МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ
ГИМНАЗИЯ №12

Чупрына Никита Ярославович
ученика 9Е класса

Система комплексной защиты информации на крупном предприятии

Годовая работа по информатике

Научный руководитель:
Учитель информатики Волкова А.А.

Липецк – 2006

ОГЛАВЛЕНИЕ

Введение

Информационная безопасность Российской Федерации определяется в Доктрине как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использовании ее в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия.

Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод граждан в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности; защиты информационных ресурсов государства от несанкционированного доступа; обеспечения безопасности информационных и телекоммуникационных систем России.

Для несанкционированного добывания информации в настоящее время используется широкий арсенал технических средств, из которых малогабаритные технические средства отражают одно из направлений в развитии современных разведывательных технологий. Выполняемые в портативном, миниатюрном и сверхминиатюрном виде, эти средства аккумулируют в себе новейшие научные, технические и технологические

достижения электроники, акустики, оптики, радиотехники и других наук. Такие средства находят широкое применение, как в деятельности правоохранительных органов, так и иностранных технических разведок, в подпольном информационном обеспечении незаконных экономических, финансовых и криминальных организаций. В условиях рыночной экономики появление значительного числа конкурирующих между собой различных структур естественным образом создало определенное пространство, на котором применение подобных устройств технической разведки для добывания информации различной значимости является наиболее вероятным.

Информационная сфера играет все возрастающую роль в обеспечении безопасности всех сфер жизнедеятельности общества. Через эту сферу реализуется значительная часть угроз не только национальной безопасности государства, но и экономическому благополучию учреждений и предприятий.

Одними из основных источников угроз информационной безопасности для последних – преступные сообщества, конкурентные организации, группы и формирования и противозаконная деятельность отдельных лиц, направленная на сбор или хищение ценной информации, закрытой для доступа посторонних лиц. Причем в последние годы приоритет в данной сфере деятельности смещается в экономическую область.

Главной причиной возникновения промышленного (экономического) шпионажа является стремление к реализации конкурентного преимущества – важнейшего условия достижения успеха в рыночной экономике. Охота за чужими секретами позволяет компаниям экономить собственные средства на ведение НИОКР и фундаментальные исследования, быть в курсе дел конкурентов, использовать их научно-технические достижения.

Промышленный шпионаж сегодня охватывает все сферы рыночной экономики. Ущерб от экономического шпионажа, например в банковской сфере, составляет сегодня в мире до 30 % от всех потерь, которые несут

банки. По неофициальным данным, хищения торговых и промышленных секретов обошлось американским кампаниям в 1992 г. в 100 млрд. долларов. По оценкам специалистов к 2003 г. указанные потери могут возрасти на 50%.

В условиях ожесточенной конкурентной борьбы на международном рынке масштабы промышленного шпионажа резко возрастают. Все шире используются плоды научно-технического прогресса. Шпионаж становится гибче, изощреннее и аморальнее. Наиболее активно промышленным шпионажем занимаются транснациональные корпорации. Подобно большому бизнесу экономическая разведка не знает границ. Существуют даже тайные биржи, где продают краденные промышленные секреты. Например, в США легально существует “Общество специалистов по добыванию сведений о конкурентах”, которое насчитывает 1500 постоянных членов. Это общество специализируется на добывании труднодоступной информации, характеризующей производственные способности фирм, образ жизни и личные наклонности их руководящего состава. Для получения такого рода информации используются как легальные, так и нелегальные методы и средства, которые представляют собой доходную разновидность бизнеса. По мнению международных экспертов, это объясняется тем, что в связи с окончанием холодной войны и уменьшением вероятности мирового вооруженного конфликта государства будут вести борьбу друг с другом в области экономики и технологий. Ту же борьбу (с поддержкой государства или без таковой) будут вести и предприятия всех видов и размеров.

Западный опыт промышленного шпионажа сегодня активно переносится на территорию России. В нашей стране промышленный шпионаж осуществляется в целях: овладения рынками сбыта, подделки товаров, дискредитации или устранения (физического или экономического подавления) конкурентов, срыва переговоров по контрактам, перепродажи фирменных секретов, шантажа определенных лиц, создания условий для подготовки и проведения террористических и диверсионных акций).

На рынке России представлен арсенал самых современных технических средств промышленного шпионажа, которые находят все более широкое применение на практике. К ним относятся: визуально-оптические, фотографические, телевизионные, тепловизионные (инфракрасные), акустические, радио-, радиотехнические и некоторые другие средства разведки.

Для организации защиты конфиденциальной информации необходимо знать возможности технических средств промышленного шпионажа и способы их применения.

Ряд владельцев локальных и выделенных систем связи (в том числе негосударственных и частных) предполагает в дальнейшем принимать меры для обеспечения конфиденциальности при передаче информации. Им необходима аппаратура, которая кроме обеспечения конфиденциальности передачи информации защищает каналы управления сетями связи от несанкционированного доступа.

За рубежом аппаратура, обеспечивающая конфиденциальность связи, имеется в свободной продаже. Появилась она и на нашем внутреннем рынке. Ведутся разработки и начата продажа отечественных устройств.

По общепринятой терминологии слово «конфиденциальный» значит: доверительный, неподлежащий огласке, секретный. Применительно к современным условиям и назначению систем связи закрытые виды информации можно подразделить на две группы: секретную и конфиденциальную.

Секретной будем считать информацию, отнесенную к государственной тайне, сохранность которой регламентируется соответствующими законами и за разглашение которой установлена уголовная ответственность. К конфиденциальной можно отнести информацию, предназначенную для использования ограниченным кругом лиц (например, коммерческие секреты, которыми пользуются доверенные лица какой-либо фирмы) и утечка которой не наносит государственного

ущерба, но может принести серьезный урон для различных учреждений и предприятий.

Обеспечение секретности передаваемой по сетям связи информации требует применения сложной аппаратуры засекречивания [ЗАС] и строгих организационных мероприятий (прокладка специальных кабелей связи; контроль за отсутствием “жучков” и побочных излучений; использование телефонных аппаратов, коммутационной и другой техники в специально защищенном исполнении и т.п.), что приводит к большим материальным затратам на оснащение и эксплуатацию сети. Этим требованиям удовлетворяют сети Правительственной связи, а также некоторые ведомственные. Аппаратура и устройства для этих сетей создаются по техническим требованиям заказчиков, осуществляющих эксплуатацию.

Обеспечение только конфиденциальности (без гарантии обеспечения секретности) требует значительно меньших материальных затрат и для подавляющего большинства абонентов сетей связи является более чем достаточным. Известно, что предотвратить случайное или преднамеренное подслушивание (обеспечить конфиденциальность) можно с помощью достаточно простых в эксплуатации устройств (в дальнейшем они будут именоваться устройствами или аппаратами конфиденциальной связи [УКС] или [АКС]) и без проведения дорогостоящих организационных и технических мероприятий.

