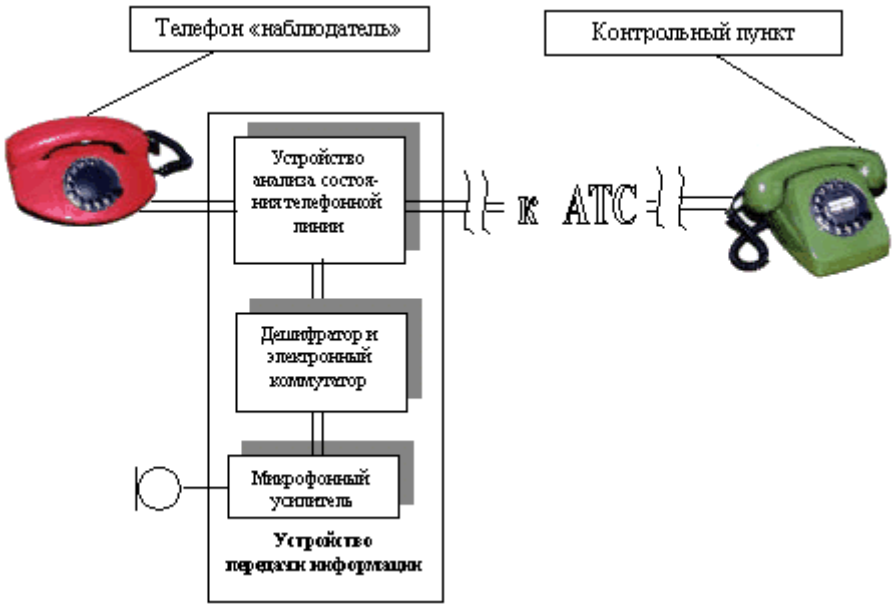


Рис. 6.12. Схема перехвата информации с использованием устройств типа “телефонное ухо”

В отличие от проводных микрофонных систем в системе перехвата информации с использованием устройств типа “телефонное ухо” дальность передачи информации практически не ограничена.

Как правило, питание устройств передачи информации осуществляется от телефонной линии.

Схема системы передачи информации по телефонной линии на высокой частоте представлена на рис. 6.13. Фактически устройство представляет собой радиопередатчик, в качестве антенны которого используется телефонный провод. Наибольшая дальность передачи информации обеспечивается при использовании частот от 200 до 600 кГц. При передаче используется сигналы с частотной модуляцией.

Дальность передачи информации при использовании подобных систем составлять несколько километров. Но при этом передача информации, в отличие от проводных микрофонных систем, возможна не только по незанятой телефонной линии, так и при ведении телефонных разговоров по ней.

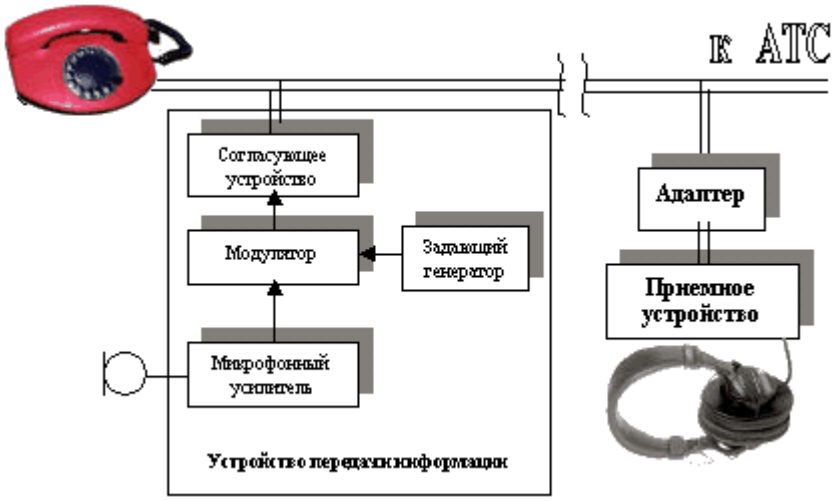


Рис. 6.13. Схема системы передачи информации по телефонной линии на высокой частоте

Питание закладных устройств с передачей информации по телефонной линии на высокой частоте может осуществляться как от телефонной линии, так и от автономных источников питания.

С целью защиты речевой информации от перехвата устройствами, использующими телефонную линию в качестве канала передачи информации, применяются пассивные и активные методы и средства защиты.

Из **пассивных средств защиты** в основном используются устройства типа “Барьер-М1”, принцип работы которых рассмотрен выше.

К **активным методам защиты** можно отнести:

- метод низкочастотной маскирующей помехи;
- метод высокочастотной широкополосной маскирующей помехи.

Метод низкочастотной маскирующей помехи аналогичен рассмотренному выше. Метод высокочастотной широкополосной маскирующей помехи заключаются в подаче в телефонную линию при положенной телефонной трубке маскирующего высокочастотного широкополосного (в диапазоне часто от 20 кГц до 30 МГц) шумового сигнала.

Прослушивание телефонных разговоров осуществляется с использованием электронных устройств перехвата речевой информации, подключаемых к телефонным линиям последовательно (в разрыв одного из проводов), параллельно (одновременно к двум проводам) и с помощью индукционного датчика (бесконтактное подключение). Основные схемы подключения устройств перехвата информации приведены на рис. 6.14 – 16.

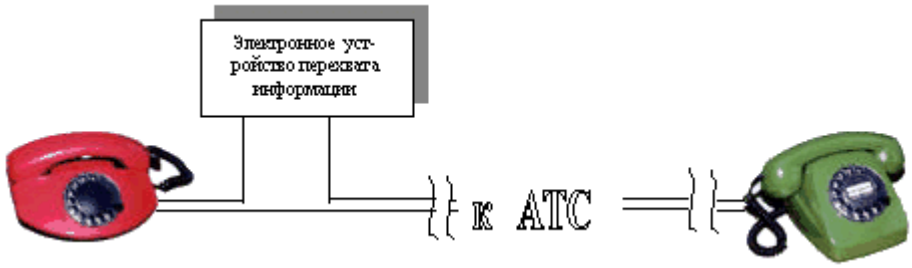


Рис.6. 14. Схема последовательного подключения электронного устройства перехвата речевой информации к телефонной линии

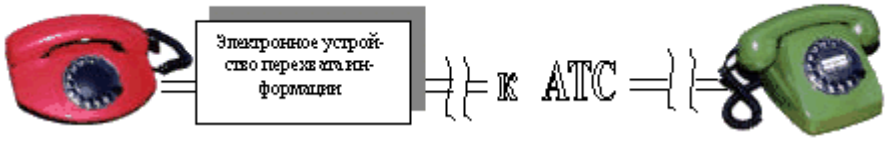
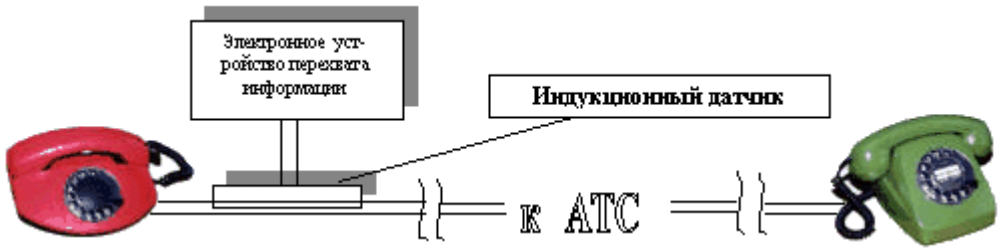


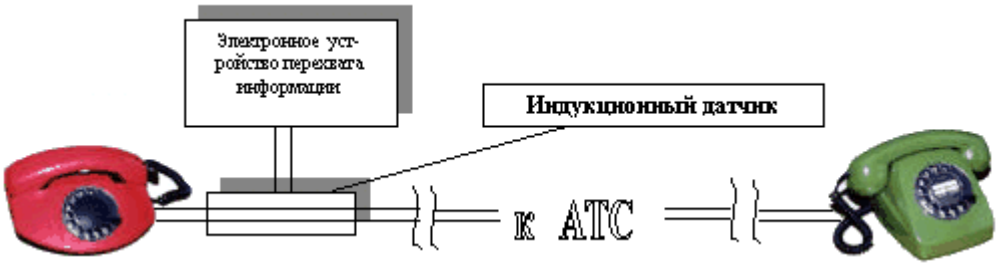
Рис. 6.15. Схема параллельного подключения электронного устройства перехвата речевой информации к телефонной линии

Питание электронных устройств перехвата речевой информации при последовательном и параллельном подключении осуществляется от телефонной линии, а при бесконтактном – от автономного источника тока. Получаемая информация передается, как правило, по радиоканалу. Радиопередающее устройство активизируется только на время телефонного разговора. Кроме того, устройство может осуществлять запись речевой информации на магнитный носитель. При этом устройство записи активизируется только в процессе ведения телефонного разговора.

Защита информации, передаваемой по телефонным линиям связи, может осуществляться на **семантическом** и **энергетическом** уровнях. Методы защиты информации на энергетическом уровне направлены на исключение (затруднение) приема противником (злоумышленником) непосредственно информационных сигналов путем уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством несанкционированного съема информации.



а) при подключению к одному из проводов



б) при подключении к двум проводам

Рис. 6.16. Схемы подключения электронного устройства перехвата речевой информации к телефонной линии с использованием индукционного датчика

При защите телефонных разговоров на энергетическом уровне осуществляется подавление электронных устройств перехвата информации с использованием активных методов и средств, к основным из которых относятся:

- метод синфазной низкочастотной маскирующей помехи;
- метод высокочастотной маскирующей помехи;
- метод “ультразвуковой” маскирующей помехи;
- метод повышения напряжения;
- метод "обнуления";
- метод низкочастотной маскирующей помехи;
- компенсационный метод;
- метод "выжигания".

Суть **метода синфазной маскирующей низкочастотной помехи** заключается в подаче во время разговора в каждый провод телефонной линии с использованием единой системы заземления аппаратуры АТС и нулевого провода электросети 220 В (нулевой провод электросети заземлен) согласованных по амплитуде и фазе маскирующих помеховых сигналов речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала от 300 до 3400 Гц) . В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не оказывают мешающего воздействия на полезный сигнал (телефонный разговор). Если же информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А так как его уровень значительно превосходит полезный сигнал, то перехват информации (выделение полезного сигнала) становится невозможным.

В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные последовательности импульсов) речевого диапазона частот.

Метод синфазной маскирующей низкочастотной помехи используется для подавления:

- электронных устройств перехвата речевой информации с телефонных линий с передачей информации по радиоканалу (такие устройства частот называют телефонными ретрансляторами или телефонными радиозакладками), подключаемых к телефонной линии последовательно (в разрыв одного из проводов);
- телефонных радиозакладок, диктофонов и устройств записи на основе использования цифровых методов, подключаемых к одному из проводов телефонной линии с помощью индукционного датчика.

Метод **высокочастотной маскирующей помехи** заключается в подаче во время разговора в телефонную линию широкополосного (ширина спектра помехового сигнала составляет несколько кГц) маскирующего помехового сигнала в диапазоне высоких частот звукового диапазона (то есть в диапазоне выше частот стандартного телефонного канала).

Частоты маскирующих помеховых сигналов подбираются таким образом, чтобы после прохождения селективных цепей модулятора радиозакладки или микрофонного усилителя диктофона их уровень оказался достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии во время разговоров абонентов), но в то же время эти сигналы не ухудшали бы качество телефонных разговоров. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешающее воздействие он оказывает на полезный сигнал. Обычно

используются частоты в диапазоне от 6 – 8 кГц до 16 – 20 кГц. Например, в устройстве Sel SP-17/D помеха создается в диапазоне 8 – 10 кГц.

Для исключения воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты устанавливается специальный низкочастотный фильтр с граничной частотой выше 3,4 кГц, подавляющий (шунтирующий) помеховые сигналы и не оказывающий существенного влияния на прохождение полезных сигналов. Аналогичную роль выполняют полосовые фильтры, установленные на городских АТС, пропускающие сигналы, частоты которых соответствуют стандартному телефонному каналу, и подавляющие помеховый сигнал.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы типа "белого шума" или дискретные сигналы типа псевдослучайной последовательности импульсов.

Данный метод используется для подавления практически всех типов электронных устройств перехвата речевой информации как контактного (последовательного и параллельного) подключений к линии, так и бесконтактного подключения к линии с использованием индукционных датчиков различного типа. Однако эффективность подавления средств съема информации с подключением к линии при помощи индукционных датчиков (особенно, не имеющих предусилителей) значительно ниже, чем средств с гальваническим подключением к линии.

У телефонных радиозакладок с параметрической стабилизацией частоты как последовательного, так и параллельного включения наблюдается "уход" несущей частоты, что может привести к потере канала приема.

Типовые спектрограммы излучения телефонных радиозакладок в условиях маскирующих высокочастотных помех приведены на рис. 6.17 и 6.18.

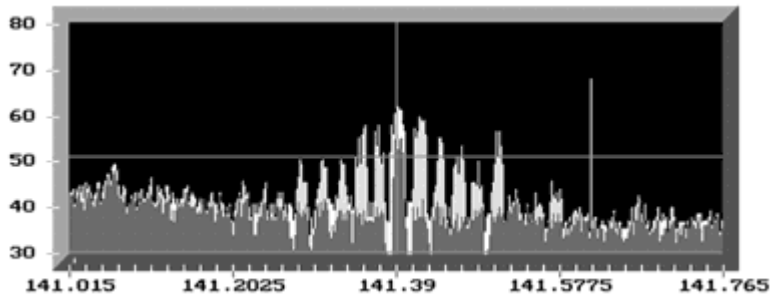


Рис. 6.17. Спектрограмма излучения телефонной радиозакладки с кварцевой стабилизацией частоты и узкополосной частотной модуляцией в условиях маскирующих высокочастотных помех, создаваемых устройством УЗТ-01.

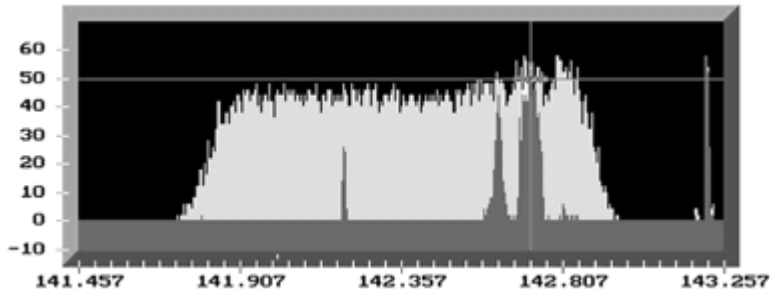


Рис. 6.18. Спектрограмма излучения телефонной радиозакладки с параметрической стабилизацией частоты и широкополосной частотной модуляцией при выключенном (темно-серый тон) и включенном (светло-серый тон) устройстве УЗТ-01

Метод “**ультразвуковой” маскирующей помехи** в основном аналогичен рассмотренному выше. Отличие состоит в том, что используемые частоты помехового сигнала находится в диапазоне от 20 – 25 кГц до 50 – 100 кГц.

Метод повышения напряжения заключается в поднятии напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных радиозакладок за счет перевода их передатчиков в нелинейный режим работы. Поднятие напряжения в линии до 18 – 24 В вызывает у телефонных радиозакладок с последовательным подключением и параметрической стабилизацией частоты "уход" несущей частоты и ухудшение разборчивости речи вследствие “размытия” спектра сигнала. У телефонных радиозакладок с последовательным подключением и кварцевой стабилизацией частоты наблюдается уменьшение отношения сигнал/шум на 3 – 10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде случаев просто отключаются.

Метод "обнуления" предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Этот метод используется для нарушения функционирования электронных устройств перехвата информации с контактным подключением к линии и использующих ее в качестве источника питания. К таким устройствам относятся параллельные телефонные аппараты и телефонные радиозакладки.

Метод низкочастотной маскирующей помехи заключается в подаче в линию при положенной телефонной трубке маскирующего низкочастотного помехового сигнала и применяется для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматыванию пленки в режиме записи шума (то есть при отсутствии полезного сигнала).

Компенсационный метод используется для маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии, и обладает высокой эффективностью подавления всех известных средств несанкционированного съема информации.

Суть метода заключается в следующем: при передаче скрываемого сообщения на приемной стороне в телефонную линию при помощи специального генератора подается маскирующая помеха (цифровой или аналоговый маскирующий сигнал речевого диапазона с известным спектром). Одновременно этот же маскирующий сигнал ("чистый" шум) подается на один из входов двухканального адаптивного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет полезный сигнал, который подается на телефонный аппарат или устройство звукозаписи.

Метод "выжигания" реализуется путем подачи в линию высоковольтных (напряжением более 1500 В) импульсов, приводящих к электрическому "выжиганию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

При использовании данного метода телефонный аппарат от линии отключается. Подача импульсов в линию осуществляется два раза. Первый (для "выжигания" параллельно подключенных устройств) – при разомкнутой телефонной линии, второй (для "выжигания" последовательно подключенных устройств) – при закороченной (как правило, в центральном распределительном щитке здания) телефонной линии.

Для защиты телефонных линий используются как простые устройства, реализующие один метод защиты, так и сложные, обеспечивающие комплексную защиту линий различными методами, включая защиту от утечки информации по электроакустическому каналу.

На отечественном рынке имеется большое разнообразие средств защиты. Среди них можно выделить следующие: SP 17/D, SI-2001, "КТЛ-3","КТЛ-400", "Ком-3", "Кзот-06", "Цикада-М" (NG –305), "Прокруст" (ПТЗ-003), "Прокруст-2000", "Консул", "Гром-ЗИ-6", "Протон" и др. Основные характеристики некоторых из них приведены в табл. 6.12.

В активных устройствах защиты телефонных линий наиболее часто реализованы метод высокочастотной маскирующей помехи (SP 17/D, "КТЛ-3","КТЛ-400", “СКИТ”, "Ком-3", "Прокруст" (ПТЗ-003), "Прокруст-2000","Гром-ЗИ-6", "Протон" и др.) и метод ультразвуковой маскирующей помехи ("Прокруст" (ПТЗ-003), "Гром-ЗИ-6").

Метод синфазной низкочастотной маскирующей помехи используется в устройстве "Цикада-М", а метод низкочастотной маскирующей помехи –- в устройствах SP 17/D, "Прокруст", "Протон", "Кзот-06" и др.

Метод "обнуления" применяется, например, в устройстве "Цикада-М", а метод повышения напряжения в линии – в устройстве "Прокруст".

Компенсационный метод маскировки речевых сообщений, передаваемых по телефонной линии, реализован в изделиях "Туман", “Щит” (односторонняя маскировка) и “Ирис” (двухсторонняя маскировка).

Устройства защиты телефонных линий имеют сравнительно небольшие размеры и вес (например, изделие "Прокруст" при размерах 62х155х195 мм весит 1 кг). Питание их, как правило, осуществляется от сети переменного тока 220 В. Однако некоторые устройства (например, "Кзот-06") питаются от автономных источников питания.

Таблица 6.12

Основные характеристики устройств активной защиты телефонных линий

Наименование характеристик	Тип устройства					
	"Прокруст" ПТЗ - 003	"Протон"	"Цикада-М" (NG – 305)	Sel SP - 17/D	Гром-ЗИ-6	Кзот-06
Метод синфазной низкочастотной маскирующей помехи	-	-	+	-	-	-
Метод высокочастотной маскирующей помехи		+	-	+	+	+
Метод ультразвуковой маскирующей помехи	+		+	-	+	
Метод повышения напряжения	+		-	-	-	
Метод "обнуления"	-	-	·	-	-	
Метод низкочастотной маскирующей помехи	+	+	-	+	-	+
Метод "выжигания"	-	-	-	-	-	-
Индикация	световая	световая	световая	световая	световая, звуковая	световая
Габаритные размеры, мм	157х64х205	205х60х285	155х60х200	152х34х104	150х50х200	210х32х85
Вес, кг	1	2,3	-	0,6	1,5	0,75
Напряжение питания, В	220	220	220	220/12	220	9
Примечание	Цифровая индикация напряжения в линии	Цифровая индикация напряжения в линии		Частотный диапазон ВЧ–помехи: 8– 10 кГц; НЧ–помехи: 0,3– 3 кГц.	Цифровая индикация уменьшения напряжения в линии	Цифровая индикация напряжения в линии

Для вывода из строя ("выжигания" входных каскадов) средств несанкционированного съема информации с гальваническим подключением к телефонной линии используются устройства типа "ПТЛ-1500", "КС-1300", "КС-1303", "Кобра" и т.д. Их основные характеристики приведены в табл. 6.13.

Таблица 6.13

Основные характеристики "выжигателей" телефонных закладных устройств

Наименование характеристик	Тип устройства		
	"Кобра"	КС-1300	КС-1303
Напряжение на выходе, В	1600		
Мощность импульса, ВА		15	50
Режимы работы	Автоматический Ручной	Автоматический Ручной	Ручной
Время непрерывной работы в автоматическом режиме	20 с	24 часа	-
Время непрерывной работы в ручном режиме	10 мин		
Временные интервалы, устанавливаемые таймером		от 10 мин до 2 суток	
Габаритные размеры, мм	65x170x185	170x180x70	170x180x70
Напряжение питания, В	220	220	220
Количество подключаемых телефонных линий	1	2	2

Приборы используют высоковольтные импульсы напряжением не менее 1500 – 1600 В. Мощность "выжигающих" импульсов составляет 15 – 50 ВА. Так как в схемах закладок применяются миниатюрные низковольтные детали, то высоковольтные импульсы их пробивают, и схема закладки выводится из строя.

"Выжигатели" телефонных закладок могут работать как в ручном, так и автоматическом режимах. Время непрерывной работы в автоматическом режиме составляет от 20 секунд до 24 часов.

Устройство "КС-1300" оборудовано специальным таймером, позволяющим при работе в автоматическом режиме устанавливать временной интервал подачи импульсов в линию в пределах от 10 минут до 2 суток.

Наряду с защитой телефонных линий от подслушивания необходимо исключить **несанкционированное использование телефонной линии** для ведения телефонных разговоров. Для этих целей используются: метод блокировки набора номера и метод низкочастотной маскирующей помехи.

Для **блокировки работы (набора номера)** несанкционированно подключенных **параллельных телефонных аппаратов** используются **специальные электронные блокираторы**. Принцип работы подобных устройств поясним на примере изделия "Рубин". В дежурном режиме устройство производит анализ состояния телефонной линии путем сравнения напряжения в линии и на эталонной (опорной) нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированно подключенного параллельного телефонного аппарата напряжение в линии уменьшается, что фиксируется устройством защиты. Если этот факт зафиксирован в момент ведения телефонного разговора (трубка на защищаемом телефонном аппарате снята), срабатывает звуковая и световая (загорается светодиод несанкционированного подключения к линии) сигнализация. А если факт несанкционированного подключения к линии зафиксирован в отсутствии телефонного разговора (трубка на защищаемом телефонном аппарате не снята), то срабатывает сигнализация и устройство защиты переходит в режим блокирования набора номера с параллельного телефонного аппарата. В этом режиме устройство защиты шунтирует телефонную линию сопротивлением 600 Ом (имитируя снятие трубки на защищаемом телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата.

Использование **метода низкочастотной маскирующей помехи**, рассмотренного ранее, исключает возможность не только набора номера, но и ведения разговора с параллельного телефонного аппарата.

На **семантическом** уровне защита информации достигается применением криптографических методов и средств защиты и направлена на исключение ее получения (выделения), даже при перехвате противником (злоумышленником) информационных сигналов.

Преобразование должно придавать информации вид, исключающий ее восприятие при использовании аппаратуры, стандартной для данного канала связи. При использовании же специальной аппаратуры восстановление исходного вида информации должно требовать затрат времени и средств, которые по оценке владельца защищаемой информации делают бессмысленным для злоумышленника вмешательство в информационный процесс.

Основные используемые в настоящее время методы преобразования речевого сигнала и их взаимосвязь показана на рис. 6.19. Часто в литературе эти методы называют криптографическими. В рамках данного пособия нет возможности рассмотреть математические и технические аспекты реализации каждого из представленных на рисунке методов, поэтому ограничимся лишь наиболее общими характеристиками.

