ГЛАВА 5

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Для обеспечения безопасной передачи информации необходимо определить основные направления обеспечения защиты.

Коммерческая тайна – это информация, охраняемая предпринимателем от посторонних лиц. Коммерческая информация может интересовать Ваших конкурентов. Например, бухгалтерская отчетность, количество денег на счетах, список деловых партнеров, оборот средств, заключаемые контракты и др.

Широкое применение находят средства скрытого наблюдения и прослушивания в коммерческой деятельности, в сфере безопасности частных лиц и быту. С целью шантажа средствами специальной техники, могут быть получены компрометирующие материалы.

Обеспечить безопасность информации можно, создав службу безопасности или воспользоваться услугами охранных фирм, у которых есть опыт работы в области защиты информации.

Наряду с организационными мерами по защите информации от несанкционированного доступа, о которых говорилось в первой главе, не следует пренебрегать техническими средствами.

В дальнейшем под защитой информации будем понимать использование технических средств.

В Украине запрещены производство и продажа специальной техники без соответствующего лицензирования. Однако, политические и экономические условия создают предпосылки быстрого заполнения рынка средствами несанкционированного съема информации и наблюдения.

Главными производителями специальной техники являются США, Германия, Япония и Россия (табл. 5.1). Появляются образцы отечественной техники.

Коммерческие фирмы уже сейчас предлагают такие изделия в широком ассортименте. Радиолюбители также пробуют свои силы и изготавливают, в основном, радиомикрофоны, устройства прослушивания телефонных сетей, выносные микрофоны.

Существует множество технических каналов информации. На рис. 5.1 представлены наиболее часто используемые.

Источники информации, доступные техническим средствам несанкционированного доступа, представлены на рис. 5.1 слева.

Таблица 5.1.

Производители специальной техники						
Наименование техники	*Оптоэлектроникс США*	*REI США*	*CCS США*	*PK Electronic Германия*	*AOR Япония*	*ICOM Япония*
Передатчики				●		
Приемники, сканеры	●	●			●	●
Оптика			●			
Видеокамеры			●			
Средства защиты информации	●	●	●			
Техника перехвата	●	●		●		
Шумогенераторы		●				

Рис. 5.1. ***Каналы утечки информации***

Технические каналы утечки информации могут быть естественными и искусственными. К естественным каналам относятся:

– акустический канал;
– телефонные линии;
– линии радиосвязи (радиотелефон, пейджинговая связь, радиостанции и т. д.);
– побочные излучения оргтехники.

Естественные каналы могут контролироваться, например, записывающими устройствами. Дистанционно речевая информация регистрируется через оконные проемы, стены зданий, открытое окно или форточку и т. п.

Искусственные каналы создаются преднамеренно. Речевая информация может записываться или передаваться посредством радиоволн (миниатюрные радиопередатчики) и по проводным линиям (линии сигнализации, сети электропитания).

Любая проводная линия может быть использована для передачи сигналов в качестве проводника или антенны. Поэтому возможностей для подключения передающих устройств сколько угодно.

Защита информации может быть активной и пассивной. Активная защита создает помехи, препятствующие съему информации. Пассивная – обнаруживает каналы информации.

В выборе устройств для защиты информации следует проконсультироваться со специалистами. Они помогут выбрать комплект оборудования в соответствии с Вашими требованиями. Они же могут обследовать помещение на наличие подслушивающих устройств. При этом будет использоваться большое количество средств обнаружения утечки информации, а работа выполняться профессионалами.

Возможно приобретение недорогого комплекта для обнаружения утечки и защиты каналов информации.

Защита от несанкционированного доступа компьютерной информации приобретает все большую актуальность.

Появление локальных и глобальных компьютерных сетей, электронной почты, широкого обмена информацией и программными продуктами привело к возможности несанкционированного доступа к системам защиты информации банков, страховых компаний, похищению безналичных средств и коммерческих секретов.

Шифраторы факсимильной и компьютерной информации предназначены для защиты данных, передаваемых по каналам связи. При передаче информация шифруется на передающей и расшифровывается на приемной стороне. Скорость передачи зашифрованных данных, например, при использовании шифраторов фирмы AT&T, составляет от 20 кбит/сек до 2 Мбит/сек (табл. 5.2).

Наиболее распространенный способ защиты данных – использование соответствующего программного обеспечения и устройств ограничения доступа.

Пользователь может «узнаваться» по вводимому коду, по специальной карточке, по отпечаткам пальцев и др.

Обеспечение безопасности хранящейся информации используются различные программные средства. К ним относятся программные продукты обеспечивающие систему паролей, различные методы шифрования, защиту от копирования программных продуктов и распространению вирусов.

Таблица 5.2.

Шифраторы факсимильной и компьютерной информации	
Тип	*Назначение*
Шифраторы факсимильной информации	
3700F	*Приставка к факсимильному аппарату для защиты информации*
3710P	*Приставка к факсимильному аппарату для защиты информации с закрытым почтовым ящиком*
DFE-7000	*Приставка к факсимильному аппарату для защиты информации на симметричных ключах*
Шифраторы компьютерной информации	
DLE-7000	*Приставка для защиты передачи данных интерфейс RS-232 C, 19,2 кбит/с или интерфейс V35/RS530, 390 кбит/с*
DLE-7010	*Приставка для защиты передачи данных, интерфейс RS-232 C, 19,2 кбит/с*
DLE-7050	*Приставка для защиты передачи данных, E1 (CCITT G.703), 2 Мбит/с*

Широкий выбор существующих программных и аппаратных средств позволяет:
- идентифицировать пользователя;
- ограничить полномочия по доступу к устройствам и разграничить по времени работы;
- ограничить доступ к банкам данных;
- использовать систему паролей;
- вести учет работы пользователей и попыток несанкционированного доступа;
- обеспечить настройку программной среды в зависимости от прав пользователя;
- обеспечивать конфиденциальность, целостность и подлинность информации, передаваемой по каналам связи.