Не вызывает сомнений, что есть достаточно много потребителей, готовых покупать и использовать УКС и АКС. Очевидно, что устройства конфиденциальной связи должны быть совместимы с аппаратурой, входящей в ВСС, и обеспечивать работу по защите информации.

Цель моей годовой работы заключается в обнаружение и классификации угроз информации, обнаружение путей утечки информации, описание и оценка основных средств разведки и зашиты информации,

вывод о современных средствах зашиты.

Глава 1. Информация как объект защиты.

1.1. Понятия информация, ее источники и носители.

Существует множество определений понятия «информация» от наиболее общего, философского: информация есть отражение материального мира, до наиболее узкого, практического: информация есть все сведения, являющиеся объектом хранения, передачи и преобразования.

До середины 20-х гг. XX в. под информацией действительно понимались «сообщения и сведения», передаваемые людьми устным, письменным или иным способом. С середины XX в. информация превращается в 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 (генетическая информация). Это одно из основных понятий кибернетики. В связи с развитием средств связи и телекоммуникаций, вычислительной техники и их использованием для обработки и передачи информации возникла необходимость измерять ее количественные характеристики. К. Шенноном и У. Уивером были предложены вероятностные методы для определения количества передаваемой информации. Появилось понятие «энтропия информации» как мера ее неопределенности.

Н. Винер предложил «информационное видение» кибернетики считать наукой об управлении в живых организмах и технических системах. Под информацией стали понимать уже не просто сведения, а только те из них, которые являются новыми и полезными для принятия решения, обеспечивающего достижение цели управления.

Информация — это сведения о предметах, объектах, явлениях, процессах, отображаемые в сознании человека или на каком-либо носителе для последующего восприятия их человеком.

Использование этого термина обычно предполагает возникновение материально-энергетического сигнала, воспринимаемого сенсорно или на

приборном уровне. Существование такого сигнала предполагает наличие носителя информации. При организации защиты засекреченной информации постоянно обращается внимание на необходимость защиты носителей секретной и конфиденциальной информации, а так как такая информация неотрывна от них, она не может существовать помимо носителя. Только получая доступ к носителю, злоумышленник может добыть интересующую информацию. При этом носитель информации становится источником ее для этого злоумышленника. Под понятием источник понимается какой-то объект, обладающий определенной информацией, к которой получили доступ одноразово или многократно интересующиеся ею лица. Источник связан с каким-то субъектом, имеющим ту или иную возможность доступа к информации. Источник в этой паре выступает как бы пассивной стороной, а субъект – активной.

Носитель секретной и конфиденциальной информации находится под постоянной защитой, доступ к нему строго регламентируется. Поэтому и доступ к такой информации соперником может быть получен только вопреки воле ее собственника. Такой несанкционированный доступ всегда связан с риском провала операции – основная цель защиты информации в конечном счете сводится к тому, чтобы не позволить сопернику получить доступ к охраняемому носителю информации.

Однако в деятельности по защите информации постоянно возникают ситуации, когда на носители информации не «повесишь замок», не закроешь их в сейф, особенно в процессе их использования, а также когда ими являются люди, различного рода излучения, служащие продуктом деятельности технических систем, каналов связи, излучением слаботочных приборов и т. д. Поэтому все эти носители являются потенциальными источниками информации. К ним-то и стремится получить доступ соперник.

Таким образом, с точки зрения обеспечения информационной безопасности под понятием носитель необходимо понимать какой-то объект, обладающий определенной информацией, которую можно получить

одноразово или многократно. Носитель связан с каким-то субъектом, имеющим ту или иную возможность доступа к информации. Тогда под носителем конфиденциальной информации будем понимать объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников. Рассматривая информацию с точки зрения отображения ее на каких–то или в каких–то материальных объектах, которые длительное время могут сохранять ее в относительно неизменном виде или переносить из одного места в другое, носителей защищаемой информации можно классифицировать следующим образом:

1.2. Виды представления информации.

Основные формы информации, представляющие интерес с точки зрения защиты:

- ✓ документальная;
- ✓ акустическая (речевая);
- ✓ телекоммуникационная и т.п.;

Документальная информация - содержится в графическом или буквенно-цифровом виде на бумаге, а также в электронном виде на магнитных и других носителях. Особенность документальной информации в том, что она в сжатом виде содержит сведения, подлежащие защите.

Акустическая информация - возникает в ходе ведения в помещениях разговоров, а также при работе систем звукоусиления и звуковоспроизведения.

Носителем речевой информации являются акустические колебания (механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины). Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4...6 кГц.

Телекоммуникационная информация - циркулирует в технических средствах обработки и хранения информации, а также в каналах

связи при ее передаче. Носителем информации при ее обработке техническими средствами и передаче по проводным каналам связи является электрический то к, а при передаче по радио и оптическому каналам – электромагнитные волны.

Основные объекты защиты информации:

- ✓ информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию;
- ✓ средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации ограниченного доступа, их информативные физические поля, т.е. системы и средства, непосредственно обрабатывающие информацию, отнесенную к коммерческой тайне, а также конфиденциальную информацию. Эти средства и системы часто называют ***техническими средствами приема, обработки, хранения и передачи информации*** (ТСПИ);
- ✓ технические средства и системы, не относящиеся к средствам и системам информатизации (ТСПИ), но размещенные в помещениях, в которых обрабатывается секретная и конфиденциальная информация. Такие технические средства и системы называются ***вспомогательными техническими средствами и системами*** (ВТСС). К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

1.3. Основные свойства информации как предмета защиты.

1*) Важность информации:* это обобщенный показатель, характеризующий значимость информации с точки зрения тех задач, для решения которых она используется. При этом необходимо определять как

важность самих задач для обеспечиваемой деятельности, так и степень важности информации для эффективного решения соответствующей задачи. Такой подход использует, например, академик И. А. Лазарев, определяющий, что одной из составляющих понятия информационная безопасность является достижение требуемого качества информации для решения важнейших задач обеспечения безопасности государства, личности, общества. Для количественной оценки важности информации используют два критерия: уровень потерь в случае нежелательных изменений информации в процессе обработки под воздействием дестабилизирующих факторов и уровень затрат на восстановление нарушенной информации.

Тогда коэффициент важности информации $К_{ви}$ можно представить в следующем виде: $K_{ви} = f(P_{пи}, P_{св})$

где $Р_{пи}$ – величина потерь при нарушении качества информации; $Р_{св}$ – величина стоимости восстановления ее качества.

Для информации, обрабатываемой и передаваемой в системе правительственной связи, существуют следующие категории важности: особой важности, совершенно секретно, секретно, конфиденциально
– характеризуемые размером ущерба для страны.