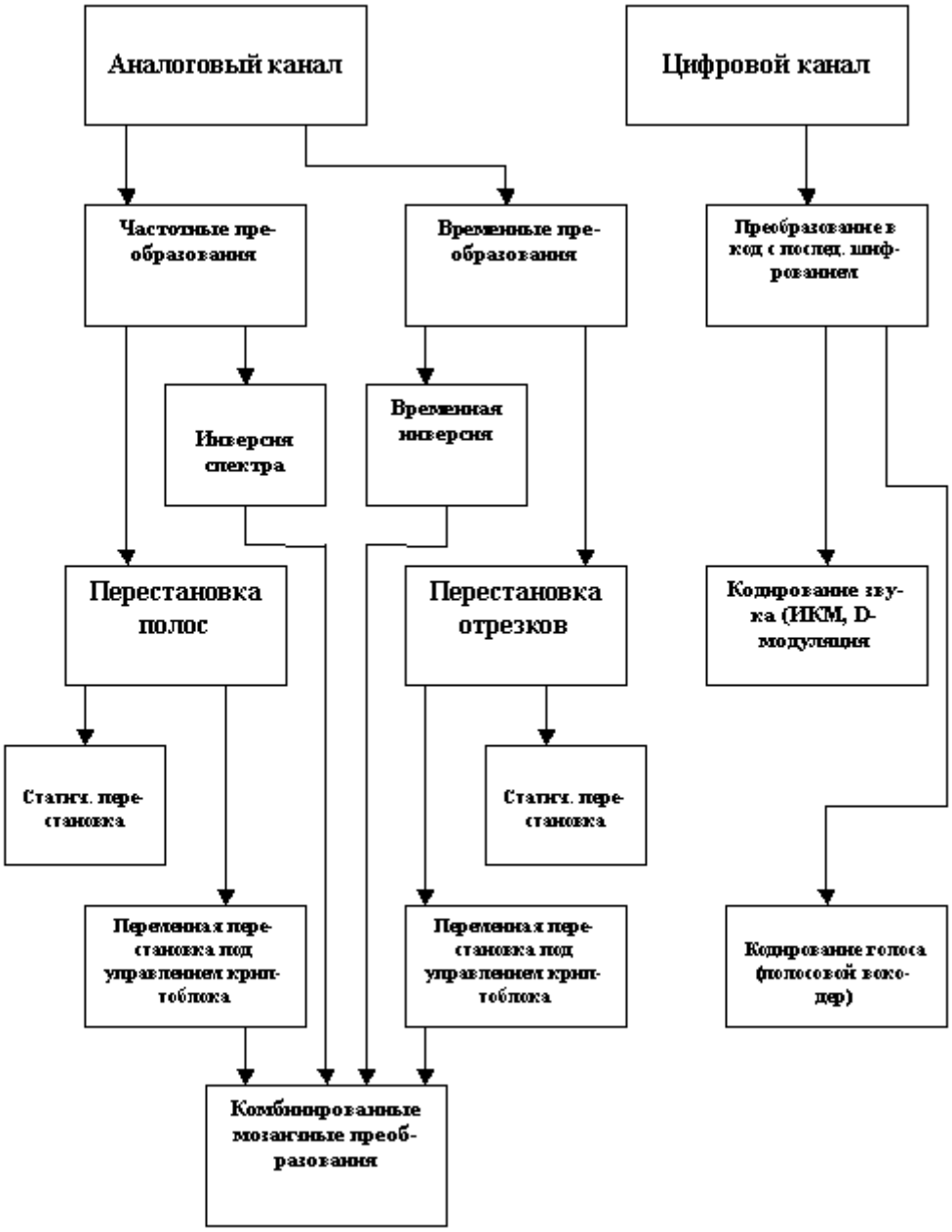


Рис. 6.19. Методы семантического преобразования сигнала

Следует сказать, что защита информации в каналах связи на семантическом уровне – наиболее перспективное направление. К числу ее несомненных достоинств относятся следующие.

- Технические средства криптографической защиты (иначе – скремблеры) обеспечивают наивысшую степень защиты телефонных переговоров.
- Защита происходит на всем протяжении линии связи. Кроме того, безразлично, какой аппаратурой перехвата пользуется злоумышленник. Все равно он не сможет в реальном масштабе времени декодировать полученную информацию, пока не раскроет ключевую систему защиты и не создаст автоматический комплекс по перехвату.
- Скремблеры могут быть использованы как в кабельных, так и беспроводных системах связи.

К недостаткам скремблеров относят два обстоятельства:

- необходимость установки однотипного оборудования на всех абонентских пунктах;
- потеря времени, необходимого для синхронизации аппаратуры и обмена ключами в начале сеанса защищенного соединения.

В табл. 6.14 представлены краткие описания некоторых современных технических средств криптографической защиты линий связи.

Таблица 6.14

Технические средства криптографической защиты линий связи

Наименование	Краткое описание
РЕЗЕДА	Устройство маскирования телефонных сообщений (УМТС) предназначено для защиты телефонных сообщений, передаваемых между мобильными радиотелефонами сотовых сетей стандарта GSM, от несанкционированного доступа (НСД) к их содержимому.
OPEX-4130	ОСНОВНЫЕ ХАРАКТЕРИСТИКИ: защита речевой информации методом частотно-временного скремблирования или на основе вокодерного преобразования (4800 бит/сек); защита факсимильных документов путём шифрования передаваемого изображения; защита межкомпьютерного обмена данными; система открытого распределения ключей Диффи-Хеллмана; шифрование по алгоритму IDEA
OPEX-4M7	Служит для защиты от прослушивания переговоров, ведущихся по каналам городской и междугородной телефонной сети в режимах скремблера и вокодера, а также для защиты факса и данных.
MOBI-GSM	Устройство защиты мобильной связи. Обеспечивает защиту на всем участке от одного абонента до другого (Point-to-Point), включая соединение между мобильным и стационарным абонентами.
OPEX-2	Устройство защиты речевой информации “Opex-2” предназначено для организации засекречивающей связи с высокой степенью защищенности от несанкционированного восстановления информации, передаваемой по коммутируемым или выделенным каналам связи с 2-х проводным абонентским окончанием.
ГРОТ	Комплекс предназначен для обеспечения криптографической защиты наиболее уязвимого фрагмента сетей связи общего пользования - абонентской линии.
CODE VOICE	Устройство Code Voice шифрует речь и данные. Устройство устанавливается между стандартным телефоном и публичной телефонной сетью. По желанию владельца CodeVoice может шифровать речь, предотвращая таким образом перехват Ваших телефонных переговоров. Дополнительно, устройство может быть подсоединено к компьютеру (через стандартный serial порт) для шифрования передаваемых по телефонным линиям данных.
СКР-511 Basic	Предназначен для передачи речи по телефонной линии в цифровом виде с применением специальных алгоритмов сжатия и защиты.
SCR-M1.2multi	Предназначен для работы совместно с офисными мини-АТС. Скремблер включается между городской телефонной линией и мини-АТС, обеспечивая работу в закрытом режиме всех телефонных и факсимильных аппаратов, подключенных к данной мини-АТС.
SCR-M1.2mini	Разработан на основе базовой модели SCR-M1.2 для работы в условиях командировок и т.д. Отличается малыми габаритами и предельной простотой управления.
ACS-2	Компактное, полностью автономное кодирующее устройство, позволяющее вести конфиденциальные переговоры с любого телефонного аппарата, в том числе с платных таксофонов, радиотелефонов и телефонов сотовой связи. Исполнен в виде насадки на телефонную трубку.
Voice Coder-2400	Для гарантированной защиты телефонных переговоров от несанкционированного перехвата с использованием алгоритмов защиты от НСД на основе методов линейного и параметрического кодирования.

Модуль 4. Компьютерная безопасность

4.7. Защита компьютерной информации от несанкционированного доступа

4.7.1. Угрозы безопасности информации в компьютерных системах

С позиции обеспечения безопасности информации в КС такие системы целесообразно рассматривать в виде единства трех компонент, оказывающих взаимное влияние друг на друга:

- информация;
- технические и программные средства;
- обслуживающий персонал и пользователи.

В отношении приведенных компонент иногда используется и термин "информационные ресурсы", который в этом случае трактуется значительно шире, чем в Федеральном законе "Об информации, информатизации и защите информации".

Целью создания любой КС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности. Информация является конечным "продуктом потребления" в КС и выступает в виде центральной компоненты системы. Безопасность информации на уровне КС обеспечивают две другие компоненты системы. Причем эта задача должна решаться путем защиты от внешних и внутренних неразрешенных (несанкционированных) воздействий. Особенности взаимодействия компонент заключаются в следующем. Внешние воздействия чаще всего оказывают несанкционированное влияние на информацию путем воздействия на другие компоненты системы. Следующей особенностью является возможность несанкционированных действий, вызываемых внутренними причинами, в отношении информации со стороны технических, программных средств, обслуживающего персонала и пользователей. В этом заключается основное противоречие взаимодействия этих компонент с информацией. Причем, обслуживающий персонал и пользователи могут сознательно осуществлять попытки несанкционированного воздействия на информацию. Таким образом, обеспечение безопасности информации в КС должно предусматривать защиту всех компонент от внешних и внутренних воздействий (угроз).

Под угрозой безопасности информации понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации. Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса: случайные угрозы и преднамеренные угрозы.

4.7.1.1. Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют *случайными* или непреднамеренными.

Реализация угроз этого класса приводит к наибольшим потерям информации (по статистическим данным - до 80 % от ущерба, наносимого информационным ресурсам КС любыми угрозами). При этом могут происходить уничтожение, нарушение целостности и доступности информации. Реже нарушается конфиденциальность информации, однако при этом создаются предпосылки для злоумышленного воздействия на информацию. К случайным можно отнести следующие виды угроз.

- Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен.
- Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств. Нарушения алгоритмов работы отдельных узлов и устройств могут также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации могут привести к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т.п.
- Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты информации.

- Согласно данным Национального Института Стандартов и Технологий США (NIST) 65 % случаев нарушения безопасности информации происходит в результате ошибок пользователей и обслуживающего персонала. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводит к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

Характеризуя угрозы информации в КС, не связанные с преднамеренными действиями, в целом, следует отметить, что механизм их реализации изучен достаточно хорошо, накоплен значительный опыт противодействия этим угрозам. Современная технология разработки технических и программных средств, эффективная система эксплуатации КС, включающая обязательное резервирование информации, позволяют значительно снизить потери от реализации угроз этого класса.

4.7.1.2. Преднамеренные угрозы

Второй класс угроз безопасности информации в КС составляют преднамеренно создаваемые угрозы. Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами. Угрозы этого класса в соответствии с их физической сущностью и механизмами реализации могут быть распределены по пяти группам:

- традиционный или универсальный шпионаж и диверсии;
- несанкционированный доступ к информации;
- электромагнитные излучения и наводки;
- модификация структур КС;
- вредительские программы.

Традиционный шпионаж и диверсии

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий, которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих КС. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты;
- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Методы и средства защиты от подслушивания достаточно подробно изложены в разделе 3.6. Остановимся на других методах шпионажа и диверсий.

Дистанционная видеоразведка для получения информации в КС малопригодна и носит, как правило, вспомогательный характер. Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из КС информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе. Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино- и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время "микроразведчик" способен преодолеть расстояние в 810 м, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г).

Для вербовки сотрудников и физического уничтожения объектов КС также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект КС, может использовать любой из методов традиционного шпионажа. Злоумышленниками,

имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео- и аудиозаписи. Для аудио- и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или "жучки". Для объектов КС наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещений. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие "закладки" ("радиозакладки") быстро устанавливаются, но также имеют демаскирующий признак - излучение в радио или оптическом диапазоне. "Радиозакладки" могут использовать в качестве источника электрические или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические "радиозакладки". Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике "радиозакладок" подавляющее большинство (около 90 %) рассчитаны на работу в диапазоне расстояний 50 - 800 м.

Для некоторых объектов КС существует угроза вооруженного нападения террористических или диверсионных групп. При этом могут быть применены средства огневого поражения.

Несанкционированный доступ к информации

Термин "несанкционированный доступ к информации" (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем. Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам КС определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в КС в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам. Выполнение установленных правил разграничения доступа в КС реализуется за счет создания системы разграничения доступа (СРД).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствует система разграничения доступа;
- сбой или отказ в КС; ошибочные действия пользователей или обслуживающего персонала КС;
- ошибки в СРД;
- фальсификация полномочий.

Если СРД отсутствует, то злоумышленник, имеющий навыки работы в КС, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств КС, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в СРД и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

Электромагнитные излучения и наводки

Механизмы возникновения ПЭМИН, а также защита от утечки информации по возникающим вследствие ПЭМИН каналам проанализированы в разделах 2.4, 2.5, 3.6. Необходимо лишь отметить, что электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные сверхвысокочастотные излучения могут вывести из строя электронные блоки КС. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

Несанкционированная модификация структур

Большую угрозу безопасности информации в КС представляет несанкционированная модификация алгоритмической, программной и технической структур системы. Несанкционированная модификация структур может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название "закладка". В процессе разработки КС "закладки" внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или

государственных учреждениях. В универсальные КС "закладки" внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки КС во враждебное государство. "Закладки", внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных КС.

Алгоритмические, программные и аппаратные "закладки" используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему. Вредительские воздействия "закладок" на КС осуществляются при получении соответствующей команды извне (в основном, характерно для программных "закладок") и при наступлении определенных событий в системе. Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления оружием или режим устранения аварийной ситуации на атомной электростанции и т.п.), наступление установленной даты, достижение определенной наработки и т.д.

Программные и аппаратные "закладки" для осуществления неконтролируемого входа в программы (например, режимов операционной системы), обхода средств защиты информации получили название "люки".

Вредительские программы

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название "вредительские программы".

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- "логические бомбы";
- "черви";
- "троянские кони";
- "компьютернрые вирусы".

"Логические бомбы" - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условиях. Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

"Червями" называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самопроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

"Троянские кони" - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

"*Компьютерные вирусы"* - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС. Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Классификация злоумышленников

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к КС. Злоумышленником может быть:

- разработчик КС;
- сотрудник из числа обслуживающего персонала;
- пользователь;
- постороннее лицо.

Разработчик владеет наиболее полной информацией о программных и аппаратных средствах КС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС. Пользователь имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения "закладок" пользователями очень ограничены. Постороннее лицо, не имеющее отношения к КС, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект КС, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность

диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

Большие возможности оказания вредительских воздействий на информацию КС имеют специалисты, обслуживающие эти системы. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

4.7.2. Программы-шпионы

4.7.2.1. Программные закладки

Современная концепция создания компьютерных систем предполагает использование программных средств различного назначения в едином комплексе. К примеру, типовая система автоматизированного документооборота состоит из операционной среды, программных средств управления базами данных, телекоммуникационных программ, текстовых редакторов, антивирусных мониторов, средств для криптографической защиты данных, а также средств аутентификации и идентификации пользователей. Главным условием правильного функционирования такой компьютерной системы является обеспечение защиты от вмешательства в процесс обработки информации тех программ, присутствие которых в компьютерной системе не обязательно. Среди подобных программ, в первую очередь, следует упомянуть компьютерные вирусы. Однако имеются вредоносные программы еще одного класса. От них, как и от вирусов, следует с особой тщательностью очищать свои компьютерные системы. Это так называемые *программные закладки,* которые могут выполнять хотя бы одно из перечисленных ниже действий:

- вносить произвольные искажения в коды программ, находящихся в оперативной памяти компьютера (программная закладка первого типа);
- переносить фрагменты информации из одних областей оперативной или внешней памяти компьютера в другие (программная закладка второго типа);
- искажать выводимую на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ (программная закладка третьего типа).

Программные закладки можно классифицировать и по методу их внедрения в компьютерную систему:

- программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера (их средой обитания, как правило, является BIOS – набор программ, записанных в виде машинного кода в постоянном запоминающем устройстве – ПЗУ);
- загрузочные закладки, ассоциированные с программами начальной загрузки, которые располагаются в загрузочных секторах (из этих секторов в процессе выполнения начальной загрузки компьютер считывает программу, берущую на себя управление для последующей загрузки самой операционной системы);
- драйверные закладки, ассоциированные с драйверами (файлами, в которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);
- прикладные закладки, ассоциированные с прикладным программным обеспечением общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);
- исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаще всего эти модули представляют собой пакетные файлы, т.е. файлы, которые состоят из команд операционной системы, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера);
- закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввода конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек и пр.);
- замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового, развлекательного назначения.

Чтобы программная закладка могла произвести какие-либо действия по отношению к другим программам или по отношению к данным, процессор должен приступить к исполнению команд, входящих в состав кода программной закладки. Это возможно только при одновременном соблюдении следующих условий:

- программная закладка должна попасть в оперативную память компьютера (если закладка относится к первому типу, то она должна быть загружена до начала работы другой программы, которая является целью воздействия закладки, или во время работы этой программы);
- работа закладки, находящейся в оперативной памяти, начинается при выполнении ряда условий, которые называются активизирующими.

Иногда сам пользователь провоцируется на запуск исполняемого файла, содержащего код программной закладки. Известен такой случай. Среди пользователей свободно распространялся набор из архивированных файлов. Для извлечения файлов из него требовалось вызвать специальную утилиту, которая, как правило, есть почти у каждого пользователя и запускается после указания ее имени в командной строке. Однако мало кто из пользователей замечал, что в полученном наборе файлов уже имелась программа с таким же именем и что запускалась именно она. Кроме разархивирования файлов, эта программная закладка дополнительно производила ряд действий негативного характера.

С учетом замечания о том, что программная закладка должна быть обязательно загружена в оперативную память компьютера, можно выделить резидентные закладки (они находятся в оперативной памяти постоянно, начиная с некоторого момента и до окончания сеанса работы компьютера, т.е. до его перезагрузки или до выключения питания) и нерезидентные (такие закладки попадают в оперативную память компьютера аналогично резидентным, однако, в отличие от последних, выгружаются по истечении некоторого времени или по выполнении особых условий).

Существуют три основные группы деструктивных действий, которые могут осуществляться программными закладками:

- копирование информации пользователя КС (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящихся в оперативной или внешней памяти этой системы либо в памяти другой КС, подключенной к ней через локальную или глобальную компьютерную сеть;
- изменение алгоритмов функционирования системных, прикладных или служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введенного пароля);
- навязывание определенного режима работы (например, блокирование записи на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована хакером).

У всех программных закладок (независимо от метода их внедрения в компьютерную систему, срока их пребывания в оперативной памяти и назначения) имеется одна важная общая черта: они обязательно выполняют операцию записи в оперативную или внешнюю память системы. При отсутствии данной операции никакого негативного влияния программная закладка оказать не может. Ясно, что для целенаправленного воздействия она должна выполнять и операцию чтения, иначе в ней может быть реализована только функция разрушения (например, удаление или замена информации в определенных секторах жесткого диска).

4.7.2.2. Модели воздействия программных закладок на компьютеры

Перехват

В модели перехват программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию, вводимую с внешних устройств КС или выводимую на эти устройства, в скрытой области памяти локальной или удаленной КС. Объектом сохранения, например, могут служить символы, введенные с клавиатуры (все повторяемые два раза последовательности символов), или электронные документы, распечатываемые на принтере.

Данная модель может быть двухступенчатой. На первом этапе сохраняются только, например, имена или начала файлов. На втором накопленные данные анализируются злоумышленником с целью принятия решения о конкретных объектах дальнейшей атаки.

Модель типа "перехват" может быть эффективно использована при атаке на защищенную операционную систему Windows NT. После старта Windows NT на экране компьютерной системы появляется приглашение нажать клавиши <Ctrl> + <Alt> + <Del>. После их нажатия загружается динамическая библиотека MSGINA.DLL, осуществляющая прием вводимого пароля и выполнение процедуры его проверки (аутентификации). Описание всех функций этой библиотеки можно найти в файле Winwlx.h. Также существует простой механизм замены исходной библиотеки MSGINA.DLL на пользовательскую (для этого необходимо просто добавить специальную строку в реестр в реестр операционной системы Windows NT и указать местоположение пользовательской библиотеки). В результате злоумышленник может модифицировать процедуру контроля за доступом к КС, работающей под управлением Windows NT.

Искажение

В модели искажение программная закладка изменяет информацию, которая записывается в память КС в результате работы программ, либо подавляет/инициирует возникновение ошибочных ситуаций в КС.

Можно выделить статическое и динамическое искажение. Статическое искажение происходит всего один раз. При этом модифицируются параметры программной среды КС, чтобы впоследствии в ней выполнялись нужные злоумышленнику действия. К статическому искажению относится, например, внесение изменений в файл AUTOEXEC.BAT операционной системы Windows 95/98, которые приводят к запуску заданной программы, прежде чем будут запущены все другие, перечисленные в этом файле. Специалистам ФАПСИ удалось выявить при анализе одной из отечественной систем цифровой подписи интересное статистическое искажение. Злоумышленник (сотрудник отдела информатизации финансовой организации, в которой была внедрена данная система) исправил в исполняемом EXE-модуле программы проверки правильности цифровой подписи символьную строку "ПОДПИСЬ НЕКОРРЕКТНА" на символьную строку "ПОДПИСЬ КОРРЕКТНА". В результате вообще перестали фиксироваться документы с неверными цифровыми подписями, и, следовательно, в электронные документы стало возможно вносить произвольные изменения уже после их подписания электронной цифровой подписью.

Динамическое искажение заключается в изменении каких-либо параметров системных или прикладных процессов при помощи заранее активизированных закладок. Динамическое искажение можно условно разделить так: искажение на входе (когда на обработку попадает уже искаженный документ) и искажение на выходе (когда искажается информация, отображаемая для восприятия человеком, или предназначенная для работы других программ).

Практика применения цифровой подписи в системах автоматизированного документооборота показала, что именно программная реализация цифровой подписи особенно подвержена влиянию программных закладок типа "динамическое искажение", которые позволяют осуществлять проводки фальшивых финансовых документов и вмешиваться в процесс разрешения споров по фактам неправомерного применения цифровой подписи. Например, в одной из программных реализаций широко известной криптосистемы PGP электронный документ, под которым требовалось поставить цифровую подпись, считывался блоками по 512 байт, причем процесс считывания считался завершенным, если в прочитанном блоке данные занимали меньше 512 байт. Работа одной программной закладки, выявленной специалистами ФАПСИ, основывалась на навязывании длины файла. Эта закладка позволяла считывать только первые 512 байт документа, и в результате цифровая подпись определялась на основе только этих 512 байт. Такая же схема действовала и при проверке поставленной под документом цифровой подписи. Следовательно, оставшаяся часть этого документа могла быть произвольным образом искажена, и цифровая подпись под ним продолжала оставаться "корректной".

Существуют 4 основных способа воздействия программных закладок на цифровую подпись:

- искажение входной информации (изменяется поступающий на подпись электронный документ);
- искажение результата проверки истинности цифровой подписи (вне зависимости от результатов работы программы цифровая подпись объявляется подлинной);
- навязывание длины электронного документа (программе цифровой подписи предъявляется документ меньшей длины, чем на самом деле, и в результате цифровая подпись ставится только под частью исходного документа);

- искажение программы цифровой подписи (вносятся изменения в исполняемый код программы с целью модификации реализованного алгоритма).

В рамках модели "искажение" также реализуются программные закладки, действие которых основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в КС, т.е. тех, которые приводят к отличному от нормального завершения исполняемой программы (предписанного соответствующей документацией).

Для инициирования статической ошибки на устройствах хранения информации создается область, при обращении к которой (чтение, запись, форматирование и т.п.) возникает ошибка, что может затруднить или блокировать некоторые нежелательные для злоумышленника действия системных или прикладных программ (например, не позволять осуществлять корректно уничтожить конфиденциальную информацию на жестком диске).

При инициировании динамической ошибки для некоторой операции генерируется ложная ошибка из числа тех ошибок, которые могут возникать при выполнении данной операции. Например, для блокирования приема или передачи информации в КС может постоянно инициироваться ошибочная ситуация "МОДЕМ ЗАНЯТ". Или при прочтении первого блока информации длиной 512 байт может устанавливаться соответствующий флажок для того, чтобы не допустить прочтения второго и последующих блоков и в итоге подделать цифровую подпись под документом.

Чтобы маскировать ошибочные ситуации, злоумышленники обычно используют подавление статической или динамической ошибки. Целью такого подавления часто является стремление блокировать нормальное функционирование КС или желание заставить ее неправильно работать. Чрезвычайно важно, чтобы КС адекватно реагировала на возникновение всех без исключения ошибочных ситуаций, поскольку отсутствие должной реакции на любую ошибку эквивалентно ее подавлению и может быть использовано злоумышленником. Известен случай успешной атаки пары аргентинских самолетов-торпедоносцев на английский эсминец "Шеффилд", закончившийся нанесением серьезных повреждений этому кораблю. Из-за ошибок в программном обеспечении установленная на нем система противовоздушной обороны не смогла выбрать цель, которую полагалось сбивать первой, поскольку атакующие самолеты летели слишком близко друг от друга.

Разновидностью искажения является также модель типа троянский конь. В этом случае программная закладка встраивается в постоянно используемое программное обеспечение и по некоторому активизирующему событию вызывает возникновение сбойной ситуации в КС. Тем самым достигаются сразу две цели: парализуется ее нормальное функционирование, а злоумышленник, получив доступ к КС для устранения неполадок, сможет, например, извлечь из нее информацию, перехваченную другими программными закладками. В качестве активизирующего события обычно используется наступление определенного момента времени, сигнал из канала связи или состояние некоторых счетчиков (например, счетчика количества запусков программы).

Уборка мусора

Как известно, при хранении компьютерных данных на внешних носителях прямого доступа выделяется несколько уровней иерархии: сектора, кластеры и файлы. Сектора являются единицами хранения информации на аппаратном уровне. Кластеры состоят из одного или нескольких подряд идущих секторов. Файл - это множество кластеров, связанных по определенному закону.

Работа с конфиденциальными электронными документами обычно сводится к последовательности следующих манипуляций файлами:

- создание;
- хранение;
- коррекция;
- уничтожение.

Для защиты конфиденциальной информации обычно используется шифрование. Основная угроза исходит отнюдь не от использования нестойких алгоритмов шифрования и "плохих" криптографических ключей (как это может показаться на первый взгляд), а от обыкновенных текстовых редакторов и баз данных, применяемых для создания и коррекции конфиденциальных документов.

Дело в том, что подобные программные средства, как правило, в процессе функционирования создают в оперативной или внешней памяти КС временные копии документов,

с которыми они работают. Естественно, все эти временные файлы выпадают из поля зрения любых программ шифрования и могут быть использованы злоумышленником для того, чтобы составить представление о содержании хранимых в зашифрованном виде конфиденциальных документов.