2) *Полнота информации*: это показатель, характеризующий меру достаточности информации для решения соответствующих задач. Полнота информации оценивается относительно вполне определенной задачи или группы задач. Поэтому, чтобы иметь возможность определять показатель полноты информации, необходимо для каждой задачи или группы задач заблаговременно составить перечень сведений, которые необходимы для их решения. Для представления таких сведений удобно воспользоваться так называемыми объектно-характеристическими таблицами (ОХТ), каждая из которых есть двухмерная матрица с приведенным в строках перечнем наименований объектов, процессов или явлений, входящих в круг интересов соответствующей задачи, а в столбцах – наименование их параметров, значения которых необходимы для решения задачи. Совокупность всех

таблиц, необходимых для обеспечения решения всех задач, может быть названа информационным кадастром объекта.

3) *Адекватность информации*: это степень соответствия действительному состоянию тех реалий, которые отображает оцениваемая информация. В общем случае адекватность определяется двумя параметрами: объективностью генерирования информации о предмете, процессе или явлении и продолжительностью интервала времени между моментом генерирования информации и текущим моментом, то есть до момента оценивания ее адекватности.

Рассматриваемый показатель широко применяётся в криптографии при оценке стойкости шифрования передаваемой информации. Например, аппаратура шифрования является аппаратурой гарантированной стойкости, если период времени до расшифрования противником перехваченного сообщения составляет такую величину, что к этому моменту значимость информации в результате ее старения близка к нулю, то и коэффициент адекватности близок к нулю.

4)*Релевантность информации*: это показатель информации, который характеризует соответствие ее потребностям решаемой задачи. Для количественного выражения данного показателя обычно используют так называемый коэффициент релевантности ($К_р$), определяющий отношение объема релевантной информации ($V_{ри}$) к общему объему анализируемой информации ($V_и$). Трудности практического использования данного коэффициента сопряжены с количественным выражениём объема информации.

Существует множество подходов в определении понятия «количество информации». Например, в сфере документооборота под этим понимается количество обрабатываемых документов. В сфере информационной обработки сигналов это понятие связано с понятием «энтропия».

5) *Толерантность информации*: это показатель, характеризующий удобство восприятия и использования информации в процёссе решения

задачи. Данное понятие является очень широким, в значительной мере неопределенным и субъективным. Так, для системы телефонной связи оно может характеризовать разборчивость речевых сообщений, передаваемых по каналам связи. Показатели первого и второго видов находятся в неразрывной связи. Так, с точки зрения обеспечения информационной безопасности объекта уровень важности информации определяет и требуемую степень ее защиты.

Проведение оценки качества информации по рассмотренным показателям позволяет проанализировать ее потенциальную ценность и исходя из этого определить необходимые меры защиты, то есть сделать информацию защищаемой.

Глава 2. Характеристика угроз безопасности информации

Виды угроз

Анализируя возможные пути воздействия на информацию, представляемую как совокупность n информационных элементов, связанных между собой логическими связями, можно выделить основные нарушения:

- ✓ физической целостности (уничтожение, разрушение элементов);
- ✓ логической целостности (разрушение логических связей);
- ✓ содержания (изменение блоков информации, внешнее навязывание ложной информации);
- ✓ конфиденциальности (разрушение защиты, уменьшение степени защищенности информации);
- ✓ прав собственности на информацию (несанкционированное копирование, использование).

Обобщая рассмотренные угрозы, можно выделить три наиболее выраженные для систем обработки информации:

1) подверженность физическому искажению или уничтожению;

2) возможность несанкционированной (случайной или злоумышленной) модификации;

3) опасность несанкционированного (случайного или преднамеренного) получения информации лицами, для которых она не предназначалась.

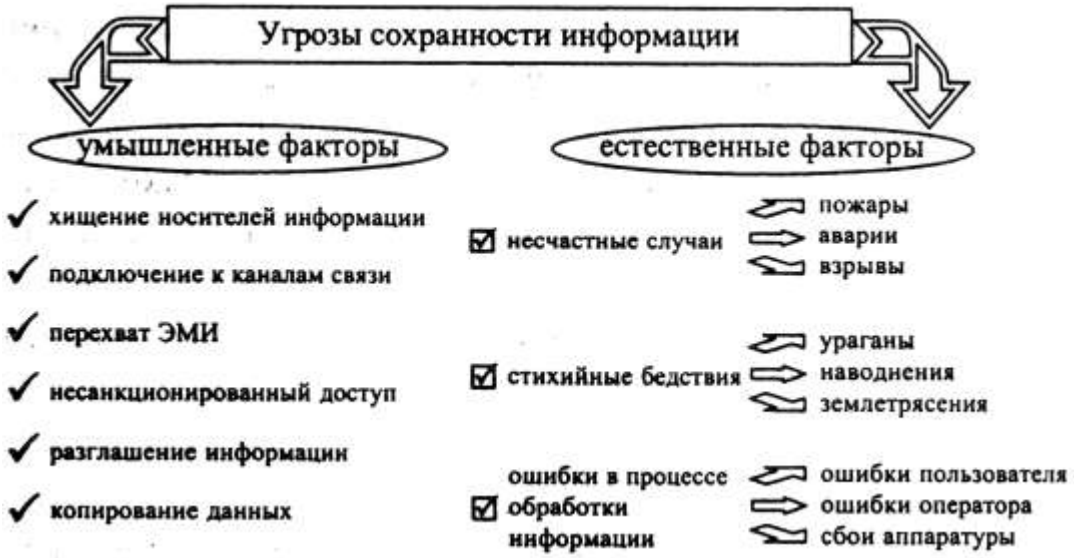
Кроме того, с точки зрения анализа процесса обработки информации выделяют такую угрозу, как блокирование доступа к обрабатываемой информации.

Характер происхождения угроз

Угрозы безопасности информации в современных системах ее обработки определяются ***умышленными*** и ***естественными*** разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных

пользователей, целями которых являются хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными, или преднамеренными, понимаются такие угрозы, которые обусловливаются злоумышленными действиями людей.

Случайными, или естественными, являются угрозы, не зависящие от воли людей. В настоящее время принята следующая классификация угроз сохранности информации:



Источники угроз

Под источником угроз понимается непосредственный исполнитель угрозы с точки зрения ее негативного воздействия на информацию. Источники можно разделить на следующие группы:

- ✓ люди;
- ✓ технические устройства;
- ✓ модели, алгоритмы, программы;
- ✓ технологические схемы обработки;
- ✓ внешняя среда.

В качестве элементов каналов утечки информации наибольший интерес представляют ТСПИ и ВТСС, имеющие выход за пределы

контролируемой зоны, 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, к ним не относящиеся, но проходящие через помещения, где установлены технические средства. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

Зона, в которой возможен перехват побочных электромагнитных излучений, называется опасной зоной. Пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется опасной зоной.(Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения).

Случайные антенны могут быть сосредоточенными и распределенными. ***Сосредоточенная случайная антенна*** представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К ***распределенным случайным антеннам*** относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Под ***техническим каналом утечки информации*** (ТКУИ) понимают совокупность объекта, технического средства разведки, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

Сигнал - является материальным носителем информации.

В зависимости от природы сигналы распространяются в определенных физических средах. Средой распространения могут быть газовые, жидкостные и твердые среды, например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт и т.п.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата технические каналы утечки можно разделить на:

1) электромагнитные, электрические и параметрические – для телекоммуникационной информации.

2) воздушные, вибрационные, электроакустические, оптико-электронный и параметрические – для речевой информации.

3)оптический – для документальной информации.

К *электромагнитным* каналам утечки информации относятся:

– перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ.

– перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС.

– перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио устройств разведки, размещенными вне контролируемой зоны.

К *электрическим* каналам утечки информации относится съем:

– наводок ПЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников.

– информационных сигналов с линий электропитания ТСПИ.

– информации путем установки в ТСПИ электронных устройств перехвата информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к системам электропитания и заземления ТСПИ. Для этих целей используются специальные средства радио и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации, устанавливаемые в ТСПИ, часто 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 информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем передается заказчику.

Параметрический канал утечки информации – образуется путем “высокочастотного облучения” ТСПИ.

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

К *воздушным техническим* каналам утечки информации относятся среды распространения акустических сигналов – воздух. Перехват информации ведется при помощи устройств перехвата акустической информации.

Для перехвата акустической (речевой) информации используются:

– портативные диктофоны и проводные микрофонные системы скрытой звукозаписи;

– направленные микрофоны;

– акустические радиозакладки (передача информации по радиоканалу);

– акустические сетевые закладки (передача информации по сети электропитания 220В);

– акустические ИК - закладки (передача информации по оптическому каналу в ИК - диапазоне длин. волн);

– акустические телефонные закладки (передача информации по телефонной линии на высокой частоте);

– акустические телефонные закладки типа “телефонное ухо” (передача информации по телефонной линии “телефону-наблюдателю” на низкой частоте).

К *вибрационным* техническим каналам утечки информации относятся среды распространения виброакустических сигналов – ограждения конструкций зданий, сооружения: стены, потолки, полы, трубы водоснабжения, канализации и другие твердые тела.

Для перехвата виброакустических колебаний используются средства разведки с контактными микрофонами:

– электронные стетоскопы;

– радиостетоскопы (передача информации по радиоканалу).

Электроакустические технические каналы утечки информации – возникают за счет преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих “микрофонным эффектом”, а также путем “высокочастотного навязывания”.

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

Технический канал утечки информации путем “высокочастотного навязывания” может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от генератора, подключенного в линию, имеющую функциональную связь с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что

нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используются специальные приемники с достаточно высокой чувствительностью.

Оптико-электронный (лазерный) канал утечки акустической информации – образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы (ЛАЛС), иногда называемые “лазерными микрофонами”.

К *оптическому* каналу утечки информации относится: фото, видео и т.п. (восприятие документальной информации при визуальном контакте, возможность восприятия речи).

Параметрические технические каналы утечки информации – могут быть реализованы путем “высокочастотного облучения” помещения, где установлены полуактивные закладные устройства или технические средства, имеющие элементы, некоторые параметры которых изменяются по закону изменения акустического (речевого) сигнала.

Глава 3. Методы и средства обеспечения информационной безопасности

Цели и задачи обеспечения информационной безопасности: формирование множества задач осуществляется на основе анализа объективных возможностей по реализации поставленных целей защиты. Такое их множество может состоять из ряда классов, включающих содержащие однородные в функциональном отношении задачи. Класс задач – однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию одной или нескольких целей.

Учитывая, что основной целью обеспечения информационной безопасности является обеспечение защиты системы от обнаружения и от информационного воздействия, а также содержания информации, выделяются задачи соответствующих видов.

ЦЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ		
Обеспечение защиты системы от обнаружения	Обеспечение защиты содержания информации	Обеспечение защиты системы от информационного воздействия
КЛАССЫ ЗАДАЧ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ		
1.1. Скрытие 1.2. Дезинформация 1.3. Легендирование	2.1. Введение избыточности 2.2. Резервирование элементов 2.3. Регулирование доступа 2.4. Регулирование использования 2.5. Маскировка 2.6. Регистрация 2.7. Уничтожение 2.8. Сигнализация 2.9. Оценка 2.10. Реагирование	3.1. Защита от воздействия на технические средства 3.2. Защита от воздействия на общество 3.3. Защита от воздействия на человека

3.1. Технические средства защиты.

Технические средства защиты – это средства, в которых основная защитная функция реализуется некоторым техническим устройством.

К несомненным достоинствам технических средств относятся широкий круг задач, достаточно высокая надежность, возможность создания развитых комплексных систем защиты, гибкое реагирование на попытки несанкционированных действий, традиционность используемых методов осуществления защитных функций. Основными недостатками являются высокая стоимость многих средств, необходимость регулярного проведения регламентных работ и контроля, возможность подачи ложных тревог.

Системную классификацию технических средств защиты удобно провести по следующей совокупности показателей:

– функциональное назначение, то есть основные задачи защиты объекта, которые могут быть решены с их применением;

– сопряженность средств защиты с другими средствами объекта обработки информации (ООИ);

– сложность средства защиты и практичность его использования;

– тип средства защиты, указывающий на принципы работы его элементов;

– стоимость приобретения, установки и эксплуатации.

Рассмотрим возможные значения перечисленных показателей:

1. Функциональное назначение

В зависимости от цели и места применения, выполняемых функций и физической реализуемости технические средства можно условно разделить на физические и аппаратные:

3.2. Аппаратные средства защиты:

– нейтрализация технических каналов утечки информации выполняет функцию защиты информации от ее утечки по техническим каналам;

– поиск закладных устройств – защита от использования злоумышленником закладных устройств съема информации;

– маскировка сигнала, содержащего конфиденциальную информацию;

– защита информации от обнаружения ее носителей (стенографические методы) и защита содержания информации от раскрытия (криптографические методы);

3.3. Физические средства защиты:

– внешняя защита: защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств объекта;

– внутренняя защита: защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации;

– опознавание: специфическая группа средств, предназначенная для опознавания людей и идентификации технических средств по различным индивидуальным характеристикам.