Важно помнить и о том, что при записи отредактированной информации меньшего объема в тот же файл, где хранилась исходная информация до начала сеанса ее редактирования, образуются так называемые "хвостовые" кластеры, в которых эта исходная информация полностью сохраняется. И тогда "хвостовые" кластеры не только не подвергаются воздействию программ шифрованию, но и остаются незатронутыми даже средствами гарантированного стирания информации. Конечно, рано или поздно информация из "хвостовых" кластеров затирается данными из других файлов, однако, по оценкам специалистов ФАПСИ, из "хвостовых" кластеров через сутки можно извлечь до 85 %, а через десять суток - до 25 - 40 % исходной информации.

Пользователям необходимо иметь в виду и то, что команда удаления файла (DEL) операционной системы DOS не изменяет содержания файла, и оно может быть в любой момент восстановлено, если поверх него не был записан другой файл. Распространенные средства гарантированного стирания файлов предварительно записывают на его место константы или случайные числа и только после этого удаляют файл стандартными средствами DOS. Однако даже такие мощные средства оказываются бессильными против программных закладок, которые нацелены на то, чтобы увеличить количество остающихся в виде "мусора" фрагментов конфиденциальной информации. Например, программная закладка может инициировать статическую ошибку, пометив один или несколько кластеров из цепочки, входящей в файл, меткой "СБОЙНЫЙ". В результате при удалении файла средствами операционной системы или средствами гарантированного уничтожения та его часть, которая размещена в сбойных кластерах, остается нетронутой и впоследствии может быть восстановлена с помощью стандартных утилит.

Наблюдение и компрометация

Помимо перечисленных существуют и другие модели воздействия программных закладок на компьютеры. В частности, при использовании модели типа "наблюдение" программная закладка встраивается в сетевое или телекоммуникационное программное обеспечение. Пользуясь тем, что подобное программное обеспечение всегда находится в состоянии активности, внедренная в него программная закладка может следить за всеми процессами обработки информации в КС, а также осуществлять установку и удаление других программных закладок. Модель типа компрометация позволяет получать доступ к информации, перехваченной другими программными закладками. Например, инициируется постоянное обращение к такой информации, приводящее к росту соотношения сигнал/шум. А это, в свою очередь, значительно облегчает перехват побочных излучений данной компьютерной системы и позволяет эффективно выделять сигналы, сгенерированной закладкой типа "компрометация", из общего фона излучения, исходящего из оборудования.

4.7.2.3. Защита от программных закладок

Задача защиты от программных закладок может рассматриваться в трех принципиально различных вариантах:

- не допустить внедрения программной закладки в КС;
- выявить внедренную программную закладку;
- удалить внедренную программную закладку.

При рассмотрении этих вариантов решение задачи защиты от программных закладок сходно с решением проблемы защиты КС от вирусов. Как и в случае борьбы с вирусами, задача решается с помощью средств контроля за целостностью запускаемых системных и прикладных программ, а также за целостностью информации, хранимой в КС и за критическими для функционирования системы событиями. Однако данные средства действенны только тогда, когда сами они не подвержены влиянию программных закладок, которые могут:

- навязывать конечные результаты контрольных проверок;
- влиять на процесс считывания информации и запуск программ, за которыми осуществляется контроль;
- изменять алгоритмы функционирования средств контроля.

При этом чрезвычайно важно, чтобы включение средств контроля выполнялось до начала воздействия программной закладки либо когда контроль осуществляется только с использованием программ управления, находящихся в ПЗУ компьютерной системы.

Защита от внедрения программных закладок

Универсальным средством защиты от внедрения программных закладок является создание изолированного компьютера. Компьютер называется изолированным, если выполнены следующие условия:

- в нем установлена система BIOS, не содержащая программных закладок;
- операционная система проверена на наличие в ней закладок;
- достоверно установлена неизменность BIOS и операционной системы для данного сеанса;
- на компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок;
- исключен запуск проверенных программ в каких-либо иных условиях, кроме перечисленных выше, т.е. вне изолированного компьютера.

Для определения степени изолированности компьютера может использоваться модель ступенчатого контроля. Сначала проверяется, нет ли изменений в BIOS. Затем, если все в порядке, считывается загрузочный сектор диска и драйверы операционной системы, которые, в свою очередь, также анализируются на предмет внесения в них несанкционированных изменений. И наконец, с помощью операционной системы запускается драйвер контроля вызовов программ, который следит за тем, чтобы в компьютере запускались только проверенные программы..

Интересный метод борьбы с внедрением программных закладок может быть использован в информационной банковской системе, в которой циркулируют исключительно файлы-документы. Чтобы не допустить проникновения программной закладки через каналы связи, в этой системе не допускается прием никакого исполняемого кода. Для распознавания событий типа "ПОЛУЧЕН ИСПОЛНЯЕМЫЙ КОД" и "ПОЛУЧЕН ФАЙЛ-ДОКУМЕНТ" применяется контроль за наличием в файле запрещенных символов: файл признается содержащим исполняемый код, если в нем присутствуют символы, которые никогда не встречаются в файлах-документах.

Выявление внедренной программной закладки

Выявление внедренного кода программной закладки заключается в обнаружении признаков его присутствия в КС. Эти признаки можно разделить на следующие два класса:

- качественные и визуальные;
- обнаруживаемые средствами тестирования и диагностики.

К качественным и визуальным признакам относятся ощущения и наблюдения пользователя компьютерной системы, который отмечает определенные отклонения в ее работе (изменяется состав и длины файлов, старые файлы куда-то пропадают, а вместо них появляются новые, программы начинают работать медленнее, или заканчивают свою работу слишком быстро, или вообще перестают запускаться). Несмотря на то, что суждение о наличии признаков этого класса кажется слишком субъективным, тем не менее, они часто свидетельствуют о наличии неполадок в КС и, в частности, о необходимости проведения дополнительных проверок присутствия программных закладок. Например, пользователи пакета шифрования и цифровой подписи "Криптоцентр" с некоторых пор стали замечать, что цифровая подпись под электронными документами ставится слишком быстро. Исследование, проведенное специалистами ФАПСИ, показало присутствие программной закладки, работа которой основывалась на навязывании длины файла. В другом случае тревогу забили пользователи пакета шифрования и цифровой подписи "Криптон", которые с удивлением отметили, что скорость шифрования по криптографическому алгоритму ГОСТ 28147-89 вдруг возросла более чем в 30 раз. А в третьем случае программная закладка обнаружила свое присутствие в программе клавиатурного ввода тем, что пораженная ею программа перестала нормально работать.

Признаки, выявляемые с помощью средств тестирования и диагностики, характерны как для программных закладок, так и для компьютерных вирусов. Например, загрузочные закладки успешно обнаруживаются антивирусными программами, которые сигнализируют о наличии подозрительного кода в загрузочном секторе диска. С инициированием статической ошибки на дисках хорошо справляется Disk Doctor, входящий в распространенный комплект утилит Norton Utilities. А средства проверки целостности данных на диске типа Adinf позволяют успешно выявлять изменения, вносимые в файлы программными закладками. Кроме того, эффективен поиск фрагментов кода программных закладок по характерным для них последовательностям нулей и единиц (сигнатурам), а также разрешение выполнения только программ с известными сигнатурами.

Удаление внедренной программной закладки

Конкретный способ удаления внедренной программной закладки зависит от метода ее внедрения в КС. Если это программно-аппаратная закладка, то следует перепрограммировать ПЗУ компьютера. Если это загрузочная, драйверная, прикладная, замаскированная закладка или закладка-имитатор, то можно заменить их на соответствующую загрузочную запись, драйвер, утилиту, прикладную или служебную программу, полученную от источника, заслуживающего доверие. Наконец, если это исполняемый программный модуль, то можно попытаться добыть его исходный текст, убрать из него имеющиеся закладки или подозрительные фрагменты, а затем заново откомпилировать.

4.7.2.4. Троянские программы

Троянской программой (троянцем, троянским конем) называется:

- программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;
- программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

Таким образом, троянская программа - это особая разновидность программной закладки. Она дополнительно наделена функциями, о существовании которых пользователь даже не подозревает. Когда троянская программа выполняет эти функции, компьютерной системе наносится определенный ущерб. Однако то, что при одних обстоятельствах причиняет непоправимый вред, при других может оказаться вполне полезным. К примеру, программу, которая форматирует жесткий диск, нельзя назвать троянской, если она как раз и предназначена для его форматирования. Но если пользователь, выполняя некоторую программу, совершенно не ждет, что она отформатирует его винчестер, - это и есть самый настоящий троянец.

В общем, троянской можно считать любую программу, которая в тайне от пользователя выполняет какие-то нежелательные для него действия. Эти действия могут быть любыми - от определения регистрационных номеров программного обеспечения, установленного на компьютере, до составления списка каталогов на его жестком диске. А сама троянская программа может маскироваться под текстовый редактор, под сетевую утилиту или любую программу, которую пользователь пожелает установить на свой компьютер.

Откуда берутся троянские программы

Троянская программа - это плод труда программиста. Никаким другим способом создать ее невозможно. Программист, пишущий троянскую программу, прекрасно осознает, чего он хочет добиться, и в своих намерениях он всегда весьма далек от альтруизма.

Большинство троянских программ предназначено для сбора конфиденциальной информации. Их задача, чаще всего, состоит в выполнении действий, позволяющих получить доступ к данным, которые не подлежат широкой огласке. К таким данным относятся пользовательские пароли, регистрационные номера программ, сведения о банковских счетах и т.д. Остальные троянцы создаются для причинения прямого ущерба компьютерной системе, приводят ее в неработоспособное состояние. К последним можно отнести, например, троянскую программу PC CYBORG, которая завлекала ничего не подозревающих пользователей обещаниями предоставить им новейшую информацию о борьбе с вирусом, вызывающим синдром приобретенного иммунодефицита (СПИД). Проникнув в компьютерную систему, PC CYBORG отсчитывала 90 перезагрузок этой системы, а затем прятала все каталоги на ее жестком диске и шифровала находящиеся там файлы.

Другая троянская программа называлась AOLGOLD. Она рассылалась по электронной почте в виде заархивированного файла. В сопроводительном письме, прилагавшемся к этому файлу, говорилось о том, что AOLGOLD предназначена для повышения качества услуг, которые предоставляет своим пользователям крупнейший американский Internet-провайдер America Online (AOL). Архив состоял из двух файлов, один из которых именовался INSTALL.BAT. Пользователь, запустивший INSTALL.BAT, рисковал стереть все файлы из каталогов C:\, C:\DOS, C:\WINDOWS и C:\WINDOWS\SYSTEM на своем жестком диске.

Подобного рода троянские программы, как правило, создаются подростками, которые хотя и одержимы страстью к разрушению, но не имеют глубоких познаний в программировании и поэтому не могут причинить существенный ущерб компьютерным системам, подвергшимся нападению созданных ими троянцев. Например, программа AOLGOLD стирала себя с жесткого диска, будучи запущена из любого другого дискового раздела за исключения C. Другое дело -

троянские программы, авторами которых являются профессиональные программисты, занимающиеся разработкой программного обеспечения в солидных фирмах. Троянцы, входящие в распространенные компьютерные приложения, утилиты и операционные системы, представляют значительно большую угрозу компьютерам, на которых они установлены, поскольку их действия носят не деструктивный характер, а имеют целью сбор конфиденциальной информации о системе. Обнаружить такие троянские программы удается, как правило, чисто случайно. А поскольку программное обеспечение, частью которого они являются, в большинстве случаев используется не только какой-то одной компанией, закупившей это программное обеспечение, но также на крупных Internet-серверах и, кроме того, распространяется через Internet, последствия могут оказаться самыми плачевными.

Случается и так, что троянцы встраиваются в некоторые утилиты программистами, не имеющими никакого отношения к разработке этих утилит. Например, в дистрибутив сканера SATAN, предназначенный для установки на компьютеры с операционной системой Linux, распространявшейся через Internet, попала троянская программа, которая "обосновалась" в утилите fping. При первом же запуске модифицированной утилиты fping в файл /etc/passwd добавлялась запись для пользователя с именем suser, который в результате мог войти в Linux и тайно получить там полномочия администратора. Однако у автора этой тороянской программы были явные пробелы в компьютерном образовании. В частности, он не знал некоторых нюансов хранения паролей в операционных системах семейства UNIX. В результате файл /ets/passwd был соответствующим образом изменен всего лишь на двух компьютерах, на которых был установлен этот испорченный дистрибутив SATAN для Linux.

Где обитают и как часто встречаются троянские программы

В настоящее время троянские программы можно отыскать практически где угодно. Они написаны для всех без исключения операционных систем и для любых платформ. Не считая случаев, когда троянские программы пишутся самими разработчиками программного обеспечения, троянцы распространяются тем же способом, что и компьютерные вирусы. Поэтому самыми подозрительными на предмет присутствия в них троянцев, в первую очередь, являются бесплатные и условно-бесплатные программы, скачанные из Internet, а также программное обеспечение, распространяемое на пиратских компакт-дисках.

Например, в январе 1999 г. было обнаружено, что популярная утилита TCP Wrapper, предназначенная для администрирования UNIX-систем и бесплатно распространяемая через Internet, на многих ftp-сайтах была заменена внешне похожей на нее программой, которая на самом деле являлась троянцем. После инсталляции он отправлял электронное сообщение по определенным внешним адресам, оповещая своего хозяина об успешном внедрении. Потом он ждал, пока будет установлено удаленное соединение с портом 421 зараженного им компьютера, и предоставлял привилегированные права доступа через этот порт.

Другая троянская программа распространялась среди пользователей AOL в виде вложения в письмо, рассылаемое по электронной почте. Открывшие это вложение заражали свой компьютер троянцем, который пытался найти пароль для подключения к AOL и в случае успеха шифровал его, а потом отсылал электронной почтой куда-то в Китай.

В настоящее время существует целый ряд троянских программ, которые можно совершенно свободно скачать, подключившись к глобальной компьютерной сети Internet. Наибольшую известность среди них получили троянцы Back Orifice, Net Bus и SubSeven. На Web-узле группы разработчиков Back Orifice, которая именует себя Cult of Dead Cow (Культ мертвой коровы), можно даже найти с десяток постеров, которые предназначены для рекламы ее последней разработки - троянца Back Orifice 2000.

Таким образом, троянские программы встречаются довольно часто и, следовательно, представляют серьезную угрозу безопасности компьютерных систем. Даже после того как троянская программа обнаружена, ее вредоносное влияние на компьютерную систему может ощущаться еще в течение очень длительного времени. Ведь зачастую никто не может с уверенностью сказать, насколько сильно пострадала компьютерная система в результате проникновения в нее троянской программы. Дело в том, что большинство троянцев являются частью других программ, которые хранятся в компьютере в откомпилированном виде. Текст этих программ представляет собой последовательность команд на машинном языке, состоящую из нулей и единиц. Рядовой пользователь, как правило, не имеет ни малейшего понятия о внутренней структуре таких программ. Он просто запускает их на исполнение путем задания имени соответствующей программы в командной строке или двойным щелчком на имени ее файла.

Когда выясняется, что в какую-то откомпилированную программу проник троянец, в сети Internet немедленно начинают распространяться бюллетени с информацией об обнаруженном троянце. Чаще всего в этих бюллетенях кратко сообщается о том, какой вред может причинить данный троянец и где можно найти замену пораженной троянцем программе.

Иногда ущерб, который может нанести троянец, оценить довольно легко. Например, если он предназначен для пересылки по электронной почте содержимого файла /etc/passwd, в котором операционные системы семейства UNIX хранят информацию о пользовательских паролях, достаточно установить "чистую" версию программы взамен той, в которой обосновался этот троянец. Затем пользователи должны будут обновить свои пароли, и на этом борьба с ним успешно завершится.

Однако далеко не всегда степень компрометации компьютерной системы, в которой поселилась троянская программа, бывает так легко определить. Предположим, что цель внедрения троянца состоит в создании дыры в защитных механизмах компьютерной системы, через которую злоумышленник сможет, например, проникать в нее, имея администраторские полномочия. И если взломщик окажется достаточно хитрым и смекалистым, чтобы замести следы своего присутствия в системе путем внесения соответствующих изменений в регистрационные файлы, то определить, насколько глубоко он проник сквозь системные защитные механизмы, будет почти невозможно, если учесть еще тот факт, что саму троянскую программу обнаружат лишь несколько месяцев спустя после ее внедрения в компьютерную систему. В этом случае может понадобиться целиком переустановить операционную систему и все приложения.

Как распознать троянскую программу

Большинство программных средств, предназначенных для защиты от троянских программ, в той или иной степени использует так называемое согласование объектов. При этом в качестве объектов фигурируют файлы и каталоги. А согласование представляет собой способ ответить на вопрос, изменились ли файлы и каталоги с момента последней проверки. В ходе согласования характеристики объектов сравниваются с характеристиками, которыми они обладали раньше. Берется, к примеру, архивная копия системного файла и ее атрибуты сравниваются с атрибутами этого файла, который в настоящий момент находится на жестком диске. Если атрибуты различаются, и никаких изменений в операционную систему не вносилось, значит в компьютер, скорее всего, проник троянец.

Одним из атрибутов любого файла является отметка о времени его последней модификации: всякий раз, когда файл открывается, изменяется и сохраняется на диске, автоматически вносятся соответствующие поправки. Однако отметка времени не может служить надежным индикатором наличия в системе троянца, поскольку этой отметкой очень легко манипулировать. Можно подкрутить назад системные часы, внести изменения в файл, затем снова вернуть часы в исходное состояние, и отметка о времени модификации файла останется неизменной.

Примерно также обстоит дело и с размерами файла. Нередко текстовый файл, который изначально занимал, скажем, 8 Кбайт дискового пространства, после редактирования и сохранения имеет тот же самый размер. Несколько иначе ведут себя двоичные файлы. Вставить в чужую программу фрагмент собственного кода так, чтобы она не утратила работоспособности и в откомпилированном виде сохранила свой размер, достаточно непросто. Поэтому размер файла является более надежным показателем, чем отметка о времени внесения в него последних изменений.

Злоумышленник, решивший запустить в компьютер троянца, обычно пытается сделать его частью системного файла. Такие файлы входят в дистрибутив операционной системы и их присутствие на любом компьютере, где эта операционная система установлена, не вызывает никаких подозрений. Однако любой системный файл имеет вполне определенную длину. Если данный атрибут будет каким-либо образом изменен, это встревожит пользователя. Зная это, злоумышленник постарается достать исходный текст соответствующей программы и внимательно проанализирует его на предмет присутствия в нем избыточных элементов, которые могут быть удалены без всякого ощутимого ущерба. Тогда вместо найденных избыточных элементов он вставит в программу своего троянца и перекомпилирует ее заново. Если размер полученного двоичного файла окажется меньше или больше размера исходного, процедура повторяется. И так до тех пор, пока не будет получен файл, размер которого в наибольшей степени близок к оригиналу.

Поскольку в борьбе с троянцами на отметку о времени последней модификации файла и его размер положиться нельзя, необходимо предложить какой-то иной метод. Одним из наиболее эффективных методов является метод "контрольной суммы" файла. Для подсчета контрольной суммы элементы файла суммируются, и получившееся в результате число объявляется его контрольной суммой. Например, в операционной системе SunOS существует специальная утилита sum, которая выводит на устройство стандартного вывода STDOUT контрольную сумму файлов, перечисленных в строке аргументов этой утилиты.

Однако и контрольную сумму в общем случае оказывается не так уж трудно подделать. Поэтому для проверки целостности файловой системы компьютера используется особая разновидность алгоритма вычисления контрольной суммы, называемая односторонним хэшированием. Функция хэширования называется односторонней, если задача отыскания двух аргументов, для которых ее значения совпадают, является трудно решаемой. Отсюда следует, что функция одностороннего хэширования может быть применена для того, чтобы отслеживать изменения, вносимые злоумышленником в файловую систему компьютера. Последнее возможно, поскольку вероятность получения неизменного значения контрольной суммы исходного и модифицированного файлов, полученное путем его одностороннего хэширования, очень мала.

Исторически сложилось так, что большинство утилит, позволяющих бороться с проникновением в компьютерную систему троянских программ путем однонаправленного хэширования файлов, было создано для операционных систем UNIX. Одной из наиболее удобных в эксплуатации и эффективных является утилита TripWire, которую можно найти в Internet по адресу **http://www.tripwiresecurity.com/**. Она позволяет производить однонаправленное хэширование файлов при помощи нескольких алгоритмов. Вычисленные хэш-значения файлов хранятся в специальной базе данных, которая, в принципе, является самым уязвимым звеном утилиты TripWire. Поэтому пользователям TripWire предлагается в обязательном порядке принимать дополнительные меры защиты, чтобы исключить доступ к этой базе данных со стороны злоумышленника (например, помещать ее на съемном носителе, предназначенном только для чтения).

Средства борьбы с троянцами в операционных системах семейства Windows (95/98/NT) традиционно являются частью их антивирусного программного обеспечения. Поэтому, чтобы отлавливать Back Orifice, NetBus, SubSeven и другие подобные им троянские программы, необходимо обзавестись самым современным антивирусом (например, программой Norton Antivirus 2000 компании Symantec, которая позволяет обнаруживать присутствие в компьютерной системе наиболее распространенных троянцев и избавляться от них). Следует регулярно проверять свой компьютер на присутствие в нем вирусов.

Достаточно хорошо известна программа The Clear компании MooSoft Development (**http://www.homestead.com/moosoft/cleaner.html**). Эта утилита используется для борьбы с более чем сорока разновидностями троянских программ в операционных системах семейства Windows.

Недавно появились программные пакеты, предназначенные для комплексной защиты от угроз, с которыми сталкиваются пользователи настольных компьютеров при работе в Internet. Одним из таких пакетов является eSafe Protect компании Aladdin Knowledge Systems (**http://www.esafe.com**). Функционально eSafe Protect делится на три компонента – антивирус, персональный брандмауэр и модуль защиты компьютерных ресурсов. Антивирус избавляет компьютер от вредоносных программ благодаря применению антивирусного модуля VisuSafe, сертифицированного американским Национальным агентством компьютерной безопасности. Персональный брандмауэр контролирует весь входящий и исходящий трафик по протоколу TCP/IP, наделяя используемые IP-адреса определенными правами (например, ограничивая доступ в Internet в определенные часы или запрещая посещение некоторых Web-узлов). Для защиты ресурсов компьютера, на котором установлен программный пакет eSafe Protect, создается специальная изолированная область – так называемая песочница. Все автоматически загружаемые из Internet Java-аплеты и компоненты ActiveX сначала помещаются в "песочницу", где они находятся под неусыпным наблюдением eSafe Protect. Если попавшая в "песочницу" программа попытается выполнить какое-либо недозволенное действие, то оно будет немедленно блокировано. В течение заданного интервала времени (от 1 до 30 дней) каждое приложение, загруженное в компьютер из Internet, проходит "карантинную" проверку в "песочнице". Полученная в ходе такой проверки информация заносится в особый журнал. По истечении

"карантина" приложение будет выполняться вне "песочницы", однако ему будут дозволены только те действия, перечень которых определяется на основе имеющихся журнальных записей.

Таким образом, по сравнению с другими подобными программными пакетами eSafe Protect обеспечивает наиболее развитые и эффективные средства комплексной защиты от троянских программ. Входящий в состав eSafe Protect антивирус помогает быстро выявлять и уничтожать троянцев, используя технологии, которые хорошо зарекомендовали себя в борьбе с вирусами. Персональный брандмауэр блокирует любые попытки связаться извне с проникшими в компьютерную систему троянскими программами. И наконец, с помощью "песочницы" своевременно предотвращается внедрение троянцев в компьютеры под видом Java-аплетов и компонентов ActiveX.

4.7.2.5. Клавиатурные шпионы

Одна из наиболее распространенных разновидностей программных закладок-клавиатурные шпионы. Такие программные закладки нацелены на перехват паролей пользователей операционной системы, а также на определение их легальных полномочий и прав доступа к компьютерным ресурсам. Компьютерные шпионы разрабатывались и для OS/370, и для UNIX, и для DOS. Их поведение в общем случае является довольно традиционным: типовой клавиатурный шпион обманным путем завладевает пользовательскими паролями, а затем переписывает эти пароли туда, откуда их может без особого труда извлечь злоумышленник. Различия между клавиатурными шпионами касаются только способа, который применяется ими для перехвата пользовательских паролей. Соответственно все клавиатурные шпионы делятся на три типа – имитаторы, фильтры и заместители.

Имитаторы

Клавиатурные шпионы этого типа работают по следующему алгоритму. Злоумышленник внедряет в операционную систему программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему. Затем внедренный модуль (имитатор) переходит в режим ожидания ввода пользовательского идентификатора и пароля. После того как пользователь идентифицирует себя и введет свой пароль, имитатор сохраняет эти данные там, где они доступны злоумышленнику. Далее имитатор инициирует выход из системы (что в большинстве случаев можно сделать программным путем), и в результате пользователь обнаруживает еще одно, но на этот раз уже настоящее приглашение для входа в систему. Обманутый пользователь, видя, что ему предлагается еще раз ввести пароль, приходит к выводу о том, что он допустил какую-то ошибку во время предыдущего ввода пароля, и послушно повторяет всю процедуру входа в систему заново. Некоторые имитаторы для убедительности выдают на экран монитора правдоподобное сообщение о якобы совершенной пользователем ошибке, например: "НЕВЕРНЫЙ ПАРОЛЬ. ПОПРОБУЙТЕ ЕЩЕ РАЗ".

Написание имитатора не требует от его создателя каких-либо особых навыков. Злоумышленнику, умеющему программировать на одном из универсальных языков программирования, понадобятся на это считанные часы. Единственная трудность, с которой он может столкнуться, состоит в том, чтобы отыскать в документации соответствующую программную функцию, реализующую выход пользователя из системы. Перехват пароля зачастую облегчают сами разработчики операционных систем, которые не затрудняют себя созданием усложненных по форме приглашений пользователю зарегистрироваться для входа в систему. Подобное пренебрежительное отношение характерно для большинства версий операционной системы UNIX, в которых регистрационное приглашение состоит из двух текстовых строк, выдаваемых поочередно на экран терминала:

login:

password:

Чтобы подделать такое приглашение, не нужно быть семи пядей во лбу. Однако само по себе усложнение внешнего вида приглашения не создает для хакера, задумавшего внедрить в операционную систему имитатор, каких-либо непреодолимых препятствий. Для этого требуется прибегнуть к более сложным и изощренным методам защиты. В качестве примера операционной системы, в которой такие меры в достаточно полном объеме реализованы на практике, можно привести Windows NT. Системный процесс WinLogon, отвечающий в операционной системе Windows NT за аутентификацию пользователей, имеет свой собственный рабочий стол - совокупность окон, одновременно видимых на экране дисплея. Этот рабочий стол называется столом аутентификации. Никакой другой процесс, в том числе и имитатор, не имеет доступа к рабочему столу аутентификации и не может расположить на нем свое окно. После запуска

Windows NT на экране компьютера возникает так называемое начальное окно рабочего стола аутентификации, содержащее указание нажать на клавиатуре клавиши <Ctrl>+<Alt>+<Del>. Сообщение о нажатии этих клавиш передается только системному процессу WinLogon, а для остальных процессов, в частности, для всех прикладных программ, их нажатие происходит совершенно незаметно. Далее производится переключение на другое, так называемое регистрационное окно рабочего стола аутентификации. В нем-то и размещается приглашение пользователю ввести свое идентификационное имя и пароль, которые будут восприняты и проверены процессом WinLogon.

Для перехвата пользовательского пароля внедренный в Windows NT имитатор обязательно должен уметь обрабатывать нажатие пользователем клавиш <Ctrl>+<Alt>+<Del>. В противном случае произойдет переключение на регистрационное окно рабочего стола аутентификации, имитатор станет неактивным и не сможет ничего перехватить, поскольку все символы пароля, введенные пользователем, минуют имитатор и станут достоянием исключительно системного процесса WinLogon. Как уже отмечалось, процедура регистрации в Windows NT устроена таким образом, что нажатие клавиш <Ctrl>+<Alt>+<Del> проходит бесследно для всех процессов, кроме WinLogon, и поэтому пользовательский пароль поступит именно ему. Нельзя исключать ситуацию, в которой имитатор может попытаться воспроизвести не начальное окно рабочего стола аутентификации (в котором высвечивается указание пользователю одновременно нажать клавиши <Ctrl>+<Alt>+<Del>), а регистрационное (где содержится приглашение вести идентификационное имя и пароль пользователя). Однако при отсутствии имитаторов в системе регистрационное окно автоматически заменяется на начальное по прошествии короткого промежутка времени (в зависимости от версии Windows NT он может продолжаться от 30 с до 1 мин), если в течение этого промежутка пользователь не предпринимает никаких попыток зарегистрироваться в системе. Таким образом, сам факт слишком долгого присутствия на экране регистрационного окна должен насторожить пользователя Windows NT и заставить его тщательно проверить свою компьютерную систему на предмет наличия в ней программных закладок.

Подводя итог, можно отметить, что степень защищенности Windows NT от имитаторов очень высока. Рассмотрение защитных механизмов, реализованных в этой операционной системе, позволяет сформулировать два необходимых условия, соблюдение которых является обязательным для обеспечения надежной защиты от имитаторов:

- системный процесс, который при входе пользователя в систему получает от него соответствующие регистрационное имя и пароль, должен иметь свой собственный рабочий стол, недоступный другим процессам;
- переключение на регистрационное окно рабочего стола аутентификации должно происходить абсолютно незаметно для прикладных программ, которые к тому же никак не могут повлиять на это переключение (например, запретить его).

Эти два условия ни в одной из операционных систем, за исключением Windows NT, не соблюдаются. Поэтому для повышения их защищенности от имитаторов можно порекомендовать воспользоваться административными мерами. Например, обязать каждого пользователя немедленно сообщать системному администратору, когда вход в систему оказывается невозможен с первого раза, несмотря на корректно заданное идентификационное имя и правильно набранный пароль.

Фильтры

Фильтры пытаются отследить данные, которые пользователь операционной системы вводит с клавиатуры компьютера. Самые элементарные фильтры просто сбрасывают перехваченный клавиатурой ввод на жесткий диск или в какое-то другое место, к которому имеет доступ злоумышленник. Более искусные программные закладки этого типа подвергают перехваченные данные анализу и отфильтровывают информацию, имеющую отношение к пользовательским паролям.

Фильтры являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры. Эти прерывания возвращают информацию о нажатой клавише и введенном символе, которая анализируется фильтрами на предмет выявления данных, имеющих отношение к паролю пользователя.

Известны несколько фильтров, созданных специально для различных версий операционной системы DOS. В 1997 г. Отмечено появление фильтров для операционных систем Windows 3.11 и Windows 95. Дело в том, что изготовить подобного рода программную закладку не составляет большого труда. В операционных системах Windows 3.11 и Windows 95/98

предусмотрен специальный программный механизм, с помощью которого в них решается ряд задач, связанных с получением доступа к вводу с клавиатуры, в том числе и проблема поддержки национальных раскладок клавиатур. К примеру, любой клавиатурный русификатор для Windows представляет собой самый что ни на есть настоящий фильтр, поскольку призван перехватывать все данные, вводимые пользователем с клавиатуры компьютера. Нетрудно "доработать" его таким образом, чтобы вместе со своей основной функцией он заодно выполнял бы и действия по перехвату паролей. Тем более что во многих учебных пособиях и руководствах пользователя операционных систем Windows имеются исходные тексты программных русификаторов клавиатуры. "Настроив" это русификатор соответствующим образом так, чтобы он взял на себя выполнение функций клавиатурного шпиона, его можно встроить перед настоящим русификатором или после него, и в результате вся информация, вводимая пользователем с клавиатуры, пойдет и через клавиатурного шпиона. Таким образом, задача создания фильтра становится такой простой, что не требует наличия каких-либо специальных знаний у злоумышленника. Ему остается только незаметно внедрить изготовленную им программную закладку в операционную систему и умело замаскировать ее присутствие.

В общем случае можно утверждать, что если в операционной системе разрешается переключать клавиатурную раскладку во время ввода пароля, то для этой операционной системы возможно создание фильтра. Поэтому, чтобы обезопасить ее от фильтров, необходимо обеспечить выполнение следующих условий:

- во время ввода пароля переключение раскладок клавиатуры не разрешается;
- конфигурировать цепочку программных модулей, участвующих в работе с паролем пользователя, может только системный администратор;
- доступ к файлам этих модулей имеет исключительно системный администратор.

Соблюсти первое из этих условий в адаптированных для России версиях операционных систем принципиально невозможно. Дело в том, что средства создания учетных пользовательских записей на русском языке являются неотъемлемой частью таких систем. Только в англоязычных версиях систем Windows NT и UNIX предусмотрены возможности, позволяющие поддерживать уровень безопасности, при котором соблюдаются все 3 перечисленные условия.

Заместители

Заместители полностью или частично подменяют собой программные модули операционной системы, отвечающие за аутентификацию пользователей. Подобного рода клавиатурные шпионы могут быть созданы для работы в среде практически любой многопользовательской операционной системы. Трудоемкость написания заместителя определяется сложностью алгоритмов, реализуемых подсистемой аутентификации, и интерфейсов между ее отдельными модулями. Также при оценке трудоемкости следует принимать во внимание степень документированности этой подсистемы. В целом можно сказать, что задача создания заместителя значительно сложнее задачи написания имитатора или фильтра. Поэтому фактов использования подобного рода программных закладок злоумышленниками пока отмечено не было. Однако в связи с тем, что в настоящее время все больше распространение получает операционная система Windows NT, имеющая мощные средства защиты от имитаторов и фильтров, в самом скором будущем от хакеров следует ожидать более активного использования заместителей в целях получения несанкционированного доступа к компьютерным системам.

Поскольку заместители берут на себя выполнение функций подсистемы аутентификации, перед тем как приступить к перехвату пользовательских паролей они должны выполнить следующие действия:

- подобно компьютерному вирусу внедриться в один или несколько системных файлов;
- использовать интерфейсные связи между программными модулями подсистемы аутентификации для встраивания себя в цепочку обработки введенного пользователем пароля.

Для того чтобы защитить систему от внедрения заместителя, ее администраторы должны строго соблюдать адекватную политику безопасности. И что особенно важно, подсистема аутентификации должна быть одним из самых защищенных элементов операционной системы. Однако, как показывает практика, администраторы, подобно всем людям, склонны к совершению ошибок. А следовательно, соблюдение адекватной политики безопасности в течение неограниченного периода времени является невыполнимой задачей. Кроме того, как только заместитель попал в компьютерную систему, любые меры защиты от внедрения программных закладок перестают быть адекватными, и поэтому необходимо предусмотреть возможность использования эффективных средств обнаружения и удаления внедренных клавиатурных

шпионов. Это значит, что администратор должен вести самый тщательный контроль целостности исполняемых системных файлов и интерфейсных функций, используемых подсистемой аутентификации для решения своих задач. Но и эти меры могут оказаться недостаточно эффективными. Ведь машинный код заместителя выполняется в контексте операционной системы, и поэтому заместитель может предпринимать особые меры, чтобы максимально затруднить собственное обнаружение. Например, он может перехватывать системные вызовы, используемые администратором для выявления программных закладок, с целью подмены возвращаемой ими информации. Или фильтровать сообщения, регистрируемые подсистемой аудита, чтобы отсеивать те, которые свидетельствуют о его присутствии в компьютере.

Как защитить систему от клавиатурных шпионов

Клавиатурные шпионы представляют реальную угрозу безопасности современных компьютерных систем. Чтобы отвести эту угрозу, требуется реализовать целый комплекс административных мер и программно-аппаратных средств защиты. Надежная защита от клавиатурных шпионов может быть построена только тогда, когда операционная система обладает определенными возможностями, затрудняющими работу клавиатурных шпионов. Они были подробно описаны выше, и не имеет смысла снова на них останавливаться. Однако необходимо еще раз отметить, что единственной операционной системой, в которой построение такой защиты возможно, является Windows NT. Да и то с оговорками, поскольку все равно ее придется снабдить дополнительными программными средствами, повышающими степень ее защищенности. В частности, в Windows NT необходимо ввести контроль целостности системных файлов и интерфейсных связей подсистемы аутентификации.

Кроме того, для надежной защиты от клавиатурных шпионов администратор операционной системы должен соблюдать политику безопасности, при которой только администратор может:

- конфигурировать цепочки программных модулей, участвующих в процессе аутентификации пользователей;
- осуществлять доступ к файлам этих программных модулей;
- конфигурировать саму подсистему аутентификации.

При организации защиты от клавиатурных шпионов всегда следует иметь в виду, что ни неукоснительное соблюдение адекватной политики безопасности, ни использование операционной системы, имеющей в своем составе средства, существенно затрудняющие внедрение клавиатурных шпионов и облегчающие их своевременное обнаружение, ни дополнительная реализация контроля за целостностью системных файловой и интерфейсных связей сами по себе не могут служить залогом надежной защиты информации в компьютере. Все эти меры должны осуществляться в комплексе.

4.7.3. Парольная защита операционных систем

4.7.3.1. Парольные взломщики

Проблему безопасности компьютерных сетей надуманной не назовешь. Практика показывает: чем масштабнее сеть и чем более ценная информация доверяется подключенным к ней компьютерам, тем больше находится желающих нарушить ее нормальное функционирование ради материальной выгоды или просто из праздного любопытства. В Internet атаки на компьютерные системы приносят очень серьезные убытки. Идет постоянная виртуальная война, в ходе которой организованности системных администраторов противостоит изобретательность компьютерных взломщиков.

Основой защиты от злонамеренных атак в компьютерной сети является система парольной защиты, которая имеется во всех современных операционных системах. В соответствии с установившейся практикой перед началом сеанса работы с операционной системой пользователь обязан зарегистрироваться, сообщив ей свое имя и пароль. Имя требуется операционной системе для идентификации пользователя, а пароль служит подтверждением правильности произведенной идентификации. Информация, введенная пользователем в диалоговом режиме, сравнивается с той, которая имеется в распоряжении операционной системы. Если проверка дает положительный результат, то пользователю становятся доступны все ресурсы операционной системы, связанные с его именем.

В настоящее время ни один злоумышленник не станет пытаться подобрать имя и пароль для входа в операционную систему, по очереди перебирая и вводя с клавиатуры все возможные

варианты. Скорость такого подбора пароля будет чрезвычайно низкой, тем более что в операционных системах с хорошо продуманной парольной защитой количество подряд идущих повторных вводов конкретного пользовательского имени и соответствующего ему пароля всегда можно ограничить двумя-тремя. При этом если это число будет превышено, то вход в систему с использованием данного имени будет заблокирован в течение фиксированного периода времени или до вмешательства системного администратора.

Гораздо более эффективным является другой метод взлома парольной защиты операционной системы, при котором атаке подвергается системный файл, содержащий информацию о ее легальных пользователях и их паролях. Однако любая современная операционная система надежно защищает при помощи шифрования пользовательские пароли, которые хранятся в этом файле. Доступ к таким файлам, как правило, по умолчанию запрещен даже системным администраторам, не говоря уже о рядовых пользователях. Тем не менее, в ряде случаев злоумышленнику удается путем различных ухищрений получить в свое распоряжение файл с именами пользователей и их зашифрованными паролями. И тогда ему на помощь приходят так называемые парольные взломщики – специализированные программы, которые служат для взлома паролей операционных систем.

Криптографические алгоритмы, применяемые для шифрования паролей пользователей в современных операционных системах, в подавляющем большинстве случаев являются слишком стойкими, чтобы можно было отыскать методы их дешифрования, более эффективные, чем тривиальный полный перебор. Поэтому парольные взломщики иногда просто шифруют все пароли с использованием того же самого криптографического алгоритма, который применяется для их засекречивания в атакуемой операционной системе, и сравнивают результаты шифрования с тем, что записано в системном файле, где находятся шифрованные пароли ее пользователей. При этом в качестве вариантов паролей парольные взломщики используют символьные последовательности, автоматически генерируемые из некоторого набора символов. Данный способ позволяет взломать все пароли, если известно их представление в зашифрованном виде, и они содержат только символы из данного набора. Максимальное время, которое потребуется для взлома пароля, можно вычислить по следующей формуле:

$$T = \frac{1}{S}\sum_{i=1}^{L} N^i,$$

где N – число символов в наборе, L – предельная длина пароля, S – количество проверок в секунду (зависит от операционной системы и быстродействия компьютера, на котором производится взлом ее парольной защиты). Анализ приведенной формулы показывает, что за счет большого числа перебираемых комбинаций, которое растет экспоненциально с увеличением числа символов в исходном наборе, такие атаки парольной защиты операционной системы могут занимать слишком много времени. Однако хорошо известно, что большинство пользователей операционных систем не особенно заботятся о выборе стойких паролей (т.е. таких, которые трудно взломать). Поэтому для более эффективного подбора паролей парольные взломщики обычно используют так называемые словари, представляющие собой заранее сформированный список слов, наиболее часто применяемых на практике в качестве паролей. Для каждого слова из словаря парольный взломщик использует одно или несколько правил. В соответствии с этими правилами слово изменяется и порождает дополнительное множество опробуемых паролей. Производится попеременное изменение буквенного регистра, в котором набрано слово, порядок следования букв в слове меняется на обратный, в начало и конец каждого слова приписывается цифра 1, некоторые буквы заменяются на близкие по начертанию цифры (например, password – pa55w0rd). Это повышает вероятность подбора пароля, поскольку в современных операционных системах, как правило, различаются пароли, набранные заглавными и строчными буквами, а пользователям этих систем рекомендуется выбирать пароли, в которых буквы чередуются с цифрами.

Одни парольные взломщики поочередно проверяют каждое слово из словаря, применяя к нему определенный набор правил для генерации дополнительного множества опробуемых паролей. Другие предварительно обрабатывают весь словарь при помощи этих же правил, получая новый словарь большего размера, и затем из него черпают проверяемые пароли. Учитывая, что обычные словари человеческих языков состоят всего из нескольких сотен тысяч слов, а скорость шифрования паролей достаточно высока, парольные взломщики, осуществляющие поиск с использованием словаря, работают достаточно быстро.

4.7.3.2. Взлом парольной защиты операционной системы UNIX

В операционной системе UNIX информацию о пароле любого пользователя можно отыскать в файле passwd, находящемся в каталоге etc. Эта информация хранится в зашифрованном виде и располагается через двоеточие сразу после имени соответствующего пользователя. Например, запись, сделанная в файле passwd относительно пользователя с именем bill, будет выглядеть примерно так:

bill:5fg63fhD3d5g:9406:12:Bill Spencer:/home/fsg/will:/bin/bash

Здесь 5fg63fhD3d5g – это и есть информация о пароле пользователя bill.

При первоначальном задании или изменении пользовательского пароля операционная система UNIX генерирует два случайных байта (в приведенном примере 5 и f), к которым добавляются байты пароля. Полученная в результате байтовая строка шифруется при помощи специальной криптографической процедуры Crypt (в качестве ключа используется пароль пользователя) и в зашифрованном виде (g63fhD3d5g) вместе с двумя случайными байтами (5f) записывается в файл /etc/passwd после имени пользователя и двоеточия.

Если злоумышленник имеет доступ к парольному файлу операционной системы UNIX, то он может скопировать этот файл на свой компьютер и затем воспользоваться одной из программ для взлома парольной защиты UNIX. Самой эффективной и популярной такой программой является Crack. И хотя она предназначена для запуска на компьютерах, работающих только под управлением операционных систем семейства UNIX, инициируемый ею процесс поиска паролей может быть без особых усилий распределен между различными платформами, подключенными к единой компьютерной сети. Среди них могут оказаться и IBM-совместимые персональные компьютеры с операционной системой Linux, и рабочие станции RS/6000 с AIX, и Macintosh с A/UX.

CrackJack – еще одна известная программа для взлома паролей операционной системы UNIX. К сожалению, работает она только под управлением операционной системы DOS, но зато весьма непритязательна в том, что касается компьютерных ресурсов. К другим недостаткам этого парольного взломщика можно отнести запрет на одновременное использование сразу нескольких словарей и принципиальную невозможность запуска CrackJack под Windows 96/98.

В отличие от CrackJack, парольный взломщик PaceCrack95 работает под Windows 95/98 в качестве полноценного DOS-приложения. К тому же он достаточно быстр, компактен и эффективен.

Парольные взломщики Q-Crack и John the Ripper примечательны тем, что существуют версии этих взломщиков, предназначенные для работы не только на DOS/Windows-платформах, но и на компьютерах с операционной системой Linux. А парольный взломщик Hades лучше остальных документирован и содержит ряд очень полезных утилит, которые позволяют осуществлять слияние нескольких словарей в один большой словарь, удалять из словаря повторяющиеся слова и добавлять в уже имеющийся словарь пароли, взломанные в процессе работы Hades.

Существует множество других программ взлома операционной системы UNIX. Что касается защиты от взлома паролей операционной системы UNIX, то ее пользователям следует порекомендовать применять только стойкие пароли, а в качестве критерия стойкости пароля использовать его отсутствие в словарях, предназначенных для парольных взломщиков. Да и сами файлы с информацией о пользовательских паролях следует прятать подальше. Достигается это обычно с помощью так называемого затенения (shadowing), когда в файле passwd шифрованные пароли пользователей заменяются служебными символами (например, звездочками), а вся парольная информация скрывается в каком-нибудь укромном месте. И хотя существуют программы, специально созданные для отыскания спрятанных парольных файлов операционной системы UNIX, к счастью для системных администраторов эти программы далеко не универсальны и успешно срабатывают не для всех операционных систем UNIX.

4.7.3.3. Взлом парольной защиты операционной системы Windows NT

База данных учетных записей пользователей

Одним из основных компонентов системы безопасности Windows NT является диспетчер учетных записей пользователей. Он обеспечивает взаимодействие других компонентов системы безопасности, приложений и служб Windows NT с базой данных учетных записей пользователей (Security Account Management Database, SAM). Эта база обязательно имеется на каждом компьютере с операционной системой Windows NT. В ней хранится вся информация, используемая для аутентификации пользователей Windows NT при интерактивном входе в

систему и при удаленном доступе к ней по компьютерной сети. База данных SAM представляет собой один из кустов (hive) системного реестра (registry) Windows NT. Этот куст принадлежит ветви (subtree) HKEY_LOCAL_MACHINE и называется SAM. Он располагается в каталоге \winnt_root\System32\Config (winnt_root – условное обозначение каталога с системными файлами Windows NT) в отдельном файле, который тоже называется SAM.

Информация в учетных записях базы данных SAM хранится в основном в двоичном виде. Доступ к ней обычно осуществляется через диспетчер учетных записей. Изменять записи, находящиеся в базе данных SAM, при помощи программ, позволяющих напрямую редактировать реестр Windows NT (REGEDT или REGEDT32), не рекомендуется. По умолчанию этого и нельзя делать, т.к. доступ к базе данных SAM запрещен для всех без исключения категорий пользователей операционной системы Windows NT.

Хранение паролей пользователей

В учетных записях базы данных SAM находится информация о пользовательских именах и паролях, которая необходима для идентификации и аутентификации пользователей при их интерактивном входе в систему. Как и в любой другой современной многопользовательской операционной системе, эта информация хранится в зашифрованном виде. В базе данных SAM каждый пароль пользователя обычно бывает представлен в виде двух 16-байтовых последовательностей, полученных разными методами. При использовании первого метода строка символов пользовательского пароля хэшируется с помощью функции MD4. В итоге из символьного пароля, введенного пользователем (до 14 символов), получается 16-байтовая последовательность – хэшированный пароль Windows NT. Данная последовательность затем шифруется по DES-алгоритму, и результат шифрования сохраняется в базе данных SAM. При этом в качестве ключа используется так называемый относительный идентификатор пользователя (Relative Identifer, RID), который представляет собой автоматически увеличивающийся порядковый номер учетной записи данного пользователя в базе данных SAM.

Для совместимости с другим программным обеспечением корпорации Microsoft (Windows for Workgroups, Windows 95/98 и Lan Manager) в базе данных SAM хранится также информация о пароле пользователя в стандарте Lan Manager. Для ее формирования используется второй метод. Все буквенные символы исходной строки пользовательского пароля приводятся к верхнему регистру, и, если пароль содержит меньше 14 символов, то он дополняется нулями. Из каждой 7-байтовой половины преобразованного таким образом пароля пользователя отдельно формируется ключ для шифрования фиксированной 8-байтовой последовательности по DES-алгоритму. Полученные в результате две 8-байтовые половины хэшированного пароля Lan Manager еще раз шифруются по DES-алгоритму (при этом в качестве ключа используется RID пользователя) и помещаются в базу данных SAM.

Использование пароля

Информация о паролях, занесенная в базу данных SAM, служит для аутентификации пользователей Windows NT. При интерактивном или сетевом входе в систему введенный пользователем пароль сначала хэшируется и шифруется, а затем сравнивается с 16-байтовой последовательностью, записанной в базе данных SAM. Если они совпадают, пользователю разрешается вход в систему.

Обычно в базе данных SAM хранятся в зашифрованном виде оба хэшированного пароля. Однако в некоторых случаях операционная система вычисляет только один из них. Например, если пользователь домена Windows NT изменит свой пароль, работая на компьютере с Windows for Workgroups, то в его учетной записи останется только пароль Lan Manager. А если пользовательский пароль содержит более 14 символов или если эти символы не входят в так называемый набор поставщика оборудования (original equipment manufacturer, OEM), то в базу данных SAM будет занесен только пароль Windows NT.

Возможные атаки на базу данных SAM

Обычно основным предметом стремления взломщика парольной защиты операционной системы являются административные полномочия. Их можно получить, узнав в хэшированном или символьном виде пароль администратора системы, который хранится в базе данных SAM. Поэтому именно на базу данных SAM бывает направлен главный удар взломщика парольной защиты Windows NT.

По умолчанию в операционной системе Windows NT доступ к файлу \winnt_root\System32\Config\SAM заблокирован для всех без исключения ее пользователей. Тем не менее, с помощью программы NTBACKUP любой обладатель права на резервное копирование

файлов и каталогов Windows NT может перенести этот файл с жесткого диска на магнитную ленту. Резервную копию реестра также можно создать утилитой REGBAK из Windows NT Resource Kit. Кроме того, явный интерес для любого взломщика представляют копия файла SAM (SAM.SAV) в каталоге \winnt_root\System32\Config и сжатая архивная копия SAM (файл SAM._) в каталоге \winnt_root\Repair.