Сопряженность с основными средствами защиты по степени взаимодействия с другими техническими устройствами средства защиты подразделяются:

– на автономные (выполняющие свои защитные функции независимо от функционирования средств ООИ, то есть полностью автономно);

– сопряженные (выполненные в виде самостоятельных устройств, но выполняющие защитные функции в сопряжении с основными средствами);

– встроенные (конструктивно включенные в состав аппаратуры технических средств ООН).

В зависимости от принципов построения технического средства защиты различают:

– функциональный узел (простое устройство);

– блок;

– агрегат (сложное устройство, состоящее из нескольких блоков);

– автономную систему.

Технические средства защиты, имеющие указанную сложность, (за исключением автономной системы), выполняют свои функции в совокупности с другими средствами защиты. Автономные технические средства защиты, как правило, решают отдельную задачу (осуществляют отдельную функцию).

По принципу работы элементов устройств средства защиты подразделяются на механические, электрические, оптические, электронные, комбинированные. Современные технические средства защиты имеют, как правило, комбинированный тип (электромеханические, оптико-электронные и т.п.).

Стоимость технических средств защиты может быть незначительной, средней, большой, очень большой. Данный показатель имеет относительный характер и может быть использован при сравнении отдельных технических средств защиты, выполняющих, например, одну и ту же функцию.

Рассмотрим характеристики некоторых современных технических средств защиты информации в соответствии с представленной классификацией:

3.4. Технические средства идентификации и установления подлинности

Идентификация и установление подлинности объекта заключаются в проверке его соответствия истинному объекту и производятся с целью определения возможности допуска объекта к информации ограниченного пользования. В основе процесса идентификации личности лежит анализ его

биометрических особенностей или специально предъявляемых носителей ключа.

На усовершенствование биометрических идентификаторов направлены изыскания ведущих международных научных центров, и именно эти разработки активно финансирует военное ведомство. Разработаны специальные методики оценки эффективности, используя которые, экспериментально определяют численные коэффициенты надежности системы: ошибки первого рода (false reject rate, «ложный отказ» – принятие «своего» за «чужого») и второго (false acceptance, «ложный допуск» – принятие «чужого» за «своего»). Основными являются следующие способы идентификации.

Геометрия руки:

Метод биологической идентификации по форме кисти руки был разработан еще в 60-е гг. Первый массовый аппарат назывался Indentimat. В качестве идентификационного параметра он использовал длину пальцев. В конце 80-х гг. появились современные системы, использующие метод трехмерной идентификации – HandKey. Этот метод предусматривает оценку нескольких параметров руки, в том числе ширины и толщины ладони в различных местах, длины пальцев, их толщины и формы.

Операция снятия, кодирования информации и сверки с банком данных занимает 1-2с. Ошибка первого рода достигает 0,03%, второго рода – 0,1%.

Почерк

Разработаны автоматические системы подтверждения подписи, измеряющие, характеристики движения руки при письме (усилия при нажатии на перо, скорость, ускорение). Преобразователи, измеряющие характеристики почерка, могут устанавливаться как в пишущем устройстве, так и под пластиной, на которой ставится подпись.

Одна из последних моделей «интеллектуальных ручек SmartPen – разработана в бельгийском исследовательском институте IMEC. Ручка содержит микродатчики для снятия трехмерных динамических параметров,

процессор для обработки данных, передатчик и систему криптографической защиты для предотвращения радиоперехвата. Ручка может писать на обычной бумаге, и ее стоимость составляет от 50 до 250 долларов.

Дактилоскопия:

Идентификация происходит по папиллярным узорам пальцев руки, которые формируются еще в утробе матери, являются строго индивидуальными и остаются неизменными на протяжении всей жизни.

Одну из самых надежных систем представляет американская компания «Indentix-TouchLock». Считывание и проверка занимают 5 – 6с. Ошибка первого рода – 2%, второго – 0,0001%. Аналогичное отечественное устройство «Кордон» имеет время идентификации 2 – 4с. Ошибка первого рода – 0,001%, второго рода – 0,00001%.

Рисунок сетчатки глаза:

Неповторимость конфигурации кровеносных сосудов сетчатки глаза доказана в 1935г. американскими исследователями Саймоном и Голдштейном. Участок сетчатки, расположенный вокруг центра хрусталика, сканируется неполяризованным, низкой интенсивности светом, испускаемым инфракрасными светодиодами. Различная интенсивность света, отраженного от различных точек сетчатки в процессе сканирования, отражает индивидуальное расположение кровеносных сосудов сетчатки глаза. Процесс идентификации занимает около 7с. Ошибка первого рода – 0,4%, второго рода – 0%. Хотя процедура сканирования полностью безопасна, около 4% сотрудников по психологическим мотивам ни при каких условиях не согласны смотреть на яркий пучок света.

Радужная оболочка глаза:

Источником информации является трабекулярная сетка радужной оболочки глаза, имеющая различные бороздки, кольца, ореол, маленькие точки и т. д.

Характеристики речи

Идентификация по голосу:

Один из бурно развивающихся методов. Современные системы анализируют несколько характеристик речи, среди которых:

– огибающая формы сигнала;

– период ВЫСОТЫ тона;

– относительный спектр амплитуды;

– резонансные частоты речевого тракта и т. д.

Для повышения достоверности опознавания используется речевая подсказка. В качестве проблем, с которыми пока плохо борется современная техника, можно отметить влияние на качество идентификации посторонних шумов и сложность в борьбе с изменениями тональности (насморк, настроение и т.д.) Кроме того, существенным оказывается психологический фактор: стоит системе один раз не пропустить пользователя, как человек, помня о неудаче, начинает волноваться, старается управлять голосом, в результате шансов на идентификацию у него становится еще меньше.

Инфракрасная карта лица:

Источником информации является тепловой образ лица – своего рода комбинация термальных свойств сосудистых структур, их формы и плотности, свойств подкожных тканей, хрящей, кожи и т. д., остающаяся постоянной даже после пластической операции.