При наличии физической копии файла SAM извлечь хранимую в нем информацию не представляет никакого труда. Загрузив файл SAM в реестр любого другого компьютера с Windows NT (например, с помощью команды Load Hive REGEDT32), можно в деталях изучить учетные записи пользователей, чтобы определить значения RID пользователей и шифрованные варианты их хэшированных паролей. Зная RID пользователя и имея зашифрованную версию его хэшированного пароля, компьютерный взломщик может попытаться расшифровать этот пароль, чтобы использовать его, например, для получения сетевого доступа к другому компьютеру. Однако для интерактивого входа в систему одного лишь знания хэшированного пароля недостаточно. Необходимо получить его символьное представление. Для восстановления пользовательских паролей операционной системы Windows NT в символьном виде существуют специальные парольные взломщики, которые выполняют как прямой подбор паролей, так и поиск по словарю. Одной из самых известных программ взлома паролей операционной системы Windows NT является LOphtCrack. Другим распространенным парольным взломщиком Windows NT является Advanced NT Security Explorer (сокращенно - ANTExp). ANTExp имеет удобный пользовательский интерфейс. Пользователь может задать набор символов, из которых будут формироваться последовательности, используемые в качестве вариантов паролей, а также верхнюю и нижнюю границы длины перебираемых паролей. Кроме того, можно выбрать тип атаки на парольную защиту Windows NT и применить либо атаку методом "грубой силы", либо словарную атаку.

Защита системы от парольных взломщиков

Итак, одной из главных задач системного администратора Windows NT является защита от несанкционированного доступа той информации, которая хранится в базе данных SAM. С этой целью ему, прежде всего, необходимо ограничить физический доступ к компьютерной сети и, прежде всего, – к контроллерам доменов. Дополнительно, при наличии соответствующих программно-аппаратных средств, следует установить пароли BIOS на включение компьютеров и на изменение настроек BIOS. Затем, используя настройки BIOS, рекомендуется отключить загрузку компьютеров с гибких и компакт-дисков. А для обеспечения контроля доступа к файлам и папкам операционной системы Windows NT системный раздел жесткого диска должен иметь формат NTFS.

Каталог \winnt_root\repair необходимо средствами операционной системы закрыть для доступа всех пользователей, включая администраторов, и разрешать к ней доступ только во время работы утилиты RDISK, создающей в этом каталоге архивные копии системного реестра Windows NT. Системные администраторы также должны внимательно следить затем, где и как хранятся дискеты аварийного восстановления (Emergency Repair Disks) и архивные копии на магнитных лентах, если на последних присутствует дубликат системного реестра Windows NT.

Для защиты базы данных SAM можно применить утилиту SYSKEY, входящую в состав пакета обновления Windows NT Service Pack 3. Эта утилита позволяет включить режим дополнительного шифрования информации о паролях, которая хранится в базе данных SAM. Уникальный 128-битовый ключ для дополнительного шифрования паролей (так называемый ключ шифрования паролей - Password Encryption Key, PEK) автоматически сохраняется в системном реестре для дальнейшего использования.

Перед помещением в системный реестр ключ PEK шифруется при помощи другого 128-битового ключа, который называется системным ключом (System Key), и может храниться либо в системном регистре, либо в файле с именем STARTUP.KEY в корневом каталоге на отдельной дискете. Можно не сохранять системный ключ на магнитном носителе, и тогда каждый раз при запуске операционной системы он будет вычисляться с помощью алгоритма MD5 на основе пароля, набираемого на клавиатуре в диалоговом окне утилиты SYSKEY.

Для повышения стойкости паролей пользователей операционной системы Windows NT к взлому рекомендуется с помощью утилиты Диспетчер пользователей (User Manager) задать минимальную длину пользовательских паролей равной не менее 8 символов и включить режим устаревания паролей, чтобы пользователи периодически их обновляли. При этом, чем выше вероятность атак на парольную защиту Windows NT, тем короче должен быть срок такого

устаревания. А чтобы пользователи не вводили свои старые пароли повторно, необходимо включить режим хранения некоторого числа ранее использовавшихся паролей.

В заключение отметим, что хотя в руках квалифицированного злоумышленника программы взлома паролей операционных систем представляют огромную опасность для их парольной защиты, сами парольные взломщики все же являются не менее ценным инструментом для системных администраторов, которые заинтересованы в выявлении слабых мест в парольной защите своих операционных систем. Основная проблема состоит не в том, что на свете существуют парольные взломщики, а в том, что ими недостаточно часто пользуются системные администраторы.

4.7.4. Аппаратно-программные средства защиты информации от НСД

Первые операционные системы (ОС) для персональных компьютеров не имели собственных средств защиты. Внедрение в современные ОС подсистем защиты не уменьшили актуальность проблемы защиты информации от НСД. Это связано, в основном, с тем, что практически любая система не способна защитить данные, находящиеся за ее пределами, например, при использовании сетевого информационного обмена.

Аппаратно-программные средства, обеспечивающие повышенный уровень защиты, можно разбить на пять основных групп.

Первую группу образуют системы идентификации и аутентификации пользователей. Такие системы применяются для ограничения доступа случайных и незаконных пользователей к ресурсам КС. Общий алгоритм работы этих систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить этому пользователю возможность работы с системой.

При построении подобных систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие типы:

- секретная информация, которой обладает пользователь (пароль, персональный идентификатор, секретный ключ и т.п.); эту информацию пользователь должен запомнить или же могут быть применены специальные средства хранения этой информации;
- физиологические параметры человека (отпечатки пальцев, "фотография" радужной оболочки глаза и т.п.) или какие-то особенности поведения человека.

Системы идентификации, основанные на первом типе информации, принято считать традиционными. Системы идентификации, использующие второй тип информации, называются биометрическими.

Вторую группу средств, обеспечивающих повышенный уровень защиты, составляют системы шифрования данных. Основная задача, решаемая такими системами, состоит в защите от несанкционированного использования данных, помещенных на магнитных носителях. Эта задача решается использованием симметричных алгоритмов шифрования данных. Основным классификационным признаком для комплексов шифрования служит уровень их встраивания в КС.

Работа прикладных программ с дисковыми накопителями состоит из двух этапов – "логического" и "физического". Логический этап соответствует уровню взаимодействия прикладной программы с ОС. На этом уровне основным объектом является файл. Физический этап соответствует уровню взаимодействия ОС и аппаратуры. В качестве объектов этого уровня выступают структуры физической организации данных – сектора диска. В результате системы шифрования данных могут осуществлять криптографические преобразования данных на уровне файлов и на уровне дисков.

К программам первого типа можно отнести архиваторы типа arj, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав известного программного пакета Norton Utilities.

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования, по которому системы шифрования делятся на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает

подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования, например, архиваторы со встроенными средствами парольной защиты.

К третьей группе средств, обеспечивающих повышенный уровень защиты, относятся системы шифрования данных, передаваемых по компьютерным сетям. Различают два основных способа шифрования: канальное и оконечное (абонентское). В случае канального шифрования защищается вся передаваемая по каналу связи информация, включая служебную. Соответствующие процедуры шифрования реализуются с помощью протокола канального уровня семиуровневой эталонной модели взаимодействия открытых систем (ЭМВОС). Этот способ шифрования обладает следующим достоинством: встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у этого подхода имеются существенные недостатки:

- шифрованию на данном уровне подлежит вся информация, включая служебные данные транспортных протоколов; это осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммутации (шлюзах, ретрансляторах и т.п.);
- шифрование служебной информации, неизбежное на данном уровне, может привести к появлению статистических закономерностей в шифрованных данных; это влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

Оконечное шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя прикладными объектами (абонентами). Оконечное шифрование реализуется с помощью протокола прикладного или представительного уровня модели ЭМВОС. В этом случае защищенным оказывается только содержание сообщения, вся служебная информация остается открытой. Данный способ позволяет избежать проблем, связанных с шифрованием служебной информации, но при этом возникают другие проблемы. В частности, злоумышленник, имеющий доступ к каналам связи компьютерной сети, получает возможность анализировать информацию о структуре обмена сообщениями, например, об отправителе и получателе, о времени и условии передачи данных, а также об объеме передаваемых данных.

Четвертую группу средств защиты составляют системы аутентификации электронных данных. При обмене электронными данными по сетям связи возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации электронных данных применяют код аутентификации сообщения (имитовставку) или электронную цифровую подпись. При формировании кода аутентификации сообщения и электронной цифровой подписи используются разные типы систем шифрования. Код аутентификации сообщения формируют с помощью симметричных систем шифрования данных. В частности, симметричный алгоритм шифрования данных DES при работе в режиме сцепления блоков шифра CBC позволяет сформировать с помощью секретного ключа и начального вектора IV код аутентификации сообщения MAC. Проверка целостности принятого сообщения осуществляется путем проверки кода MAC получателем сообщения.

Аналогичные возможности предоставляет отечественный стандарт симметричного шифрования данных ГОСТ 28147-89. В этом алгоритме предусмотрен режим выработки имитовставки, обеспечивающий имитозащиту, т.е. защиту системы шифрованной связи от навязывания ложных данных. Имитовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем сообщения, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.

Электронная цифровая подпись (ЭЦП) представляет собой относительно небольшое количество дополнительной аутентифицирующей цифровой информации, передаваемой вместе с пописываемым текстом. Для реализации ЭЦП используются принципы асимметрического шифрования. Система ЭЦП включает процедуру формирования цифровой подписи отправителем с использованием секретного ключа отправителя и процедуру проверки подписи получателя с использованием открытого ключа отправителя.

Пятую группу средств, обеспечивающих повышенный уровень защиты, образуют средства управления ключевой информацией, под которой понимается совокупность всех используемых в компьютерной системе или сети криптографических ключей. Безопасность любого криптографического алгоритма определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в КС.

Основным классификационным признаком средств управления ключевой информацией является вид функции управления ключами. Различают следующие основные виды функций управления ключами: генерация ключей, хранение ключей и распределение ключей.

Способы генерации ключей различаются для симметричных и асимметричных криптосистем. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел, в частности схемы с применением блочного симметричного алгоритма шифрования. Генерация ключей для асимметричных криптосистем представляет существенно более сложную задачу в связи с необходимостью получения ключей с определенными математическими свойствами.

Функция хранения ключей предполагает организацию безопасного хранения, учета и удаления ключей. Для обеспечения безопасного хранения и передачи ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входят главный ключ (мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключей являются критическими вопросами криптографической защиты.

Распределение ключей является самым ответственным процессом в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также оперативность и точность их распределения. Различают два основных способа распределения ключей между пользователями компьютерной сети:

- применение одного или нескольких центров распределения ключей;
- прямой обмен сеансовыми ключами между пользователями.

Существуют различные программно-аппаратные комплексы (АПК) защиты компьютерной информации от НСД. Они имеют много общего. Рассмотрим сертифицированный Гостехкомиссией РФ АПК Secret Net, разработанный "Инормзацитой", одной из ведущих организаций России в области информационной безопасности. АПК Secret Net реализован как в автономном, так и в сетевом (локальные сети) вариантах. Автономный вариант системы защиты информации Secret Net предназначен для защиты ресурсов рабочей станции локальной сети или неподключенного к сети компьютера. АПК Secret Net функционирует во взаимодействии с разными операционными системами. Рассмотрим для определенности вариант системы Secret Net NT, функционирующий в среде ОС Windows NT. Система Secret Net дополняет стандартные защитные механизмы ОС Windows NT функциями, обеспечивающими:

- идентификацию пользователей при помощи специальных аппаратных средств (Touch Memory, Smart Card, Smarty, eToken);
- дополнительно к избирательному (дискреционному) управлению доступом, реализованному в ОС Windows NT, полномочное (мандатное) управление доступом пользователей к конфиденциальной информации на локальных и подключенных сетевых дисках;
- оперативный контроль над работой пользователей компьютера путем регистрации событий, связанных с безопасностью ИС. Удобные средства просмотра и представления зарегистрированной информации;
- контроль целостности программ, используемых пользователями и операционной системой;
- возможность создания для любого пользователя замкнутой программной среды (списка разрешенных и запрещенных для запуска программ);
- простоту управления объектами благодаря использованию механизма шаблонов настроек.

Комплекс включает в себя следующие компоненты и подсистемы:

- ядро системы защиты;
- подсистема управления;
- подсистема криптографической защиты информации;
- база данных системы защиты;
- подсистема избирательного управления доступом;
- подсистема разграничения доступа к дискам;

- подсистема разграничения полномочного доступа;
- подсистема замкнутой программной среды;
- подсистема контроля целостности;
- подсистема контроля входа.

Ядро системы защиты

Ядро системы защиты представляет собой программу, которая автоматически запускается на защищенном компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Ядро системы осуществляет управление подсистемами и компонентами системы защиты и обеспечивает их взаимодействие. В процессе работы системы защиты ядро выполняет следующие функции:

- обеспечивает обмен данными между компонентами системы и обработку команд, поступающих от этих компонент;
- обеспечивает доступ других компонент системы к информации, хранящейся в базе данных системы защиты;
- осуществляет сбор сведений о состоянии компьютера;
- контролирует доступ пользователя к ресурсам компьютера;
- обрабатывает информацию, поступающую от компонент системы защиты, о событиях, происходящих на компьютере и связанных с безопасностью системы, и осуществляет их регистрацию в журнале безопасности ОС Windows NT.

Подсистема регистрации

Подсистема регистрации является одним из элементов ядра системы и предназначена для управления регистрацией в журнале безопасности Windows NT событий, связанных с работой ОС и Secret Net. Эта информация поступает от отдельных подсистем системы защиты, которые следят за происходящими в информационной среде событиями.

Регистрация событий осуществляется системными средствами (ОС Windows NT) или средствами системы защиты Secret Net NT. Перечень регистрируемых событий устанавливается администратором с помощью подсистемы управления. Для просмотра журнала используется специальная программа подсистемы управления, обладающая развитыми средствами работы с журналами регистрации.

Подсистема управления

Подсистема управления располагает средствами для настройки защитных механизмов через управление общими параметрами работы компьютера, свойствами пользователей и групп пользователей. В частности она обеспечивает:

- отображение и управление состоянием защищаемого компьютера;
- управление пользователями, настройками компьютера и сохранение относящихся к ним данных в БД системы защиты;
- получение информации из БД системы защиты;
- обработку и представление информации из журнала безопасности ОС Windows NT.

В состав подсистемы управления входит программа, предназначенная для просмотра журнала безопасности. С ее помощью можно выполнить: просмотр, отбор, сортировку, поиск записей, печать, экспорт журнала в другие форматы.

База данных Secret Net

База данных Secret Net предназначена для хранения сведений, необходимых для работы защищенного компьютера. БД Secret Net размещается в реестре ОС Windows NT и содержит информацию об общих настройках системы защиты, свойствах пользователей и групп пользователей.

Доступ подсистем и компонент системы защиты к данным, хранящимся в БД

Secret Net, обеспечивается ядром системы защиты. Первоначальное заполнение БД выполняется при установке Secret Net. Для этого используются данные, содержащиеся в БД безопасности Windows NT (политика безопасности, состав пользователей и групп пользователей и т.д.), и данные, устанавливаемые по умолчанию для Secret Net (значения общих параметров, некоторые свойства пользователей, набор шаблонов и т.д.). Синхронизацию данных в БД безопасности Windows NT и БД Secret Net обеспечивает ядро системы защиты. В дальнейшем информация, содержащаяся в БД, создается и модифицируется подсистемой управления и другими подсистемами.

Подсистема избирательного управления доступом

Подсистема избирательного управления доступом обеспечивает разграничение доступа пользователей к ресурсам файловой системы, аппаратным ресурсам и ресурсам операционной системы компьютера. Для управления доступом к ресурсам файловой системы, системному реестру и системным средствам управления компьютером используются стандартные средства ОС Windows NT, а непосредственное управление осуществляется с использованием интерфейса Secret Net NT. Для управления доступом к дискам и портам используются средства Secret Net NT.

Подсистема полномочного управления доступом

Подсистема полномочного управления доступом обеспечивает разграничение доступа пользователей к конфиденциальной информации, хранящейся в файлах на локальных и сетевых дисках. Доступ осуществляется в соответствии с категорией конфиденциальности, присвоенной информации, и уровнем допуска пользователя к конфиденциальной информации.

Подсистема полномочного управления доступом включает в себя: драйвер полномочного управления доступом и компоненту управления допуском к ресурсам. Компонента управления конфиденциальностью ресурсов включается в программу “Проводник” (Explorer). Из программы “Проводник” и осуществляется управление категориями конфиденциальности, которые присваиваются файлам. Диски обязательно должны быть размечены для работы с файловой системой NTFS. Драйвер полномочного управления доступом контролирует доступ пользователей к конфиденциальным ресурсам. Когда пользователь (или программа, запущенная пользователем) осуществляет попытку выполнить какую-либо операцию над конфиденциальным ресурсом, драйвер определяет категорию конфиденциальности ресурса и передает ее диспетчеру доступа, входящему в состав ядра системы защиты. Диспетчер доступа сопоставляет категорию конфиденциальности ресурса и уровень допуска данного пользователя к конфиденциальной информации. Также он проверяет, не противоречат ли действия пользователя с ресурсом другим настройкам системы (например, условиям копирования через буфер обмена). Если уровень допуска или настройки системы не позволяют выполнить операцию, диспетчер доступа передает драйверу запрещающую команду, и операция блокируется. При этом подсистема регистрации ядра системы фиксирует в журнале попытку несанкционированного доступа.

Подсистема замкнутой программной среды

Подсистема замкнутой программной среды позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска. Драйвер замкнутой программной среды контролирует запуск пользователем программ. Когда пользователь (программа, запущенная пользователем) осуществляет попытку запуска какой-либо программы, драйвер передает диспетчеру доступа, входящему в состав ядра системы защиты, сведения о запускаемой программе. Диспетчер доступа проверяет, включена ли эта программа в персональный список программ, разрешенных для запуска. Если программа содержится в списке, диспетчер доступа передает драйверу разрешающую команду. Если пользователю запрещено запускать данную программу, диспетчер доступа передает драйверу запрещающую команду, и запуск программы блокируется. В этом случае подсистема регистрации фиксирует в журнале безопасности попытку несанкционированного доступа.

Подсистема контроля входа

Подсистема контроля входа обеспечивает идентификацию и аутентификацию пользователя при его входе в систему. Подсистема включает в себя модуль идентификации пользователя, а также может содержать средства аппаратной поддержки, например, Secret Net TM Card или Электронный замок “Соболь”, если они установлены на компьютере, и программу-драйвер, с помощью которой осуществляется управление аппаратными средствами.

Подсистема контроля входа запрашивает и получает информацию о входящем в систему пользователе (имя, пароль, персональный идентификатор пользователя). Затем сравнивает полученную информацию с информацией, хранящейся в БД системы защиты. Предоставление информации из БД обеспечивает ядро системы за

щиты. Если в БД отсутствует информация о пользователе, вход пользователя в систему запрещается.

Для целей идентификации и аутентификации могут использоваться аппаратные средства. Для управления ими необходимы специальные программы-драйверы, которые обеспечивают обмен информацией между устройствами аппаратной поддержки и модулями системы защиты. Драйверы входят в комплект поставки и устанавливаются на компьютер вместе с системой Secret

Net NT. При загрузке компьютера подсистема контроля целостности проверяет целостность системных файлов. Если целостность файлов не нарушена, подсистема контроля целостности передает управление подсистеме идентификации пользователя. В случае нарушения целостности файлов вход пользователя в систему может быть запрещен.

Подсистема контроля целостности

Подсистема контроля целостности осуществляет слежение за неизменностью контролируемых объектов (файлов, ключей системного реестра и т.д.) с целью защиты их от модификации. Для этого определяется перечень контролируемых объектов. Для каждого из входящих в него объектов рассчитываются эталонные значения контролируемых параметров. Вычисления контрольных сумм проводятся с использованием хеш-функций (в соответствии с ГОСТ Р 34-10) или по оригинальному (быстрому) алгоритму собственной разработки. Эталонные контрольные суммы и другие значения контролируемых параметров для проверяемых объектов, а также информация о размещении объектов хранятся в пакетах контроля целостности. Целостность объектов контролируется в соответствии с установленным расписанием. Подсистема контроля входа передает подсистеме контроля целостности перечень контролируемых объектов и порядок их контроля при запуске компьютера.

Ядро системы передает подсистеме контроля целостности расписание контроля, составленное администратором с помощью подсистемы управления. В соответствии с расписанием контроля текущие значения контролируемых параметров сравниваются с ранее полученными их эталонными значениями. Если выявляется нарушение целостности объектов, подсистема контроля целостности сообщает об этом диспетчеру доступа.

Защитные механизмы

Система Secret Net NT дополняет операционную систему Windows NT рядом защитных средств, которые можно отнести к следующим группам.

1. Средства защиты от несанкционированного входа в систему:

- механизм идентификации и аутентификации пользователей (в том числе с помощью аппаратных средств защиты);
- функция временной блокировки компьютера на время паузы в работе пользователя для защиты компьютера от использования посторонним лицом;
- аппаратные средства защиты от загрузки ОС с гибкого диска.

2. Средства управления доступом и защиты ресурсов:

- разграничение доступа пользователей к ресурсам компьютера с использованием механизмов избирательного и полномочного управления доступом;
- создание для любого пользователя замкнутой программной среды (списка разрешенных для запуска программ);
- функция затирания удаленных данных на локальных дисках.

3. Средства регистрации и оперативного контроля:

- политика регистрации, ведение журнала регистрации событий, имеющих отношение к безопасности системы. Работа с журналом, управление временем хранения и удалением записей;
- контроль целостности файлов; управление расписанием контроля и выбор реакции на нарушение целостности;
- контроль аппаратной конфигурации компьютера.

Отличительной особенностью системы Secret Net NT является возможность гибкого управления набором защитных средств системы. Пользователь, имеющий привилегии на администрирование системы, может активизировать различные комбинации защитных механизмов системы, выбирая из них только необходимые и устанавливая соответствующие режимы их работы.

Механизмы контроля входа в систему

Защита от несанкционированного входа предназначена для предотвращения доступа посторонних пользователей к защищенному компьютеру. К этой группе средств, как уже говорилось, могут быть отнесены:

- программные и аппаратные средства идентификации и аутентификации;
- функция временной блокировки компьютера;
- аппаратные средства защиты от загрузки ОС с гибкого диска.

Механизм идентификации и аутентификации пользователей

Идентификация и аутентификация пользователей выполняется при каждом входе пользователя в систему. При загрузке компьютера система Secret Net NT запрашивает у пользователя его идентификатор и пароль. Затем проверяется, был ли зарегистрирован в системе пользователь с таким именем и правильно ли указан его пароль. В качестве идентификаторов могут использоваться: уникальные имена и уникальные номера аппаратных устройств идентификации (персональных идентификаторов). В Secret Net NT поддерживается работа с паролями длиной до 16 символов. Если пароль указан неверно, в журнале безопасности регистрируется попытка несанкционированного доступа к компьютеру. При определенном числе неверных попыток ввода пароля происходит блокировка учетной записи пользователя. Идентификаторы пользователей (имена и номера аппаратных идентификаторов) хранятся в базе данных системы защиты в открытом виде, а пароли пользователей – в кодированном виде.

Аппаратные средства защиты от несанкционированного входа

Средства аппаратной поддержки в системах защиты предназначены для обеспечения работы различных электронных идентификаторов (Touch Memory, Smart Card, Smarty, eToken). А при использовании электронного замка "Соболь" появляются дополнительные возможности:

- контроля загрузки ОС со съемных носителей (гибких и компакт-дисков);
- контроля целостности файлов и секторов дисков до загрузки ОС.

Работу системы защиты с аппаратными средствами обеспечивают специальные программы-драйверы, управляющие обменом информацией между устройством и модулями системы защиты. В системе Secret Net NT предусмотрено несколько режимов идентификации и аутентификации с использованием аппаратных средств. Это дает возможность проводить их внедрение поэтапно. При "мягком" режиме работы любой пользователь может войти в систему либо предъявив персональный идентификатор, либо указав свое имя. При "жестком" режиме вход в систему любого пользователя разрешен только при предъявлении персонального идентификатора.

Функция временной блокировки компьютера

Функция временной блокировки компьютера предназначена для предотвращения использования компьютера посторонними лицами. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора (хранителем экрана). Включить режим временной блокировки компьютера может сам пользователь, нажав определенную, заданную им, комбинацию клавиш. Компьютер может быть заблокирован и автоматически после некоторого периода простоя. Длительность этого интервала устанавливается настройкой параметров. Для снятия блокировки необходимо указать пароль текущего пользователя.

Механизмы управления доступом и защиты ресурсов

Система Secret Net NT включает в свой состав несколько механизмов управления доступом пользователей к ресурсам компьютера:

- механизм избирательного управления доступом;
- механизм полномочного управления доступом;
- механизм замкнутой программной среды.

Все ресурсы компьютера в системе Secret Net NT делятся на три типа:

1. Ресурсы файловой системы. Локальные логические диски и размещающиеся на них каталоги и файлы.

2. Аппаратные ресурсы. Локальные и сетевые принтеры, коммуникационные порты, физические диски, дисководы, приводы CD ROM.

3. Ресурсы операционной системы. Системные файлы, ключи системного реестра, системное время, диалоги настройки параметров системы.

Механизм полномочного управления доступом и механизм замкнутой программной среды применяются только к ресурсам файловой системы.

Механизм избирательного управления доступом

Управление избирательным доступом к локальным ресурсам компьютера осуществляется на основании предоставления пользователям компьютера прав и привилегий. В Secret Net NT для управления доступом к ресурсам файловой системы, системному реестру и системным средствам управления компьютером используются стандартные механизмы ОС Windows NT. Для управления доступом к дискам и портам используются собственные механизмы системы Secret Net NT.

Механизм полномочного управления доступом

Система Secret Net NT включает в свой состав средства, позволяющие организовать полномочное (мандатное) управление доступом пользователей к конфиденциальной информации. При организации полномочного управления доступом для каждого пользователя компьютера устанавливается некоторый уровень допуска к конфиденциальной информации. Файлам и каталогам, находящимся на локальных дисках компьютера или на подключенных сетевых дисках, назначается категория конфиденциальности, которая определяется специальной меткой, устанавливаемой на файл. Используются три категории конфиденциальности информации: “Нет” (для общедоступной информации), “Конфиденциально”, “Строго конфиденциально”. Доступ к конфиденциальным файлам осуществляется следующим образом. Когда пользователь (программа, запущенная пользователем) осуществляет попытку доступа к конфиденциальному каталогу или находящемуся в нем файлу, диспетчер доступа Secret Net NT определяет категорию конфиденциальности данного ресурса. Затем категория конфиденциальности ресурса сопоставляется с уровнем допуска пользователя к конфиденциальной информации. Если текущий пользователь не превышает свой уровень допуска, то ему предоставляется доступ к ресурсу. При работе системы Secret Net NT в режиме полномочного управления доступом контролируются потоки конфиденциальной информации. Это позволяет, например, предотвратить копирование конфиденциальных документов в неконфиденциальные области дисков и запретить свободный доступ к принтерам. Печать конфиденциальных документов в этом случае осуществляется под контролем системы защиты.

Механизм замкнутой программной среды

Механизм замкнутой программной среды позволяет без использования системы атрибутов ограничить доступ пользователей к исполняемым файлам только теми программами, которые действительно необходимы ему для выполнения своих служебных обязанностей. Перечень программ, разрешенных и запрещенных для запуска, определяется индивидуально для каждого пользователя и фиксируется в UEL-файле. Список может быть сформирован автоматически на основании сведений об используемых программах из журнала безопасности и отредактирован средствами специального редактора SnEdit.

Механизмы контроля и регистрации

Система Secret Net NT включает в свой состав следующие средства, позволяющие контролировать ее работу:

- механизм регистрации событий;
- механизм проверки целостности.

Механизм регистрации событий

В процессе работы системы Secret Net NT события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журнале безопасности Windows NT. События описываются следующими характеристиками:

- дата и время, определяющие момент наступления события;
- идентификатор пользователя, действия которого привели к появлению события;
- краткая характеристика события;
- имя программы, работа которой привела к появлению события;
- ресурс, при работе с которым произошло событие.

В общей сложности в журнал заносятся сведения более чем о ста видах событий. Механизм регистрации событий обладает гибкими возможностями управления. Для каждого пользователя можно определить индивидуальный режим регистрации. От общего объема регистрируемых событий зависит размер журнала и, соответственно, время записи и последующего анализа событий. Для журнала безопасности может быть установлен предельный срок хранения регистрационных записей, по истечении которого устаревшие записи будут автоматически удаляться из журнала. Право на настройку режимов регистрации событий предоставляется пользователю посредством соответствующих привилегий на администрирование системы.

Механизм проверки целостности

Контроль целостности предназначен для слежения за изменениями характеристик выбранных объектов информационной среды. Объектами контроля могут быть: файлы, каталоги, элементы системного реестра и секторы дисков (последние только при использовании электронного замка "Соболь"). Каждый тип объектов имеет свой набор контролируемых данных. Так, например, файлы могут контролироваться на целостность содержимого, прав доступа,

атрибутов, а также на их существование, т.е. на наличие по заданному пути. Кроме того, для каждого из типов объектов могут использоваться различные алгоритмы контроля целостности. В системе предусмотрена гибкая возможность выбора времени контроля. В частности, контроль может быть выполнен при загрузке ОС, при входе или выходе пользователя из системы, по заранее составленному расписанию. Кроме того, может быть проведен и немедленный контроль. При обнаружении несоответствия предусмотрены следующие варианты реакции на возникающие ситуации:

- регистрация изменений в системном журнале;
- блокировка компьютера;
- отклонение или принятие изменений.

Для каждого типа контролируемых объектов на рабочей станции хранятся список имен объектов и задания для контроля тех или иных характеристик указанных объектов. Эта информация размещается в базе данных подсистемы контроля целостности, которая реализована в виде набора файлов определенного формата, расположенных в отдельном каталоге. База данных содержит всю необходимую информацию для функционирования подсистемы. Задание на контроль содержит необходимую информацию об эталонном состоянии объекта, порядке контроля характеристик и действий, которые надо выполнить при обнаружении изменений. Результаты контроля и обработки запросов фиксируются в журнале безопасности. Подсистема контроля целостности взаимодействует с другими подсистемами через ядро системы защиты. Для просмотра и редактирования списков контроля целостности, режимов контроля и номенклатуры контролируемых объектов используется подсистема управления. Кроме того, подсистема контроля целостности самостоятельно выполняет контроль объектов и взаимодействует для выполнения различных действий со следующими подсистемами Secret Net:

- подсистемой контроля входа – для получения информации о входе или выходе пользователя из системы;
- подсистемой регистрации – для регистрации событий в журнале безопасности;
- подсистемой криптографической защиты – для выполнения криптографических операций при контроле целостности.
- Подсистема контроля целостности используется в нескольких типичных случаях:
- для контроля в автоматическом режиме целостности объектов по установленному расписанию;
- для выполнения внеплановых проверок по указанию администратора системы;
- для обработки запросов от программы управления с целью просмотра и изменения характеристик контролируемых объектов.

Контроль аппаратной конфигурации компьютера

Контроль аппаратной конфигурации компьютера предназначен для своевременного обнаружения изменений конфигурации и выбора наиболее целесообразного способа реагирования на эти изменения. Изменения аппаратной конфигурации компьютера могут быть вызваны: выходом из строя, добавлением или заменой отдельных компонентов компьютера. Для эффективного контроля конфигурации используется широкий набор контролируемых параметров, с каждым из которых связаны правила обнаружения изменений и действия, выполняемые в ответ на эти изменения. Сведения об аппаратной конфигурации компьютера хранятся в БД системы защиты. Первоначальные (эталонные) данные о конфигурации поступают от программы установки. Каждый раз при загрузке компьютера, а также при повторном входе пользователя, система получает сведения об актуальной аппаратной конфигурации и сравнивает ее с эталонной.

Контроль конфигурации аппаратных средств производится ядром системы Secret Net. По результатам контроля ядро принимает решение о необходимости блокировки компьютера. Решение принимается после входа пользователя и зависит от настроек пользователя. Значение настроек пользователя определяет администратор

безопасности.

Средства аппаратной поддержки Secret Net

В качестве средств аппаратной поддержки в Secret Net могут быть использованы следующие устройства.

- **Secret Net NT ROM BIOS** – микросхема с расширением BIOS, устанавливается на сетевой карте компьютера в кроватку для микросхемы удаленной загрузки. Обеспечивает запрет загрузки компьютера с гибких дисков и компакт-дисков.

- **Secret Net Touch Memory Card** – плата с разъемом для подключения считывателя Touch Memory или считывателя бесконтактных радиокарт Proximity, устанавливаемая внутри компьютера в разъем ISA или PCI. Обеспечивает идентификацию пользователей по электронным идентификаторам Touch Memory или картам Proximity.
- **Контроллер "Соболь"** – плата с разъемом для подключения считывателя Touch Memory, аппаратным датчиком случайных чисел, двумя (четырьмя) каналами физической блокировки устройств и внутренней энергонезависимой памятью. Устанавливается внутри компьютера в разъем ISA или PCI. В системе Secret Net может быть использован для идентификации пользователей до загрузки ОС, а также для генерации криптографических ключей.
- **Считыватель Smart Card** – устройство, подключаемое к COM-порту, устанавливаемое внутри корпуса компьютера или интегрированное в компоненты компьютеров (клавиатуру, системный блок) и предназначенное для обеспечения работы со Smart-картами. В системе Secret Net используется для идентификации пользователей по Smart-картам до загрузки операционной системы, а также хранения во внутренней памяти карты дополнительной информации. Поддерживаются PC/SC совместимые считыватели Smart Card.
- **Smarty** – устройства для работы со Smart-картами, использующие стандартное устройство для чтения 3,5"-дискет. В системе Secret Net используются для идентификации пользователей по Smart-картам до загрузки операционной системы, а также для хранения во внутренней памяти карты дополнительной информации. Поддерживаются PC/SC совместимые считыватели Smart Card.
- **Считыватель бесконтактных радиокарт Proximity**. Подключается к разъему Secret Net Touch Memory Card и устанавливается внутри корпуса компьютера. В системе Secret Net используется для идентификации пользователей по картам Proximity до загрузки ОС.
- **Электронный идентификатор eToken R2**. Используется для аутентификации пользователя при входе в систему и для хранения ключевой информации. Подключается к USB-порту компьютера.

4.7.5. Проблемы обеспечения безопасности в глобальных сетях

Глобальная сеть Internet создавалась как открытая система, предназначенная для свободного обмена информацией. В силу открытости своей идеологии Internet представляет для злоумышленников значительно большие возможности по сравнению с традиционными информационными системами. Через Internet нарушитель может:

- вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;
- незаконно скопировать важную и ценную для предприятия информацию;
- получить пароли, адреса серверов и их содержимое;
- входить в информационную систему предприятия под именем зарегистрированного пользователя и т.д.

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны. В отечественной литературе до последнего времени использовались вместо этого термина другие термины: брандмауэр и firewall. Вне компьютерной сферы брандмауэром (или firewall) называют стену, сделанную из негорючих материалов и препятствующую распространению пожара. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от фигурального пожара – попыток злоумышленников вторгнуться во внутреннюю сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети.

Межсетевой экран (МЭ) – это система межсетевой защиты, позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия. МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение – пропускать его или отбросить. Для того чтобы МЭ мог осуществить это, ему необходимо определить набор правил фильтрации.

Обычно межсетевые экраны защищают внутреннюю сеть предприятия от "вторжений" из глобальной сети Internet, однако они могут использоваться и для защиты от "нападений" из корпоративной интрасети, к которой подключена локальная сеть предприятия. Ни один МЭ не может гарантировать полной защиты внутренней сети при всех возможных обстоятельствах. Однако для большинства коммерческих организаций установка МЭ является необходимым условием обеспечения безопасности внутренней сети. Главный довод в пользу применения МЭ состоит в том, что без него системы внутренней сети подвергаются опасности со стороны слабо защищенных служб сети Internet, а также зондированию и атакам с каких-либо других хост-компьютеров внешней сети.

Проблемы недостаточной информационной безопасности являются "традиционными" практически для всех протоколов и служб Internet. Большая часть этих проблем связана с исторической зависимостью Internet от операционной системы UNIX. Известно, что сеть Arpanet строилась как сеть, связывающая исследовательские центры, научные, военные и правительственные учреждения, крупные учреждения США. Эти структуры использовали операционную систему UNIX в качестве платформы для коммуникаций и решения собственных задач. Поэтому особенности методологии программирования в среде UNIX и ее архитектуры наложили отпечаток на реализацию протоколов обмена и политики безопасности сети. Из-за открытости и распространенности система UNIX стала любимой добычей хакеров. Поэтому совсем не удивительно, что набор проколов TCP/IP, который обеспечивает коммуникации в глобальной сети Internet и в интрасетях, имеет "врожденные" недостатки защиты.

Наилучшим из известных в настоящее время сертифицированных аппаратно-программных комплексов, способных решить проблему защиты от всевозможных атак "извне", является разработанный "Информзащитой" "Континент-К", являющийся реализацией идеологии VPN (Virtual Private Network). Технология VPN позволяет формировать виртуальные защищенные каналы в сетях общего пользования (например, Internet), гарантирующие конфиденциальность и достоверность информации. VPN-сеть представляет собой объединение локальных сетей (ЛВС) или отдельных компьютеров, подключенных к сети общего пользования, в единую защищенную виртуальную сеть. Растущий интерес к данной технологии обусловлен следующими факторами:

- низкой стоимостью эксплуатации за счет использования сетей общего пользования вместо собственных или арендуемых линий связи;
- практически неограниченной масштабируемостью;
- простотой изменения конфигурации и наращивания корпоративной сети;
- “прозрачностью” для пользователей и приложений.

Переход от распределенной корпоративной сети на базе выделенных каналов к VPN на основе сетей общего пользования позволяет существенно снизить эксплуатационные расходы. Но использование сетей общего пользования для организации VPN предъявляет дополнительные требования к обеспечению защиты информационных ресурсов предприятия от несанкционированного доступа (НСД). Для надежной защиты информации в VPN и предназначен аппаратно-программный комплекс "Континент-К". Этот комплекс обеспечивает защиту конфиденциальной информации в корпоративных VPN-сетях, использующих протоколы семейства TCP/IP. В качестве составных частей VPN могут выступать ЛВС предприятия или их отдельные фрагменты.

Аппаратно-программный комплекс “Континент-К” обеспечивает:

- защиту внутренних сегментов сети от несанкционированного доступа со стороны пользователей сетей общего пользования;
- скрытие внутренней структуры защищаемых сегментов сети;
- криптографическую защиту данных, передаваемых по каналам связи сетей общего пользования между защищаемыми сегментами сети (абонентскими пунктами);
- безопасный доступ пользователей VPN к ресурсам сетей общего пользования;
- централизованное управление настройками VPN-устройств сети.

Комплекс “Континент-К” включает в свой состав следующие компоненты:

- центр управления сетью криптографических шлюзов;
- криптографический шлюз;
- программа управления сетью криптографических шлюзов.

Центр управления сетью (ЦУС) осуществляет управление работой всех КШ, входящих в состав виртуальной сети. ЦУС осуществляет контроль над состоянием всех зарегистрированных

КШ, проводит рассылку ключевой информации, предоставляет администратору функции удаленного управления КШ, обеспечивает получение и хранение содержимого системных журналов КШ, а также ведение журнала событий НСД.

Криптографический шлюз (КШ) обеспечивает криптографическую защиту информации при ее передаче по открытым каналам сетей общего пользования и защиту внутренних сегментов сети от проникновения извне.

Программа управления обеспечивает отображение состояний КШ, просмотр содержимого системных журналов КШ, изменение настроек маршрутизации и правил фильтрации пакетов.

Комплекс *"Континент-К"* может использоваться в следующих вариантах:

- защита соединения «точка-точка»;
- защищенная корпоративная VPN-сеть.

Рис. 7.1. Защита соединения «точка-точка»

Защита соединения «точка-точка» (рис. 7.1) предполагает использование КШ для защиты данных, передаваемых по неконтролируемой территории между двумя защищенными сегментами территориально разделенных ЛВС через сеть Internet или по выделенному каналу связи. В этом случае обеспечивается шифрование и имитозащита данных, передаваемых между двумя защищенными сегментами разделенной ЛВС. Управление параметрами КШ осуществляется из той ЛВС, в которой установлена программа управления и на криптошлюзе которой установлен центр управления сетью.

Защищенная корпоративная VPN-сеть (рис. 7.2) предполагает, что защищаемые сегменты сети предприятия объединены между собой через каналы передачи данных сети общего пользования (выделенные каналы различной пропускной способности, в том числе сеть Internet). В этом случае обеспечивается:

- шифрование и имитозащита данных, передаваемых по каналам связи;
- аутентификация удаленных абонентов;
- фильтрация входящих и исходящих *IP*-пакетов;
- скрытие внутренней структуры каждого защищаемого сегмента сети;
- распределение и управление сменой ключей шифрования.

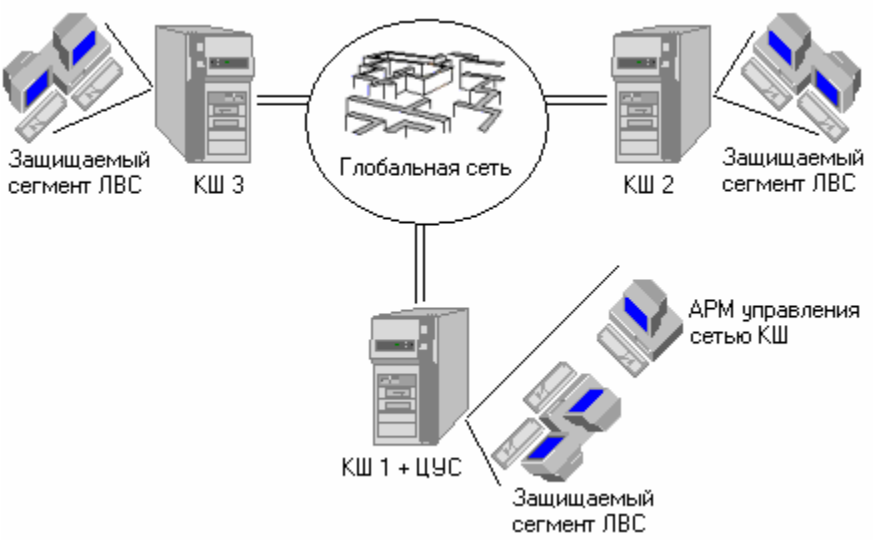


Рис. 7.2. Защищенная корпоративная сеть

Для централизованного управления работой КШ (настройка, контроль состояния, распределение ключей шифрования и т.д.) используются центр управления сетью и программа управления. Центр управления сетью устанавливается на одном из криптошлюзов сети. Программа управления может быть установлена на компьютерах внутри защищаемых центром управления сегментов сети. Оповещение администратора о попытках НСД осуществляется на АРМ управления сетью. Шифрование передаваемой информации для пользователей VPN является прозрачным.

В аппаратно-программном комплексе используется симметричная ключевая система. Криптографическое соединение между КШ в сети осуществляется на ключах парной связи. Шифрование каждого пакета производится на индивидуальном ключе, который формируется из ключа парной связи. Для шифрования данных используется алгоритм ГОСТ 28147-89 в режиме гаммирования с обратной связью. Имитозащита данных осуществляется с использованием алгоритма ГОСТ 28147-89 в режиме имитовставки. Ключи парной связи генерируются центром управления сетью для каждого КШ сети и для каждого АП при помощи специальной программы. Передача ключей на КШ с ЦУС производится по защищенному каналу связи (на ключе связи с ЦУС). В качестве ключевого носителя для ключа связи с ЦУС используется дискета. Ключи парной связи хранятся на диске в зашифрованном виде (на ключе хранения). Ключ хранения находится в защищенной энергонезависимой памяти ЭЗ “Соболь”. Для защиты соединения между управляющей консолью и ЦУС используется специальный административный ключ. Этот ключ хранится на ключевом диске администратора системы. Плановая смена ключей на КШ осуществляется из ЦУС по каналу связи в защищенном виде на ключе связи с ЦУС.

Криптографический шлюз представляет собой специализированное программно-аппаратное устройство, функционирующее под управлением сокращенной версии ОС FreeBSD. Он обеспечивает:

- прием и передачу пакетов по протоколам семейства TCP/IP (статическая маршрутизация);
- шифрование передаваемых и принимаемых IP-пакетов (ГОСТ 28147-89, режим гаммирования с обратной связью);
- сжатие защищаемых данных;
- защиту данных от искажения (ГОСТ 28147-89, режим имитовставки);
- фильтрацию IP-пакетов в соответствии с заданными правилами фильтрации;
- скрытие внутренней структуры защищаемого сегмента сети;
- криптографическую аутентификацию удаленных абонентов;
- периодическое оповещение ЦУС о своей активности;
- регистрацию событий, связанных с работой КШ;
- оповещение администратора (в реальном режиме времени) о событиях, требующих оперативного вмешательства;

- идентификацию и аутентификацию администратора при запуске КШ (средствами ЭЗ “Соболь”);
- контроль целостности программного обеспечения КШ до загрузки операционной системы (средствами ЭЗ “Соболь”).

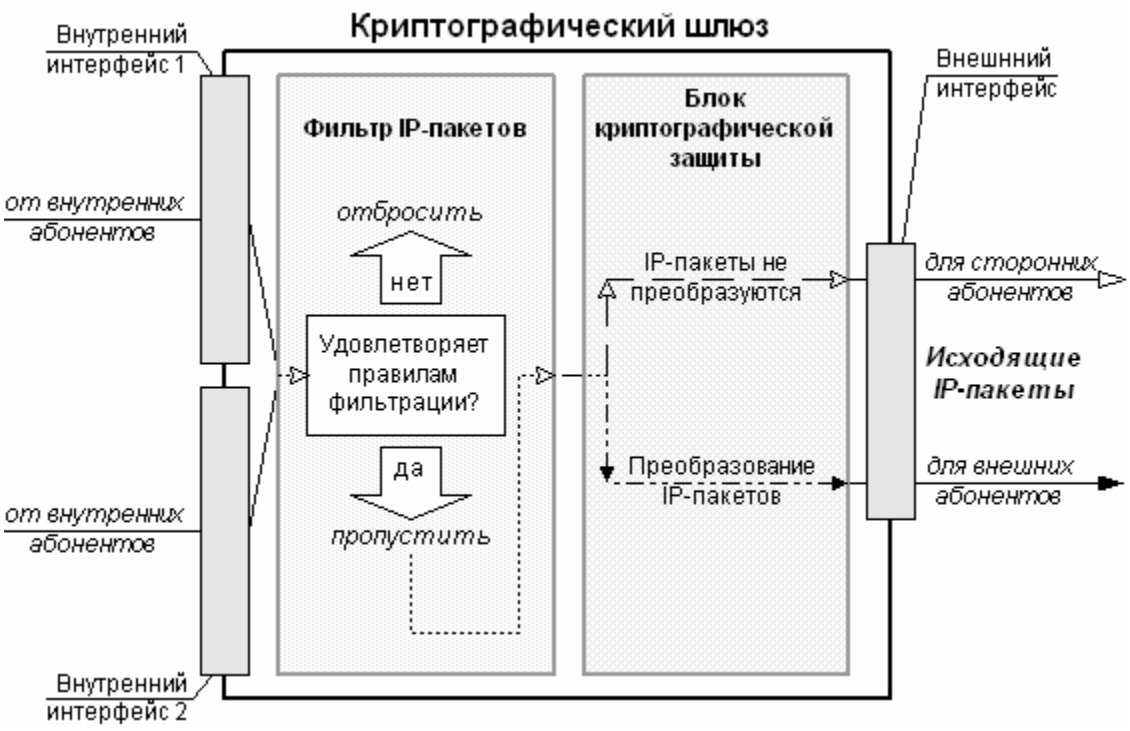


Рис. 7.3. Обработка исходящих IP-пакетов

- Обработка исходящих IP-пакетов представлена на рис. 7.3. Все IP-пакеты, поступившие от внутренних абонентов защищаемого сегмента, вначале подвергаются фильтрации. Фильтрация IP-пакетов осуществляется в соответствии с установленными администратором правилами на основе IP-адресов отправителя и получателя, допустимых значений полей заголовка, используемых портов UDP/TCP и флагов TCP/IP-пакета. Если пакет не удовлетворят правилам фильтрации, он отвергается. Отправитель пакета получает ICMP-сообщение о недоступности абонента. При установке КШ автоматически генерируются правила, необходимые для обеспечения защищенного взаимодействия с ЦУС, корректной работы механизма маршрутизации пакетов, обработки управляющего трафика коммуникационного оборудования и обеспечения возможности начала работы VPN-функций без дополнительного конфигурирования. IP-пакеты, удовлетворяющие правилам фильтрации, обрабатываются блоком криптографической защиты и передаются на внешний интерфейс КШ. КШ-отправитель обеспечивает его сжатие, шифрование и имитозащиту, инкапсуляцию в новый IP-пакет, в котором в качестве IP-адреса приемника выступает IP-адрес КШ-получателя, а в качестве IP-адреса источника выступает IP-адрес КШ-отправителя. IP-пакеты, адресованные абонентам, внешним по отношению к VPN-сети (Web-сайты, ftp-серверы), передаются в открытом виде. Это позволяет использовать КШ при доступе к общедоступным ресурсам сетей общего пользования в качестве межсетевого экрана пакетного уровня. Обработка входящих пакетов представлена на рис. 7.4. Входящие IP-пакеты от открытых абонентов

блоком криптографической защиты не обрабатываются и поступают непосредственно в фильтр IP-пакетов.