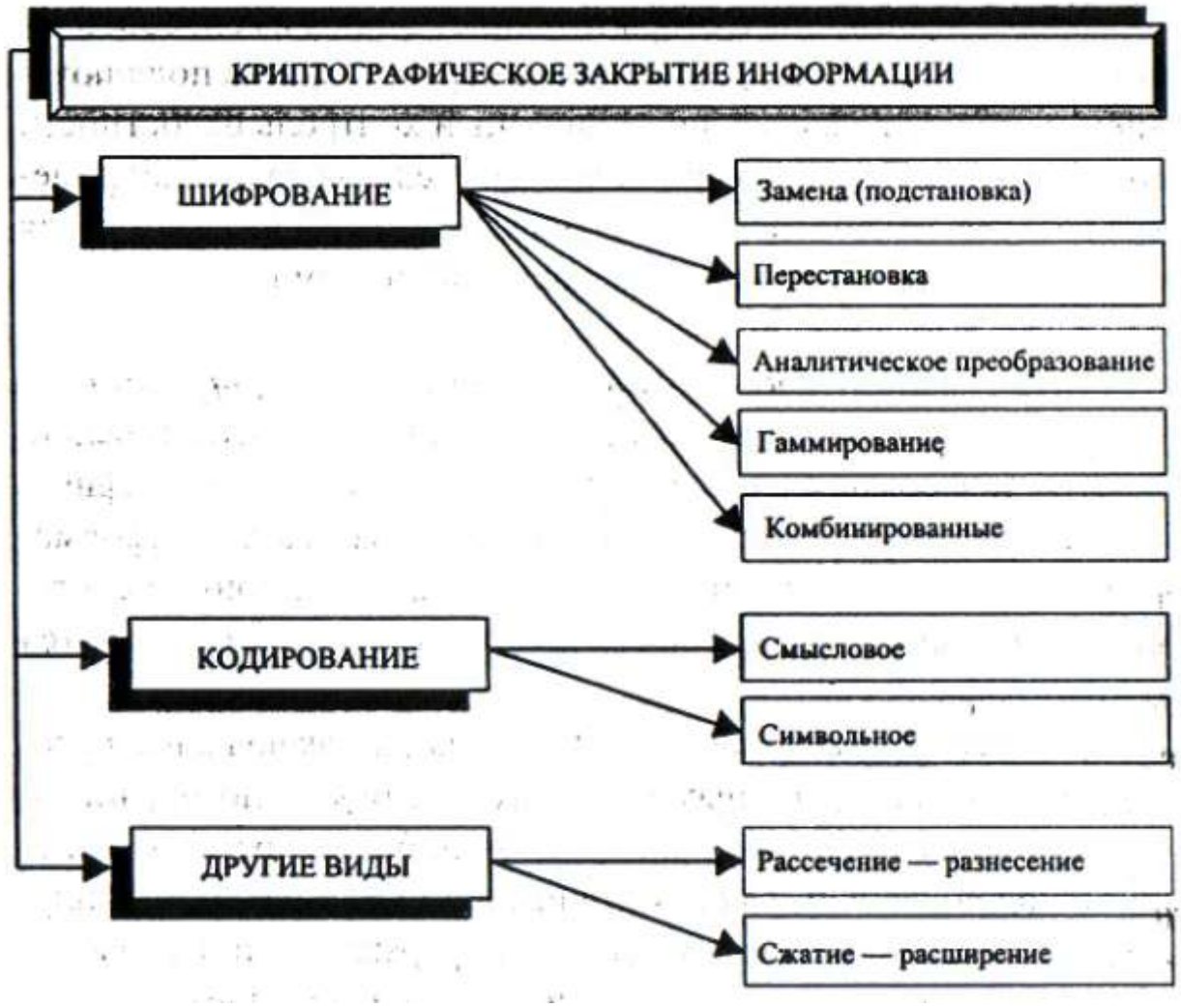
3.5. Технические средства маскировки информации

Как было указано выше, данная категория аппаратных средств защиты информации реализуется на основе стенографических и криптографических методов преобразования информации. В рамках информационно-телекоммуникационной системы специального назначения (ИТКС СН) основными являются, криптографические средства.

Криптографическое закрытие информации заключается в преобразовании ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, то есть в приведении ее к неявному виду. Для ознакомления с шифрованной

информацией применяется обратный процесс — декодирование (дешифрование).

Классификация криптографических методов преобразования информации:



Под шифрованием понимается такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения. Все известные способы шифрования можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование.

Под кодированием понимается такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами

(цифровыми, буквенными, буквенно-цифровыми сочетаниями и т. п.). Этот метод имеет две разновидности:

– смысловое кодирование, когда кодируемые элементы имеют вполне определенный смысл (слова, предложения, группы предложений);

– символьное кодирование, когда кодируется каждый символ защищаемого сообщения.

К отдельным видам криптографического закрытия отнесены методы расчленения – разнесения и сжатия данных. Расчленение — разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам ЗУ или располагаются на различных носителях. Сжатие данных представляет собой замену часто встречающихся одинаковых строк данных или последовательностей одинаковых символов некоторыми заранее выбранными символами.

Криптографическая защита на ОИ может применяться как для защиты информации, обрабатываемой в ЭВМ иди хранящейся в различного типа ЗУ, так и для закрытия информации, передаваемой между различными элементами системы по линиям связи. Поэтому криптографические методы могут использоваться как внутри отдельных устройств или звеньев системы, так и на различных участках линий связи.

Аппаратура шифрования в соответствии со своим предназначением может классифицироваться по следующим показателям:

• *по виду обрабатываемого сигнала:*

– аппаратура шифрования данных. Используется в сетях передачи данных систем документальной связи;

– аппаратура телефонной шифрованной связи. Конструктивно отличается от первой наличием аналого-цифровых преобразователей;

• *по режиму использования:*

– аппаратура линейного шифрования – производит криптографические преобразования входного сигнала в режиме реального времени;

– аппаратура предварительного шифрования. Зашифрованное с ее помощью сообщение передается по любым, в том числе и открытым, каналам связи;

• *по месту установки в ИТКС СН:*

– аппаратура шифрования канального уровня. Включает аппаратные средства, предназначенные для работы по телефонным, телеграфным и цифровым (в то числе широкополосным) каналам связи;

– аппаратура абонентского шифрования. Устройства криптографической защиты совмещены с терминальным (оконечным) оборудованием пользователя.

3.6. Программные средства защиты

Для нейтрализации всего комплекса угроз информации, обрабатываемой на ПЭВМ, необходимо, как указывалось выше, решить две основные группы задач по защите информации:

1) обеспечение целостности информации (физической и логической);

2) защита от несанкционированного доступа (для предупреждения несанкционированной модификации, получения и копирования информации).

Основную опасность для целостности информации представляют преднамеренные угрозы, создаваемые людьми в злоумышленных целях. Такие угрозы могут быть непосредственными, если злоумышленники получает доступ к ПЭВМ, и опосредованными, когда угрозы создаются с помощью промежуточного носителя, чаще всего с помощью дискеты. Из преднамеренных угроз наибольшее распространение получили так называемые разрушающие программные средства (РПС).

Программные средства являются одними из основных средств борьбы с РПС.

Эти программы можно разделить на несколько видов:

1) *Программы – детекторы* проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы – детекторы могут обнаруживать лишь те вирусы, которые ей известны. Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова – в ней может сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, не известная программам – детекторам.

2) *Программы – доктора*, или фаги, «лечат» зараженные программы, «выкусывая» из зараженных программ тело вируса. Большинство программ-докторов умеют «лечить» только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов.

3) *Программы – ревизоры* сначала запоминают сведения о состоянии программ и системных дисков. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходными. О выявленных несоответствиях сообщается пользователю

4) *Доктора – ревизоры*: это гибриды ревизоров и докторов (не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние). Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей диска. Это позволяет вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы. Конечно, доктора – ревизоры: это не панацея. Они могут лечить не от всех вирусов, а только от тех, которые используют

«стандартные», известные на момент написания программы, механизмы заражения файлов. Но все же защита от 90–95% вирусов это совсем неплохо.

5) *Программы – фильтры* располагаются резидентно в оперативной памяти компьютера и перехватывают все обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда. Такими «подозрительными» действиями являются, в частности, изменение .COM и .EXE – файлов, снятие с файла атрибута «только для чтения», прямая запись на диск, форматирование диска, установка «резидентной» программы. При каждом запросе на «подозрительное» действие на экран компьютера выводится сообщение о том, какое действие затребовано, и какая программа желает его выполнить. Можно либо разрешить выполнение этого действия, либо запретить его. Степень защиты, обеспечиваемую программами –фильтрами, не следует переоценивать, так как многие вирусы для своего размножения и нанесения вреда обращаются непосредственно к программам операционной системы, не используя стандартного способа вызова этих программ через прерывания, а резидентные программы для защиты от вируса перехватывают только эти прерывания. Кроме того, программы – фильтры не помогают от заражения винчестера вирусами, которые распространяются через загрузочный сектор, поскольку такое заражение происходит при загрузке DOS, то есть до запуска любых программ или установки драйверов. Однако преимущества программ – фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

6) *Программы – вакцины*, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными (крайне неэффективны).

Как показывает практика, несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленного завладения защищаемой информацией в современных АСОД.

Основными программными средствами защиты ПЭВМ от НСД являются следующими:

1. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации. При решении этой задачи система защиты должна надежно определять законность каждого обращения к ресурсам, а законный пользователь должен иметь возможность убедиться, что ему предоставляются именно необходимые компоненты. Для опознавания пользователей к настоящему времени разработаны и нашли практическое применение следующие способы:

– *С использованием простого пароля*. Каждому зарегистрированному пользователю выдается персональный пароль, который он должен держать в тайне. При каждом обращении к ЭВМ специальная программа сравнивает введенный пользователем пароль с эталоном, и при совпадении запрос пользователя принимается к исполнению;

– *Опознавание в диалоговом режиме*. В файлах механизмов защиты заблаговременно создаются записи, содержащие персонифицирующие пользователя данные (дата рождения, рост, вес, имена и даты рождения родных и т. п.) или достаточно большой и упорядоченный набор паролей. При обращении пользователя к системе программа механизма защиты предлагает ему назвать некоторые данные из указанных файлов. По результатам сравнения принимается решение о допуске;

– *Опознавание по индивидуальным особенностям и физиологическим характеристикам* (пример таких систем приводился выше). Данный способ является весьма надежным, но требует применения специальных устройств для съема и ввода соответствующих параметров и программ их обработки и сравнения с эталоном. Одним из вариантов, использующим только программное обеспечение и удешевляющим процесс опознавания, является

опознавание пользователя по параметрам его работы с клавиатурой (скорость набора текста, интервалы между нажатием клавиш и др.);

– *Опознавание по радиокодовым устройствам*, генерирующим индивидуальные для каждого пользователя радиосигналы;

– *Опознавание по специальным идентификационным карточкам*, на которые наносятся данные, персонифицирующие пользователя (персональный номер, специальный шифр или код и т. п.).

2. Разграничение доступа к элементам защищаемой информации.

Каждому зарегистрированному пользователю предоставляется возможность беспрепятственного доступа к информации в пределах его полномочий и исключается возможность их превышения. Данное разграничение может осуществляться несколькими способами:

– *По уровням секретности*. Защищаемые данные распределяются по массивам таким образом, чтобы в каждом из них содержались данные одного уровня секретности. Пользователю разрешается доступ к определенному уровню и массивам низших уровней;

– *По специальным спискам*. Для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов данных, к которым ему предоставлено право доступа;

– *По матрицам полномочий*. Формируется двумерная матрица, в строках которой содержатся идентификаторы зарегистрированных пользователей, а в столбцах – идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента (например, 00 — доступ запрещен, 01 — разрешено только чтение, 10—разрешена только запись, 11 — разрешены запись и чтение);

– *По специальным мандатам*: способ разового разрешения на допуск к защищаемому элементу данных.

3. Криптографическое закрытие защищаемой информации.

Данный механизм защиты можно подразделить на:

– *Криптографическое закрытие информации, хранимой на носителях*. При этом достигаются две цели защиты информации: во-первых, с помощью известных алгоритмов шифрования обеспечивается требуемая криптографическая стойкость защиты; во-вторых, как правило, криптографические преобразования информации сопровождаются архивацией данных с уменьшением их объемов (сжатие данных);

– *Криптографическое преобразование информации в процессе ее обработки и передачи*. Данный механизм предполагает засекречивание информации непосредственно в процессе ее обработки, практически полностью исключая тем самым возможность НСД к ней. Для этого дополнительно к программным используются специализированные аппаратные средства защиты, например устройство «Криптон».

4. Регистрация всех обращений к защищаемой информации.

Данный механизм позволяет решить следующиё задачи:

– *Контроль использования защищаемой информации*;

– *Выявление попыток НСД к информации*;

– *Накопление статистических данных о функционировании систем защиты с целью повышения её эффективности*;

Как правило, это реализуется соответствующими программами регистрации, позволяющими накапливать данные о попытках доступа к информации в определенных «спрятанных» файлах.

Множество программных средств защиты не ограничиваются рассмотренными. Данные средства решают также широкий круг задач в системах контроля и управления доступом на объекты, поиска закладных устройств, выявления технических каналов утечки информации и др.

3.7. Средства поиска закладных устройств

Индикаторы электромагнитного поля позволяют обнаруживать излучающие закладные устройства, использующие для передачи информации

практически все виды сигналов, включая широкополосные шумоподобные и сигналы с псевдослучайной скачкообразной перестройкой несущей частоты.

Принцип действия приборов основан на интегральном методе измерения уровня электромагнитного поля в точке их расположения. Наведенный в антенне и спроектированный сигнал усиливается, и в случае превышения им установленного порога срабатывает звуковая или световая сигнализация.

В качестве индикаторов электромагнитного поля используются отечественные приборы: ИПФ-Ч, D-006, D-008, РТ022, РТ025, RM-10, «Оса», ДИ-04, ИП-3, ИП-4, ИПАР-01, «Гамма-2» и другие, а также импортные – VL-5000P, HKG GD 4120, Delta V/2, TRD-800, CPM-700 и т.д.