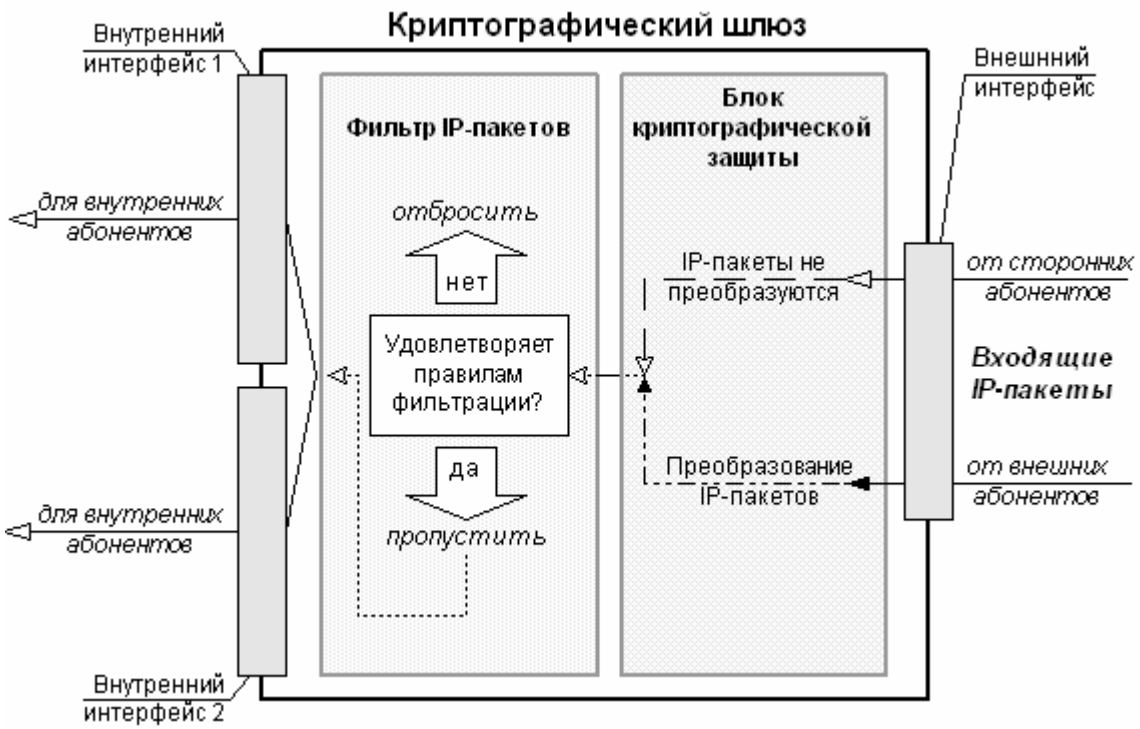


Рис. 7.4. Обработка входящих IP-пакетов

Для пакетов, полученных от абонентов VPN, блок криптографической защиты осуществляет проверку целостности пакетов и расшифровывает их, после чего пакеты поступают в фильтр IP-пакетов. Если целостность пакета нарушена, то пакет отбрасывается без расшифрования и без оповещения отправителя пакета с генерацией сообщения о НСД. IP-пакеты, удовлетворяющие правилам фильтрации, передаются через внутренний интерфейс внутренним абонентам. Криптографический шлюз осуществляет регистрацию следующих событий:

- загрузку и инициализацию системы и ее программный останов;
- вход (выход) администратора КШ в систему (из системы);
- запросы на установление виртуальных соединений между криптошлюзами, между КШ и Центром управления;
- результат фильтрации входящих/исходящих пакетов;
- попытки НСД;
- любые нештатные ситуации, происходящие при работе КШ;
- информацию о потере и восстановлении связи на физическом уровне протоколов.

Перечень регистрируемых событий при эксплуатации КШ определяется администратором. При регистрации события фиксируются:

- дата, время и код регистрируемого события;
- адрес источника и адрес получателя (при фильтрации), включая порты протоколов TCP, IP
- результат попытки осуществления регистрируемого события - успешная или неуспешная (или результат фильтрации);
- идентификатор администратора КШ, предъявленный при попытке осуществления регистрируемого события (для событий локального/удаленного управления).

Оповещение о событиях, требующих вмешательства администратора, осуществляется по протоколу SNMP. Оповещения передаются в открытом виде на ЦУС, откуда могут быть получены консолью управления. Криптографический шлюз обеспечивает сжатие передаваемых данных об однотипных событиях. Локальная сигнализация о событиях, требующих вмешательства

администратора, осуществляется путем вывода соответствующих сообщений на монитор криптошлюза.

Предусматривается два варианта комплектации криптографического шлюза:

- На базе стандартного IBM-совместимого компьютера;
- На базе промышленного компьютера, предназначенного для монтажа в 19” стойку.

Независимо от комплектации в состав криптографического шлюза входят:

- плата Электронного замка “Соболь”;
- считыватель Touch Memory;
- электронные идентификаторы Touch Memory DS1992 (2 шт);
- сетевые платы Ethernet (от 2 до 16 портов).

Центр управления сетью осуществляет управление работой всех КШ, входящих в состав системы защиты. ЦУС осуществляет контроль состояния всех зарегистрированных КШ, проводит рассылку ключевой информации, предоставляет администратору функции удаленного управления КШ, обеспечивает получение и хранение содержимого системных журналов КШ, а также ведение журнала событий НСД. ЦУС обеспечивает:

- аутентификацию КШ и консолей управления;
- контроль текущего состояния всех КШ системы;
- хранение информации о состоянии системы защиты (сети КШ);
- централизованное управление криптографическими ключами и настройками каждого КШ сети;
- взаимодействие с программой управления;
- регистрацию событий по управлению и изменению параметров КШ;
- получение журналов регистрации от всех имеющихся КШ и их хранение.

Программное обеспечение ЦУС устанавливается на одном из КШ защищаемой сети. Программа управления предназначена для централизованного управления всеми КШ, работающими под управлением одного ЦУС. Эта программа позволяет:

- отображать информацию о текущем состоянии всех имеющихся КШ;
- добавлять в систему новые КШ, изменять сведения о существующий КШ или удалять КШ;
- централизованно управлять настройками КШ;
- управлять правилами маршрутизации КШ;
- управлять ключами шифрования;
- анализировать содержание журналов регистрации КШ.

Программа управления предназначена для работы на компьютерах, оснащенных процессорами семейства Intel x86 или совместимыми с ними, и функционирующих под управлением ОС Windows NT 4.0 (Service Pack 4 и выше) или ОС Windows 98. На этих компьютерах должны быть установлены компоненты, обеспечивающие работу с сетевыми протоколами семейства TCP/IP.

4.7.6. Построение комплексных систем защиты информации

4.7.6.1. Концепция создания защищенных КС

При разработке и построении комплексной системы защиты информации в компьютерных системах необходимо придерживаться определенных методологических принципов проведения исследований, проектирования, производства, эксплуатации и развития таких систем. Системы защиты информации относятся к классу сложных систем, и для их построения могут использоваться основные принципы построения сложных систем с учетом специфики решаемых задач:

- параллельная разработка КС и СЗИ;
- системный подход к построению защищенных КС;
- многоуровневая структура СЗИ;
- иерархическая система управления СЗИ;
- блочная архитектура защищенных КС;
- возможность развития СЗИ;
- дружественный интерфейс защищенных КС с пользователями и обслуживающим персоналом.

Первый из приведенных принципов построения СЗИ требует проведения одновременной параллельной разработки КС и механизмов защиты. Только в этом случае можно эффективно

обеспечить реализацию всех остальных принципов. Причем в процессе разработки защищенных КС должен соблюдаться разумный компромисс между созданием встроенных неразделимых механизмов защиты и блочных унифицированных средств и процедур защиты. Только на этапе разработки КС можно полностью учесть взаимное влияние блоков и устройств собственно КС и механизмов защиты, добиться системности защиты оптимальным образом.

Принцип системности является одним из основных концептуальных и методологических принципов построения защищенных КС. Он предполагает:

- анализ всех возможных угроз безопасности информации;
- обеспечение защиты на всех жизненных циклах КС;
- защиту информации во всех звеньях КС;
- комплексное использование механизмов защиты.

Потенциальные угрозы выявляются в процессе создания и исследования модели угроз. В результате исследований должны быть получены данные о возможных угрозах безопасности информации, о степени их опасности и вероятности реализации. При построении СЗИ учитываются потенциальные угрозы, реализация которых может привести к существенному ущербу, и вероятность таких событий не близка к нулю.

Защита ресурсов КС должна осуществляться на этапах разработки, производства, эксплуатации и модернизации, а также по всей технологической цепочке ввода, обработки, передачи, хранения и выдачи информации. Реализация этих принципов позволяет обеспечить создание СЗИ, в которой отсутствуют слабые звенья как на различных жизненных циклах КС, так и в любых элементах и режимах работы КС.

Механизмы защиты, которые используются при построении защищенных систем, должны быть взаимоувязаны по месту, времени и характеру действия. Комплексность предполагает также использование в оптимальном сочетании различных методов и средств защиты информации: технических, программных, криптографических, организационных и правовых. Любая, даже простая СЗИ, является комплексной.

Система защиты информации должна иметь несколько уровней, перекрывающих друг друга, т.е. такие системы целесообразно строить по принципу построения матрешек. Чтобы добраться до закрытой информации, злоумышленнику необходимо «взломать» все уровни защиты.

Например, для отдельного объекта КС можно выделить 6 уровней (рубежей) защиты:

15. охрана по периметру территории объекта;
16. охрана по периметру здания;
17. охрана помещения;
18. защита аппаратных средств;
19. защита программных средств;
20. защита информации.

Комплексные системы защиты информации всегда должны иметь централизованное управление. В распределенных КС управление защитой может осуществляться по иерархическому принципу. Централизация управления защитой информации объясняется необходимостью проведения единой политики в области безопасности информационных ресурсов в рамках предприятия, организации, корпорации, министерства. Для осуществления централизованного управления в СЗИ должны быть предусмотрены специальные средства дистанционного контроля, распределения ключей, разграничения доступа, изготовления атрибутов идентификации и другие.

Одним из важных принципов построения защищенных КС является использование блочной архитектуры. Применение данного принципа позволяет получить целый ряд преимуществ:

- упрощается разработка, отладка, контроль и верификация устройств (программ, алгоритмов);
- допускается параллельность разработки блоков;
- упрощается модернизация систем;
- используются унифицированные стандартные блоки;
- удобство и простота эксплуатации.

Основываясь на принципе блочной архитектуры защищенной КС, можно представить структуру идеальной защищенной системы. В такой системе имеется минимальное ядро защиты, отвечающее нижней границе защищенности систем определенного класса, например ПЭВМ. Если в системе необходимо обеспечить более высокий уровень защиты, то это достигается за счет

согласованного подключения аппаратных блоков или инсталляции дополнительных программных средств (аналогично режиму “Plug and Play” в ОС Windows 98).

В случае необходимости могут быть использованы более совершенные блоки КС, чтобы не допустить снижения эффективности применения системы по прямому назначению. Это объясняется потреблением части ресурсов КС вводимыми блоками защиты.

Стандартные входные и выходные интерфейсы блоков позволяют упростить процесс модернизации СЗИ, альтернативно использовать аппаратные или программные блоки. Здесь просматривается аналогия с семиуровневой моделью ЭМВОС.

При разработке сложной КС, например, вычислительной сети, необходимо предусматривать возможность ее развития в двух направлениях: увеличения числа пользователей и наращивания возможностей сети по мере совершенствования информационных технологий. С этой целью при разработке КС предусматривается определенный запас ресурсов по сравнению с потребностями на момент разработки. Наибольший запас производительности необходимо предусмотреть для наиболее консервативной части сложных систем – каналов связи. Часть резерва ресурсов КС может быть востребована при развитии СЗИ. На практике резерв ресурсов, предусмотренный на этапе разработки, исчерпывается уже на момент полного ввода в эксплуатацию сложных систем. Поэтому при разработке КС предусматривается возможность модернизации системы. В этом смысле сложные системы должны быть развивающимися или открытыми. Термин открытости в этой трактовке относится и к защищенным КС. Причем механизмы защиты, постоянно совершенствуясь, вызывают необходимость наращивания ресурсов КС. Новые возможности, режимы КС, а также появление новых угроз в свою очередь стимулируют развитие новых механизмов защиты. Важное место в процессе создания открытых систем играют международные стандарты в области взаимодействия устройств, подсистем. Они позволяют использовать подсистемы различных типов, имеющих стандартные интерфейсы взаимодействия.

Комплексная система защиты информации должна быть дружественной по отношению к пользователям и обслуживающему персоналу. Она должна быть максимально автоматизирована и не должна требовать от пользователя выполнять значительный объем действий, связанных с СЗИ. Комплексная СЗИ не должна создавать ограничений в выполнении пользователем своих функциональных обязанностей. В СЗИ необходимо предусмотреть меры снятия защиты с отказавших устройств для восстановления их работоспособности.

4.7.6.2. Этапы создания комплексной системы защиты информации

Система защиты информации должна создаваться совместно с создаваемой компьютерной системой. При построении системы защиты могут использоваться существующие средства защиты, или же они разрабатываются специально для конкретной КС. В зависимости от особенностей компьютерной системы, условий ее эксплуатации и требований к защите информации процесс создания КСЗИ может не содержать отдельных этапов, или содержание их может несколько отличаться от общепринятых норм при разработке сложных аппаратно-программных систем. Но обычно разработка таких систем включает следующие этапы:

- разработка технического задания;
- эскизное проектирование;
- техническое проектирование;
- рабочее проектирование;
- производство опытного образца.

Одним из основных этапов разработки КСЗИ является этап разработки технического задания. Именно на этом этапе решаются практически все специфические задачи, характерные именно для разработки КСЗИ.

Процесс разработки систем, заканчивающийся выработкой технического задания, называют научно-исследовательской разработкой, а остальную часть работы по созданию сложной системы называют опытно-конструкторской разработкой. Опытно-конструкторская разработка аппаратно-программных средств ведется с применением систем автоматизации проектирования, алгоритмы проектирования хорошо изучены и отработаны. Поэтому особый интерес представляет рассмотрение процесса научно-исследовательского проектирования.

4.7.6.3. Научно-исследовательская разработка КСЗИ

Целью этого этапа является разработка технического задания на проектирование КСЗИ. Техническое задание содержит основные технические требования к разрабатываемой КСЗИ, а также согласованные взаимные обязательства заказчика и исполнителя разработки. Технические

требования определяют значения основных технических характеристик, выполняемые функции, режимы работы, взаимодействие с внешними системами и т.д.

Аппаратные средства оцениваются следующими характеристиками: быстродействие, производительность, емкость запоминающих устройств, разрядность, стоимость, характеристики надежности и др. Программные средства характеризуются требуемым объемом оперативной и внешней памяти, системой программирования, в которой разработаны эти средства, совместимостью с ОС и другими программными средствами, временем выполнения, стоимостью и т.д.

Получение значений этих характеристик, а также состава выполняемых функций и режимов работы средств защиты, порядка их использования и взаимодействия с внешними системами составляют основное содержание этапа научно-исследовательской разработки. Для проведения исследований на этом этапе заказчик может привлекать исполнителя или научно-исследовательское учреждение, либо организует совместную их работу.

Научно-исследовательская разработка начинается с анализа угроз безопасности информации, анализа защищаемой КС и анализа конфиденциальности и важности информации в КС. Прежде всего, производится анализ конфиденциальности и важности информации, которая должна обрабатываться, храниться и передаваться в КС. На основе анализа делается вывод о целесообразности создания КСЗИ. Если информация не является конфиденциальной и легко может быть восстановлена, то создавать КСЗИ нет необходимости. Не имеет смысла также создавать КСЗИ в КС, если потеря целостности и конфиденциальности информации связана с незначительными потерями. В этих случаях достаточно использовать штатные средства КС и, возможно, страхование от утраты информации.

При анализе информации определяются потоки конфиденциальной информации, элементы КС, в которых она обрабатывается и хранится. На этом этапе рассматриваются также вопросы разграничения доступа к информации отдельных пользователей и целых сегментов КС. На основе анализа информации определяются требования к ее защищенности. Требования задаются путем присвоения определенного грифа конфиденциальности, установления правил разграничения доступа.

Очень важная исходная информация для построения КСЗИ получается в результате анализа защищаемой КС. Т.к. КСЗИ является подсистемой КС, то взаимодействие системы защиты с КС можно определить как внутреннее, а взаимодействие с внешней средой – как внешнее.

Внутренние условия взаимодействия определяются архитектурой КС. При построении КСЗИ учитываются:

- географическое положение КС;
- тип КС (распределенная или сосредоточенная);
- структуры КС (техническая, программная, информационная и т.д.);
- производительность и надежность элементов КС;
- типы используемых аппаратных и программных средств и режимы их работы;
- угрозы безопасности информации, которые порождаются внутри КС (отказы аппаратных и программных средств, алгоритмические ошибки и т.п.);

Учитываются следующие внешние условия:

- взаимодействие с внешними системами;
- случайные и преднамеренные угрозы.

Анализ угроз безопасности является одним из обязательных условий построения КСЗИ. По результатам проведенного анализа строится модель угроз безопасности информации в КС, которая содержит систематизированные данные о случайных и преднамеренных угрозах безопасности информации в конкретной КС. Систематизация данных модели предполагает наличие сведений обо всех возможных угрозах, их опасности, временных рамках действия, вероятности реализации. Часто модель угроз рассматривается как композиция модели злоумышленника и модели случайных угроз. Модели представляются в виде таблиц, графов или на вербальном уровне. При построении модели злоумышленника используется два подхода:

1. модель ориентируется только на высококвалифицированного злоумышленника-профессионала, оснащенного всем необходимым и имеющего легальный доступ на всех рубежах защиты;
2. модель учитывает квалификацию злоумышленника, его оснащенность (возможности) и официальный статус в КС.

Первый подход проще реализуется и позволяет определить верхнюю границу преднамеренных угроз безопасности информации. Второй подход отличается гибкостью и позволяет учитывать особенности КС в полной мере. Градация злоумышленников по их квалификации может быть различной. Например, может быть выделено три класса злоумышленников:

1. высококвалифицированный злоумышленник-профессионал;
2. квалифицированный злоумышленник-непрофессионал;
3. неквалифицированный злоумышленник-непрофессионал.

Класс злоумышленника, его оснащенность и статус на объекте КС определяют возможности злоумышленника по несанкционированному доступу к ресурсам КС. Угрозы, связанные с непреднамеренными действиями, хорошо изучены, и большая часть их может быть формализована. Сюда следует отнести угрозы безопасности, которые связаны с конечной надежностью технических систем. Угрозы, порождаемые стихией или человеком, формализовать сложнее. Но с другой стороны, по ним накоплен большой объем статистических данных. На основании этих данных можно прогнозировать проявление угроз этого класса.

Модель злоумышленника и модель случайных угроз позволяют получить полный спектр угроз и их характеристик. В совокупности с исходными данными, полученными в результате анализа информации, особенностей архитектуры проектируемой КС, модели угроз безопасности информации позволяют получить исходные данные для построения модели КСЗИ.

4.7.6.4. Моделирование КСЗИ

Оценка эффективности функционирования КСЗИ представляет собой сложную научно-техническую задачу. Комплексная СЗИ оценивается в процессе разработки КС, в период эксплуатации и при создании (модернизации) СЗИ для уже существующих КС. При разработке сложных систем распространенным методом проектирования является синтез с последующим анализом. Система синтезируется путем согласованного объединения блоков, устройств, подсистем и анализируется (оценивается) эффективность полученного решения. Из множества синтезированных систем выбирается лучшая по результатам анализа, который осуществляется с помощью моделирования.

Моделирование КСЗИ заключается в построении образа (модели) системы, с определенной точностью воспроизводящего процессы, происходящие в реальной системе. Реализация модели позволяет получать и исследовать характеристики реальной системы.

Для оценки систем используются аналитические и имитационные модели. В аналитических моделях функционирование исследуемой системы записывается в виде математических или логических соотношений. Для этих целей используется мощный математический аппарат: алгебра, функциональный анализ, разностные уравнения, теория вероятностей, математическая статистика, теория множеств, теория массового обслуживания, теория связи и т.д.

При имитационном моделировании моделируемая система представляется в виде некоторого аналога реальной системы. В процессе имитационного моделирования на ЭВМ реализуются алгоритмы изменения основных характеристик реальной системы в соответствии с эквивалентными реальным процессам математическими и логическими зависимостями.

Модели делятся также на детерминированные и стохастические. Модели, которые оперируют со случайными величинами, называются стохастическими. Т.к. на процессы защиты информации основное влияние оказывают случайные факторы, то модели систем защиты являются стохастическими.

Моделирование КСЗИ является сложной задачей, потому что такие системы относятся к классу сложных организационно-технических систем, которым присущи следующие особенности:

- сложность формального представления процессов функционирования таких систем, главным образом, из-за сложности формализации действий человека;
- многообразие архитектур сложной системы, которое обуславливается многообразием структур ее подсистем и множественностью путей объединения подсистем в единую систему;
- большое число взаимосвязанных между собой элементов и подсистем;
- сложность функций, выполняемых системой;
- функционирование систем в условиях неполной определенности и случайности процессов, оказывающих воздействие на систему;
- наличие множества критериев оценки эффективности функционирования сложной системы;

- существование интегрированных признаков, присущих системе в целом, но не свойственных каждому элементу в отдельности (например, система с резервированием является надежной, при ненадежных элементах);
- наличие управления, часто имеющего сложную иерархическую структуру;
- разветвленность и высокая интенсивность информационных потоков.

Для преодоления этих сложностей применяются:

1. специальные методы неформального моделирования;
2. декомпозиция общей задачи на ряд частных задач;
3. макромоделирование.

Специальные методы неформального моделирования

Специальные методы неформального моделирования основаны на применении неформальной теории систем. Основными составными частями неформальной теории систем являются:

- структурирование архитектуры и процессов функционирования сложных систем;
- неформальные методы оценивания;
- неформальные методы поиска оптимальных решений.

Структурирование является развитием формального описания систем, распространенного на организационно-технические системы. Примером структурированного процесса является конвейерное производство. В основе такого производства лежат два принципа:

- строгая регламентация технологического процесса производства;
- специализация исполнителей и оборудования.

Предполагается, что конструкция производимой продукции отвечает следующим требованиям:

- изделие состоит из конструктивных иерархических элементов (блоков, узлов, схем, деталей и т.п.);
- максимальная простота, унифицированность и стандартность конструктивных решений и технологических операций.

В настоящее время процесс производства технических средств КС достаточно полно структурирован. Структурное программирование также вписывается в рамки структурированных процессов. На основе обобщения принципов и методов структурного программирования могут быть сформулированы условия структурированного описания изучаемых систем и процессов их функционирования:

1. полнота отображения основных элементов и их взаимосвязей;
2. адекватность;
3. простота внутренней организации элементов описания и взаимосвязей элементов между собой;
4. стандартность и унифицированность внутренней структуры элементов и структуры взаимосвязей между ними;
5. модульность;
6. гибкость, под которой понимается возможность расширения и изменения структуры одних компонентов модели без существенных изменений других компонентов;
7. доступность изучения и использования модели любому специалисту средней квалификации соответствующего профиля.

В процессе проектирования систем необходимо получить их характеристики. Некоторые характеристики могут быть получены путем измерения. Другие получаются с использованием аналитических соотношений, а также в процессе обработки статистических данных. Однако существуют характеристики сложных систем, которые не могут быть получены приведенными методами. К таким характеристикам СЗИ относятся вероятности реализации некоторых угроз, отдельные характеристики эффективности системы защиты и другие.

Указанные характеристики могут быть получены единственно доступными методами – методами неформального оценивания. Сущность методов заключается в привлечении для получения некоторых характеристик специалистов-экспертов в соответствующих областях знания. Наибольшее распространение из неформальных методов оценивания получил метод экспертных оценок, который представляет собой алгоритм подбора специалистов-экспертов, задания правил получения независимых оценок каждым экспертом и последующей статистической обработки полученных результатов. Методы экспертных оценок используются давно, хорошо отработаны. В

некоторых случаях они являются единственно возможными методами оценивания характеристик систем.

Неформальные методы поиска оптимальных решений могут быть распределены по двум группам:

- методы неформального сведения сложной задачи к формальному описанию и решение задачи формальными методами;
- неформальный поиск оптимального решения.
- Для моделирования систем защиты информации целесообразно использовать следующие теории и методы, позволяющие свести решение задачи к формальным алгоритмам:
- теория нечетких множеств;
- теория конфликтов;
- теория графов;
- формально-эвристические методы;
- эволюционное моделирование.

Методы теории нечетких множеств позволяют получать аналитические выражения для количественных оценок нечетких условий принадлежности элементов к тому или иному множеству. Теория нечетких множеств хорошо согласуется с условиями моделирования систем защиты, т.к. многие исходные данные моделирования (например, характеристики угроз и отдельных механизмов защиты) не являются строго определенными.

Теория конфликтов является относительно новым направлением исследования сложных человеко-машинных систем. Конфликт между злоумышленником и системой защиты, разворачивающийся на фоне случайных угроз, является классическим для применения теории конфликтов. Две противоборствующие стороны преследуют строго противоположные цели. Конфликт развивается в условиях неоднозначности и слабой предсказуемости процессов, способности сторон оперативно изменять цели. Теория конфликтов является развитием теории игр. Теория игр позволяет:

- структурировать задачу, представить ее в обозримом виде, найти области количественных оценок, упорядочений, предпочтений, выявить доминирующие стратегии, если они существуют;
- до конца решить задачи, которые описываются стохастическими моделями.

Теория игр позволяет найти решение, оптимальное или рациональное в среднем. Она исходит из принципа минимизации среднего риска. Такой подход не вполне адекватно отражает поведение сторон в реальных конфликтах, каждый из которых является уникальным. В теории конфликтов предпринята попытка преодоления этих недостатков теории игр. Теория конфликтов позволяет решать ряд практических задач исследования сложных систем. Однако она еще не получила широкого распространения и открыта для дальнейшего развития.

Из теории графов для исследования систем защиты информации в наибольшей степени применим аппарат сетей Петри. Управление условиями в узлах сети Петри позволяет моделировать процессы преодоления защиты злоумышленником. Аппарат сетей Петри позволяет формализовать процесс исследования эффективности СЗИ.

К формально-эвристическим методам отнесены методы поиска оптимальных решений не на основе строгих математических, логических соотношений, а основываясь на опыте человека, имеющихся знаниях и интуиции. Получаемые решения могут быть далекими от оптимальных, но они всегда будут лучше решений, получаемых без эвристических методов.