В результате дальнейшего развития индикаторов поля созданы широкополосные радиоприемные устройства – *интерсепторы*. Приборы автоматически настраиваются на частоту наиболее мощного радиосигнала (как правило, уровень этого сигнала на 5–20 дБ превышает все остальные) и осуществляют его детектирование. Принцип «захвата» частоты радиосигнала с максимальным уровнем и последующим анализом его характеристик микропроцессором положен в основу работы современных портативных радиочастотомеров. Микропроцессор производит запись сигнала во внутреннюю память, цифровую фильтрацию, проверку на стабильность и когерентность сигнала и измерение его частоты с точностью от единиц герц до десятков килогерц. Значение частоты в цифровой форме отображается на жидкокристаллическом экране. Кроме частоты сигнала, многие радиочастотомеры позволяют определить его относительный уровень.

Наиболее широко применяются частотомеры фирм «Optoelectronics-MI», «Scout», «Cub», «ОЕ-ЗОООА» и другие. Они позволяют практически мгновенно определять частоту сигналов в диапазоне частот от 10 Гц –10 МГц до 1,4–3,0 ГГц. Чувствительность радиочастотомеров составляет от 0,5 До 12 мВ – на частотах до 1 ГГц и от 1 До 100 мВ – на частотах от 1 до 3 ГГц.

Для обнаружения работающих диктофонов применяются так называемые *детекторы диктофонов*, которые, по сути, являются детекторными приемниками магнитного поля. Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи.

Сканерные приемники можно разделить на две группы: переносимые и перевозимые, портативные. К переносимым относятся малогабаритные сканерные приемники весом 150—350 г. Они имеют автономные аккумуляторные источники питания и свободно умещаются во внутреннем кармане пиджака.

Перевозимые сканерные приемники отличаются от переносимых несколько большим весом (от 1,2 до 6,8 кг), габаритами и, конечно, большими возможностями. Они, как правило, устанавливаются или в помещениях, или в автомашинах. Почти все перевозимые сканерные приемники имеют возможность управления с ПЭВМ.

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

– автоматического сканирования в заданном диапазоне частот;

– автоматического сканирования по фиксированным частотам;

– ручном.

Портативные анализаторы спектра, в отличие от сканерных приемников, при сравнительно небольших габаритах (до 30 см) и весе (от 9,5 до 20 кг) позволяют не только принимать сигналы в диапазоне частот от 30 Гц...9 кГц до 1 ,8...40 ГГц, но и анализировать их тонкую структуру. Например, цифровые анализаторы спектра HP8561E фирмы «Hewlett Packard» позволяют измерять параметры сигнала в диапазоне частот от 30 Гц до 6,5 ГГц, а анализаторы спектра фирмы «Tektronix» – в диапазоне частот от 9 кГц до 40 ГГц.

Средства контроля проводных линий предназначены для выявления, идентификации и определения местоположения закладных устройств, подключаемых к проводным линиям. К ним относятся в том числе, электросеть, телефонные кабели, линии селекторной связи, пожарной сигнализации и т. п.

Немалые локаторы, металлоискатели, обнаружители пустот и рентгеновские аппараты используют физические свойства среды, в которой может размещаться закладное устройство, или свойства элементов закладных устройств, независимо от режима их работы.

Способность нелинейного локатора обнаруживать радиоэлектронные устройства основана на следующем. Любые радиоэлектронные устройства (РЭУ), независимо от размера и функционального назначения, состоят из печатных плат с проводниками, которые представляют для зондирующего сигнала локатора набор элементарных антенн – вибраторов. В разрыв отдельных проводников включены полупроводниковые элементы: диоды, транзисторы, микросхемы.

В результате облучения РЭУ зондирующим сигналом на частоте f на его полупроводниковых элементах через элементарные антенны наводится переменная ЭДС. В силу нелинейного характера вольт – амперной характеристики (ВАХ) элементов РЭУ переменный сигнал высокой частоты локатора претерпевает нелинейное преобразование в набор гармоник, частоты которых равны кратному целому числу зондирующей частоты локатора (2 f, 3 f и т.д.). С помощью тех же самых проводников печатной платы (элементарных антенн) весь спектр, включающий сигналы как на основной частоте f, так и на частотах гармоник 2 f 3 f и т.д., переизлучается в эфир. Приемник локатора, принимая любую высшую гармонику переотраженного зондирующего сигнала локатора, устанавливает наличие в зоне облучения РЭУ. Так как амплитуда сигнала на гармонике резко убывает с увеличением ее номера, то в нелинейных локаторах в основном используют вторую и реже третью гармоники.

Ряд закладных устройств выполняются по МОП – технологии, в экранированных корпусах. Поэтому их обнаружение даже с использованием нелинейных локаторов затруднено, так как уровень переизлученных сигналов на второй и третьей гармониках незначителен. Для поиска таких закладных устройств могут использоваться металлоискатели.

Технические средства обнаружения пустот позволяют повысить достоверность их выявления в сплошных средах (кирпичных и бетонных стенах, в деревянных конструкциях и др.), которое ранее осуществлялось путем простукивания этих сред. Пустоты в сплошных средах изменяют характер распространения структурного звука и спектр колебаний среды под действием ударов. В итоге звук от участка с пустотой воспринимается более громким и звонким. В качестве технических средств, выявления пустоты на основе акустических свойств, могут применяться различные ультразвуковые приборы.

Для просмотра предметов неизвестного назначения и выявления закладных устройств применяют переносные досмотровые рентгеновские комплексы двух видов: устройства с отображением изображения на экране просмотровой приставки и рентгенотелевизионные установки.

Заключение

С каждым годом проблема зашиты информации становится все острее, информационная сфера играет все возрастающую роль в обеспечении безопасности всех сфер жизнедеятельности общества, зависимость человека от информации растет, и проблема зашиты информации становится все острее. Поэтому с каждым годом совершенствуются и средства зашиты и средства разведки, в этой отрасли аккумулируются последние достижения электроники, акустики, оптики, радиотехники.

В своей работе я рассмотрел новейшие средства разведки и зашиты информации, охарактеризовал основные угрозы информационной безопасности и основные методы зашиты информации, как для частных лиц, так и для крупных предприятий и организаций.

Литература

Методические основы обеспечения информационной безопасности объекта. В.Ф.Шпак

Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие - М.Гелиос АРВ, 2005.-192с.

Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И.

Интернет

http://www.sinf.ru/index.htm - НПО "Защита информации"

http://daily.sec.ru/dailypbls.cfm?rid=9 - Защита информации / Публикации на Sec.Ru

http://www.stack.net/db/sect/413 - Защита информации, средства защиты и методы защиты информации

http://www.rambler.ru & http://www.yandex.ru– Поисковые системы.