Наибольшее распространение из эвристических методов получили лабиринтные и концептуальные методы. В соответствии с лабиринтной моделью задача представляется человеку в виде лабиринта возможных путей решения. Предполагается, что человек обладает способностью быстрого отсечения бесперспективных путей движения по лабиринту. В результате среди оставшихся путей с большой вероятностью находится путь, ведущий к решению поставленной задачи.

Концептуальный метод предполагает выполнение действий с концептами. Под концептами понимаются обобщенные элементы и связи между ними. Концепты получаются человеком, возможно и неосознанно, в процессе построения структурированной модели. В соответствии с концептуальным методом набор концепт универсален и ему соответствуют имеющиеся у человека механизмы вычисления, трансформации и формирования отношений. Человек проводит

мысленный эксперимент со структурированной моделью и порождает ограниченный участок лабиринта, в котором уже несложно найти решение.

Эволюционное моделирование представляет собой разновидность имитационного моделирования. Особенность его заключается в том, что в процессе моделирования совершенствуется алгоритм моделирования.

Сущность неформальных методов непосредственного поиска оптимальных решений состоит в том, что человек участвует не только в построении модели, но и в процессе ее реализации.

Декомпозиция общей задачи оценки эффективности функционирования КСЗИ

Сложность выполняемых функций, значительная доля нечетко определенных данных, большое количество механизмов защиты, сложность их взаимных связей и многие другие факторы делают практически неразрешимой проблему оценки эффективности системы в целом с помощью одного какого-либо метода моделирования. Для решения этой проблемы применяется метод декомпозиции (разделения) общей задачи оценки эффективности на ряд частных задач. Так, задача оценки эффективности КСЗИ может разбиваться на частные задачи:

- оценку эффективности защиты от сбоев и отказов аппаратных и программных средств;
- оценку эффективности защиты от НСДИ;
- оценку эффективности защиты от ПЭМИН и т.д.

При оценке эффективности защиты от отказов, приводящих к уничтожению информации, используется, например, такая величина, как вероятность безотказной работы P(t) системы за время t. Этот показатель вычисляется по формуле

$P(t)=1-P_{OT}(t)$,

где $P_{OT}(t)$ – вероятность отказа системы за время t.

Величина $P_{OT}(t)$, в свою очередь, определяется в соответствии с известным выражением:

$P_{OT}(t) = \exp(-\lambda t)$,

где λ – интенсивность отказов системы.

Таким образом, частная задача оценки влияния отказов на безопасность информации может быть довольно просто решена известными формальными методами. Довольно просто решается частная задача оценки эффективности метода шифрования при условии, что атака на шифр возможна только путем перебора ключей, и известен метод шифрования. Среднее время взлома шифра при этих условиях определяется по формуле:

$T=A^S t/2$,

где T – среднее время взлома шифра; A – число символов, которые могут быть использованы при выборе ключа (мощность алгоритма шифрования); S – длина ключа, выраженная в количестве символов; t – время проверки одного ключа.

Время t зависит от производительности, используемой для атаки на шифр КС и сложности алгоритма шифрования. При расчете криптостойкости обычно считается, что злоумышленник имеет в своем распоряжении КС наивысшей производительности, уже существующей или перспективной.

Частные задачи, в свою очередь могут быть декомпозированы на подзадачи. Главная сложность метода декомпозиции при оценке систем заключается в учете взаимосвязи и взаимного влияния частных задач оценивания и оптимизации. Это влияние учитывается как при решении задачи декомпозиции, так и в процессе получения интегральных оценок. Например, при решении задачи защиты информации от электромагнитных излучений используется экранирование металлическими экранами, а для повышения надежности функционирования системы необходимо резервирование блоков, в том числе и блоков, обеспечивающих бесперебойное питание. Решение этих двух частных задач взаимосвязано, например, при создании КСЗИ на летательных аппаратах, где существуют строгие ограничения на вес. При декомпозиции задачи оптимизации комплексной системы защиты приходится всякий раз учитывать общий лимит веса оборудования.

Макромоделирование

При оценке сложных систем используется также макромоделирование. Такое моделирование осуществляется с целью общей оценки системы. Задача при этом упрощается за счет использования при построении модели только основных характеристик. К макромоделированию прибегают в основном для получения предварительных оценок системы.

Если в КСЗИ используется k уровней защиты, то в зависимости от выбранной модели злоумышленника ему необходимо преодолеть k-m уровней защиты, где m – номер наивысшего уровня защиты, который злоумышленник беспрепятственно преодолевает в соответствии со своим

официальным статусом. Если злоумышленник не имеет никакого официального статуса на объекте КС, то ему, в общем случае, необходимо преодолеть все k уровней защиты, чтобы получить доступ к информации. Для такого злоумышленника вероятность получения несанкционированного доступа к информации $P_{НСД}$ может быть рассчитана по формуле:

$$P_{НСД} = \prod_{i}^{k} P_i ,$$

где P_i – вероятность преодоления злоумышленником i-го уровня защиты.

На макроуровне можно, например, исследовать требуемое число уровней защиты, их эффективность по отношению к предполагаемой модели нарушителя с учетом особенностей КС и финансовых возможностей проектирования и построения КСЗИ.

4.7.6.5. Выбор показателей эффективности и критериев оптимальности КСЗИ

Эффективность систем оценивается с помощью показателей эффективности. Иногда используется термин – показатель качества. Показателями качества, как правило, характеризуют степень совершенства какого-либо товара, устройства, машины. В отношении сложных человеко-машинных систем предпочтительнее использование термина показатель эффективности функционирования, который характеризует степень соответствия оцениваемой системы своему назначению.

Показатели эффективности системы, как правило, представляют собой некоторое множество функций y_k от характеристик x_i:

$y_k = f(x_1, x_2, \ldots, x_n)$, $k = 1, 2, \ldots, K$; $n=1, 2, \ldots, N$,

где K – мощность множества показателей эффективности системы, N – мощность множества характеристик системы.

Характеристиками системы $x_1, x_2, \ldots, x_n$ называются первичные данные, отражающие свойства и особенности системы. Используются количественные и качественные характеристики. Количественные характеристики систем имеют числовое выражение. Их называют также параметрами. К количественным характеристикам относят разрядность устройства, быстродействие процессора, длину пароля, длину ключа шифрования и т.п. Качественные характеристики определяют наличие (отсутствие) определенных режимов, защитных механизмов или сравнительную степень свойств систем ("хорошо", "удовлетворительно", "лучше", "хуже").

Примером показателя эффективности является криптостойкость шифра, которая выражается временем или стоимостью взлома шифра. Этот показатель для шифра DES, например, зависит от одной характеристики – разрядности ключа. Для методов замены криптостойкость зависит от количества используемых алфавитов замены, а для методов перестановок – от размерности таблицы и количества используемых маршрутов Гамильтона.

Для того чтобы оценить эффективность системы защиты информации или сравнить системы по их эффективности, необходимо задать некоторое правило предпочтения. Такое правило или соотношение, основанное на использовании показателей эффективности, называют критерием эффективности. Для получения критерия эффективности при использовании некоторого множества k показателей используют ряд подходов.

1. Выбирается один главный показатель, и оптимальной считается система, для которой этот показатель достигает экстремума (при условии, что остальные показатели удовлетворяют системе ограничений, заданных в виде неравенств). Например, оптимальной может считаться система, удовлетворяющая следующему критерию эффективности:

$$P_{HZ} = P_{HZ}^{\max} \text{ при } C \le C_{доп},\ G \le G_{доп},$$

где P_{HZ} – вероятность непреодоления злоумышленником системы защиты за определенное время, C и G – стоимостные и весовые показатели, соответственно, которые не должны превышать допустимых значений.

2. Методы, основанные на ранжировании показателей по важности. При сравнении систем одноименные показатели эффективности сопоставляются в порядке убывания их важности по определенным алгоритмам. Примерами таких методов могут служить лексикографический метод и метод последовательных уступок.

Лексикографический метод применим, если степень различия показателей по важности велика. Две системы сравниваются сначала по наиболее важному показателю. Оптимальной считается такая система, у которой лучше этот показатель. При равенстве самых важных показателей сравниваются показатели, занимающие по рангу вторую позицию. При равенстве и этих показателей сравнение продолжается до получения предпочтения в i-м показателе.

Метод последовательных уступок предполагает оптимизацию системы по наиболее важному показателю Y_1. Определяется допустимая величина изменения показателя Y_1, которая называется уступкой. Измененная величина показателя $Y_1'=Y_1\pm\Delta_1$ (Δ_1 – величина уступки) фиксируется. Определяется оптимальная величина показателя Y_2 при фиксированном значении Y_1', выбирается уступка Δ_2, и процесс повторяется до получения Y_{K-1}.

3. Мультипликативные и аддитивные методы получения критериев эффективности основываются на объединении всех или части показателей с помощью операций умножения или сложения в обобщенные показатели ($Z_П$, Z_C). Показатели, используемые в обобщенных показателях, называют частными (y_i, y_j).Если в произведение (сумму) включается часть показателей, то остальные частные показатели включаются в ограничения. Показатели, образующие произведение (сумму), могут иметь весовые коэффициенты k_i (k_j). В общем виде эти методы можно представить следующим образом:

$$Z_П = \text{extr} \prod_i k_i y_i; \qquad Z_C = \text{extr} \sum_j k_j y_j.$$

4. Оценка эффективности СЗИ может осуществляться также методом Парето, сущность которого заключается в следующем. При использовании n показателей эффективности системе соответствует точка в n-мерном пространстве, в котором строится область Парето-оптимальных решений. В этой области располагаются несравнимые решения, для которых улучшение какого-либо показателя невозможно без ухудшения других показателей эффективности. Выбор наилучшего решения из числа Парето-оптимальных может осуществляться по различным правилам.

4.7.6.6. Математическая постановка задачи разработки комплексной системы защиты информации

После выбора показателей эффективности и критерия эффективности может быть осуществлена математическая постановка задачи разработки КСЗИ. На этом этапе уже известны:

- $F=\{f_1, f_2, \ldots, f_n\}$ – функции, которые должна выполнять КСЗИ;
- $M=\{m_1, m_2, \ldots, m_k\}$ – возможные механизмы защиты;
- $U=\{u_1, u_2, \ldots, u_p\}$ – способы управления КСЗИ;
- $Y=\{y_1, y_2, \ldots, y_w\}$ – показатели эффективности КСЗИ.

Показатели эффективности зависят от выполняемых функций, механизмов защиты и способов управления КСЗИ: У=Ф(F, M, U).

Критерий эффективности получается с использованием показателей эффективности: К=Е(У).

Тогда математическая постановка задачи разработки КСЗИ в общем случае может быть представлена в следующем виде: найти extrS(F, M*, U*), при $M^* \in M$, $U^* \in U$, которым соответствуют $У^* \in Y_Д$, где $Y_Д$ – множество допустимых значений показателей эффективности КСЗИ. Другими словами, требуется создать или выбрать такие механизмы защиты информации и способы управления системой защиты, при которых обеспечивается выполнение всего множества требуемых функций и достигается максимум или минимум выбранного критерия, а также выполняются ограничения на некоторые показатели эффективности.

Такая постановка задачи применима не только для решения общей, но и частных задач оценки эффективности комплексной системы защиты информации.

4.7.6.7. Подходы к оценке эффективности КСЗИ

Эффективность КСЗИ оценивается как на этапе разработки, так и в процессе эксплуатации. В оценке эффективности КСЗИ, в зависимости от используемых показателей и способов их получения, можно выделить три подхода:

- классический;
- официальный;
- экспериментальный.

Классический подход

Под классическим подходом к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения

показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной КС. Такой подход используется при разработке и модернизации КСЗИ. Однако возможности классических методов комплексного оценивания эффективности применительно к КСЗИ ограничены в силу ряда причин. Высокая степень неопределенности исходных данных, сложность формализации процессов функционирования, отсутствие общепризнанных методик расчета показателей эффективности и выбора критериев оптимальности создают значительные трудности для применения классических методов оценки эффективности.

Официальный подход

Большую практическую значимость имеет подход к определению эффективности КСЗИ, который условно можно назвать официальным. Политика безопасности информационных технологий проводится государством и должна опираться на нормативные акты. В этих документах необходимо определить требования к защищенности информации различных категорий конфиденциальности и важности.

Требования могут задаваться перечнем механизмов защиты информации, которые необходимо иметь в КС, чтобы она соответствовала определенному классу защиты. Используя такие документы, можно оценить эффективность КСЗИ. В этом случае критерием эффективности КСЗИ является ее класс защищенности. Несомненным достоинством таких классификаторов (стандартов) является простота использования. Основным недостатком официального подхода к определению эффективности систем защиты является то, что не определяется эффективность конкретного механизма защиты, а констатируется лишь факт его наличия или отсутствия. Этот недостаток в какой-то мере компенсируется заданием в некоторых документах достаточно подробных требований к этим механизмам защиты.

Во всех развитых странах разработаны свои стандарты защищенности компьютерных систем критического применения. Так, в министерстве обороны США используется стандарт TCSEC (Department of Defence Trusted Computer System Evaluation Criteria), который известен как Оранжевая книга. Согласно этой книге для оценки информационных систем рассматривается четыре группы безопасности: A, B, C, D. В некоторых случаях группы безопасности делятся дополнительно на классы безопасности.

Группа A (гарантированная или проверяемая защита) обеспечивает гарантированный уровень безопасности. Методы защиты, реализованные в системе, могут быть проверены формальными методами. В этой группе только один класс – A1.

Группа B (полномочная или полная защита) представляет полную защиту КС. В этой группе выделены классы безопасности B1, B2, B3.

Класс B1 (защита через грифы или метки) обеспечивается использованием в КС грифов секретности, определяющих доступ пользователей к частям системы.

Класс B2 (структурированная защита) достигается разделением информации на защищенные и незащищенные блоки и контролем доступа к ним пользователей.

Класс B3 (области или домены безопасности) предусматривает разделение КС на подсистемы с различным уровнем безопасности и контролем доступа к ним пользователей.

Группа C (избирательная защита) представляет избирательную защиту подсистем с контролем доступа к ним пользователей. В этой группе выделены классы безопасности C1 и C2.

Класс C1 (избирательная защита информации) предусматривает разделение в КС пользователей и данных. Этот класс обеспечивает самый низкий уровень защиты КС.

Класс C2 (защита через управляемый или контролируемый доступ) обеспечивается раздельным доступом пользователей к данным.

Группу D (минимальной безопасности) составляют КС, проверенные на безопасность, но которые не могут быть отнесены к классам A, B или C.

Организация защиты информации в вычислительных сетях министерства обороны США осуществляется в соответствии с требованиями руководства "The Trusted Network Interpretation of Department of Defense Trusted Computer System Evaluation Guidelines". Этот документ получил название Красная книга.

Подобные стандарты защищенности КС приняты и в других развитых странах. Так, в 1991 году Франция, Германия, Нидерланды и Великобритания приняли согласованные "Европейские критерии", в которых рассмотрено 7 классов безопасности от E0 до E6.

В России аналогичный стандарт разработан в 1992 году Государственной технической комиссией (ГТК) при Президенте РФ. Этим стандартом является руководящий документ ГТК "Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к

информации". Устанавливается семь классов защищенности средств вычислительной техники (СВТ) от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Кроме требований к защищенности отдельных элементов СВТ, в Руководящем документе приведены требования к защищенности автоматизированных систем (АС). В отличие от СВТ автоматизированные системы являются функционально ориентированными. При создании АС учитываются особенности пользовательской информации, технология обработки, хранения и передачи информации, конкретные модели угроз. Устанавливается девять классов защищенности АС от НСД к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Третья группа классифицирует АС, с которыми работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А. Во вторую группу сведены АС, пользователи которых имеют одинаковые права доступа ко всей информации АС. Группа содержит два класса – 2Б и 2А. Первую группу составляют многопользовательские АС, в которых пользователи имеют разные права доступа к информации. Группа включает пять классов – 1Д, 1Г, 1В, 1Б, 1А. К каждому из девяти классов защищенности АС предъявляются свои требования.

Глоссарий

Администратор безопасности - лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.

Акустический сигнал – возмущения упругой среды различной формы и длительности (акустические колебания), распространяющиеся от источника в окружающее пространство.

Аппаратные средства - приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации.

Аудит - совокупность мер, связанных с регистрацией, анализом и документированием событий, связанных с работой системы защиты.

Аутентификация - проверка подлинности регистрационной информации о пользователе.

Безопасность - состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз.

Видовая информация - информация о внешнем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений.

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, непосредственно не участвующие в обработке информации ограниченного доступа, но находящиеся в зоне электромагнитных полей, создаваемых ТСПИ.

Журнал - файл с информацией о событиях, зарегистрированных в системе защиты, например, попытках использования ресурсов.

Замкнутая среда - режим работы системы защиты, при котором для каждого пользователя определяется перечень доступных для запуска программ. Совокупность этих ресурсов и образует замкнутую среду работы пользователя. Замкнутая среда может контролироваться в "жестком" или "мягком" режиме.

Инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба производственной деятельности.

Интерсепторы - широкополосные радиоприемные устройства, автоматически настраивающиеся на частоту наиболее мощного радиосигнала и осуществляющие его детектирование.

Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств.

Информационные ресурсы - отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

Информация - это субстанция, объединяющая в себе элементы идеального и материального, имеющая измеряемые определенными единицами физические параметры, стоимость и цену, обладающая специфическими свойствами дуализма и легкости копирования, которой можно владеть, ее использовать и ею распоряжаться.

Источники конфиденциальной информации - люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.

Источники угроз - конкуренты, преступники, коррупционеры, административно-управленческие органы.

Канал утечки информации - физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям.

"Компьютерные вирусы" - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Контролируемая зона (КЗ), - зона, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.

Контрольная сумма - числовое значение, вычисляемое по специальному алгоритму и используемое для контроля целостности информации.

Криптоанализ - это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.

Криптографические средства - специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Криптографический ключ - параметр, с помощью которого выбирается отдельное используемое криптографическое преобразование.

Криптографический шлюз (КШ) обеспечивает криптографическую защиту информации при ее передаче по открытым каналам сетей общего пользования и защиту внутренних сегментов сети от проникновения извне.

Криптография - совокупность методов преобразования данных, ориентированных на то, чтобы сделать эти данные бесполезными для злоумышленника.

"Логические бомбы" - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условиях.

Межсетевой экран (МЭ) – это система межсетевой защиты, позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую.

Механизм контроля целостности - механизм контроля целостности представляет собой защитные средства для своевременного обнаружения изменений ресурсов системы. Использование этого механизма обеспечивает правильное функционирование системы защиты и целостность обрабатываемой информации.

Механизм регистрации событий - механизм, обеспечивающий с помощью специальных средств контроля получение, регистрацию в журнале и последующий анализ информации о работе системы защиты. Анализ собранной информации позволяет выявить причины и наметить способы исправления ситуации.

Направления обеспечения информационной безопасности - это нормативно-правовые категории, ориентированные на обеспечение комплексной защиты информации от внутренних и внешних угроз.

Нелинейный локатор – устройство, предназначенное для обнаружения дистанционно-управляемых и (или) включающихся по голосовому сигналу закладных устройств, а также обнаружения скрытно установленных записывающих устройств.

НСД - несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Объект - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

Объект угроз информационной безопасности - сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Одностороннее хэширование - особая разновидность алгоритма вычисления контрольной суммы.

Оптико-электронный (лазерный) канал утечки речевой информации – канал, образующийся при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (оконных стекол, зеркал, картинных стекол).

Организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого либо ущерба исполнителям.

Организационное мероприятие – это мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств.

Основные направления защиты информации - правовая, организационная и инженерно-техническая защиты информации.

Охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения.

Пакет контроля целостности - список, содержащий информацию о местоположении контролируемых объектов (например, файлов на диске) и эталонные значения контролируемых параметров объектов.

Параметрические технические каналы утечки речевой информации – каналы, образуемые за счет высокочастотного облучения элементов ТСПИ и ВТСС или пассивных закладных устройств.

Персональный идентификатор пользователя - средство аппаратной поддержки системы защиты, предназначенное для идентификации пользователя. Носителями персональной ключевой информации в системе Secret Net являются электронные идентификаторы (например, Touch Memory или eToken).

Побочные электромагнитные излучения (ПЭМИ) - магнитные и электрические поля, порождаемые электрическим током при его прохождении по токоведущим элементам ТСПИ между различными точками его схемы.

Подсистема замкнутой программной среды – подсистема, позволяющая сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска.

Подсистема избирательного управления доступом – подсистема, обеспечивающая разграничение доступа пользователей к ресурсам файловой системы, аппаратным ресурсам и ресурсам операционной системы компьютера.

Подсистема полномочного управления доступом – подсистема, обеспечивающая разграничение доступа пользователей к конфиденциальной информации, хранящейся в файлах на локальных и сетевых дисках.

Подсистема контроля входа – подсистема, обеспечивающая идентификацию и аутентификацию пользователя при его входе в систему.

Подсистема контроля целостности осуществляет слежение за неизменностью контролируемых объектов (файлов, ключей системного реестра и т.д.) с целью защиты их от модификации.

Политика информационной безопасности - документально зафиксированная совокупность принципов, правил и рекомендаций, определяющих порядок организации защиты информации.

Полномочный доступ - разграничение доступа к информационным ресурсам в соответствии со степенью конфиденциальности содержащихся в них сведений и уровнем допуска пользователей к конфиденциальной информации.

Права - правила, ассоциированные с объектом, определяющие какие пользователи и каким способом могут осуществлять доступ к этому объекту.

Правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Привилегия - предоставляемая пользователю возможность выполнить определенное действие в системе. Привилегия имеет приоритет перед правами.

Программные средства - специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных.

Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

Ресурс - любой компонент компьютера или сети, например, диск, принтер или память, который может быть выделен выполняющейся программе или процессу или совместно использоваться в локальной сети.

Система безопасности - организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Система защиты - комплекс специальных мер правового и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности информационной системы.

Сложный сигнал - сигнал, содержащий спектр гармонических составляющих.

Случайные угрозы - угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени.

Способы защиты информации - всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие несанкционированному доступу.

Средства защиты информации - физические средства, аппаратные средства, программные средства и криптографические методы.

Технические (аппаратно-программные) средства защиты - различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографические функции и т.д.).

Технические средства приема, обработки, хранения и передачи информации (ТСПИ) - технические средства, непосредственно обрабатывающие информацию ограниченного доступа.

Технический канал утечки информации (ТКУИ) есть способ получения разведывательной информации об объекте с помощью технического средства разведки.

Техническое мероприятие – это мероприятие, предусматривающее применение специальных активных и пассивных технических средств и реализацию технических решений.

Тональный сигнал – сигнал, вызываемый колебанием, совершающимся по синусоидальному закону.

"Троянские кони" - это программы, полученные путем явного изменения или добавления команд в пользовательские программы.

Угрозы - потенциально или реально существующие воздействия, приводящие к моральному или материальному ущербу.

Утечка - факт получения охраняемых сведений злоумышленниками или конкурентами.

Физические средства защиты – средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств и финансов и информации от противоправных воздействий.

Цели защиты информации - предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при их разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

"Черви" - программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самопроизводить копии.

Шаблон настроек - набор параметров и их значений, позволяющий управлять свойствами объектов системы защиты. Хранится в БД системы защиты. Использование шаблонов позволяет упростить процедуру настройки свойств объектов.

Электронная цифровая подпись (ЭЦП) - относительно небольшое количество дополнительной аутентифицирующей цифровой информации, передаваемой вместе с пописываемым текстом.

Ядро системы защиты - программа, которая автоматически запускается на защищенном компьютере при его включении и функционирует на протяжении всего времени работы компьютера.

UEL (User Executive List) - список программ, доступных для запуска пользователем в режиме замкнутой программной среды. Каждому пользователю присвоен свой UEL. См. Замкнутая среда.

СПИСОК ЛИТЕРАТУРЫ

Основная

21. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. – М.: РГГУ, 2002.
22. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.
23. Хорев А.А. Защита информации от утечки по техническим каналам. – М.: Гостехкомиссия России, 1998. – 320 с.
24. Ярочкин В.И. Информационная безопасность. – М.: Междунар. отношения, 2000. – 400 с.

Дополнительная

Алексеев Ю.И. и др./Под общей ред. А.Ф.Федорова, В.Н.Цыгичко. – М.: ПИР-Центр, 2001 – 238 с.

Алферов А.П., Зубов А.Ю., Кузмин А.С., Черемушкин А.В. Основы криптографии. – М.: Изд-во "Гелиос АРВ", 2001.

Бачило И.Н., Лопатин В.Н., Федотов М.А. Информационное право./Под ред. Акад. Б.Н.Топорнина. СПб.: Юридический центр,2001. – 789 с.

Кулаков В.Г., Андреев А.Б., Заряев А.В. и др. Защита информации в телекоммуникационных системах. – Воронеж: Воронежский институт МВД России, 2002. – 300 с.

Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.

Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений. – М.: ЮНИТИ-ДАНА, 2001.

Михаэль А.Бэнкс. Информационная защита ПК: Пер. с англ. – К.: ВЕК+, М.: Энтроп, СПб.: Корона-Принт 2001. – 272 с.

Панарин И.Н. Информационная война и власть. – М.: "Мир безопасности", 2001.

Таненбаум Э. Компьютеные сети. – СПб.: Питер, 2002. – 848 с.