Как правило, факты промышленного шпионажа не обнародуются. Наиболее часто встречающиеся случаи – запись разговора, а магнитную ленту, подслушивание телефонных разговоров и радиомикрофоны.

Для несанкционированного получения коммерческой информации используются радиомикрофоны, диктофоны, контроллеры телефонных линий, малогабаритные телевизионные камеры и пр.

Например, контролируя телефонную линию можно получить полную информацию о привычках абонента, его связях, виде деятельности и распорядке дня. В случае обычного радиотелефона эта задача упрощается, так как для прослушивания линии достаточно использования обычного сканирующего приемника.

Диктофоны

Самым простым и дешевым средством прослушивания помещений и телефонных линий являются диктофоны. Они используются наиболее часто благодаря малым размерам, высокой чувствительности, наличию функции VOX и нескольких скоростей записи (обычно две).

Функция VOX автоматически включает диктофон на запись, при наличии звуковых сигналов, и отключает его спустя примерно 10 сек при их отсутствии. Таким образом, на микрокассету записывается речь без пауз. К диктофону подключается внешний чувствительный микрофон.

Обнаружить диктофон можно на расстоянии до 15 см миниатюрным детектором «TRD-800», а на расстоянии до 1 м – стационарным детектором «PTRD.014» и «PTRD.016».

Однако, существуют специальные диктофоны, которые детекторами не обнаруживаются. В этом случае используют активные средства защиты, например, генераторы шума.

Для обнаружения посетителей с передатчиками или звукозаписывающей аппаратурой предназначен портативный детектор диктофонов и микропередатчиков «TRD-800».

Он приспособлен как для автономного, так и стационарного использования и сигнализирует с помощью внутреннего бесшумного вибратора или светового индикатора о наличии нелегальных подслушивающих устройств, не привлекая внимания окружающих.

Детектор прост в обращении. Настраивается на уровень электромагнитных излучений в помещении, где будет использоваться. В случае обнаружения передающего или звукозаписывающего устройства подает сигнал.

Сканирующие приемники

Диапазон частот передатчиков радиомикрофонов находится в интервале частот от 100 кГц до 1 ГГц. Причем для частот в районе 900 МГц железобетонные стены зданий прозрачны.

Передатчики с автономным питанием имеют длительность непрерывной работы от десятков часов до нескольких месяцев. Передатчики, подключаемые к электросети или телефонной линии работают неограниченно долго. Дальность их действия составляет от 100 до 500 метров.

Для обнаружения таких передатчиков используются сканирующие универсальные приемники. Они автоматически управляются встроенным процессором или от внешней ПЭВМ.

Например, сканирующие приемники AR-3000A и AR-8000 работают в диапазоне частот от 100 кГц до 2 ГГц. Осуществляют прием сигналов всех видов модуляции с чувствительностью не хуже 1 мкВ.

Генераторы шума

Существует возможность прослушивания помещений через стены толщиной до 800 мм стетоскопом, направленными микрофонами через открытую форточку комнаты или автомобиля, лазерными устройствами со стекол и, наконец, используя проводные коммуникации помещения.

Для этих целей выпускается широкий набор специализированной техники.

Лазерные устройства для считывания со стекол длительное время могли работать только под прямым углом к стеклу на расстоянии до 500 м.

Последние разработки, использующие принцип обратного рассеивания лазерного луча, работают при отклонении от прямого угла до 30°. Однако подобные способы относятся к экзотическим и используются в основном спецслужбами.

Для нейтрализации подслушивающих акустических устройств используются генераторы шума.

Генератор «ANG-2000» – акустический генератор, создающий колебания звуковой частоты в диапазоне частот 250...5 кГц. Он предотвращает возможность прослушивания через проводные микрофоны, радиомикрофоны и стетоскопы. Блокирует лазерный съем с окон и создает помехи звукозаписывающей аппаратуре. Он оснащен вибрационными и акустическими излучателями. Количество излучателей, подключаемых к одному генератору – до 18.

Стационарный шумогенератор «Гном-3» предназначен для создания помех устройствам, передающим информацию по радиоканалу и защиты от утечки информации по каналам побочных электромагнитных излучений электронно-вычислительной аппаратуры. Он создает шумовые электромагнитные помехи в диапазоне частот от 10 кГц до 1 ГГц.

Скремблеры

Для защиты информации при передаче по телефонным линиям используется скремблирование (кодирование) и устройства, сигнализирующие о несанкционированном подключении к телефонной линии. Кодирующие устройства называются скремблерами. Они выполняются в виде телефонных приставок, телефонного аппарата, или накладной телефонной трубки.

Наиболее удобные скремблеры для речевых сообщений представляют собой телефонную трубку с автономным питанием, которая прикладывается к трубке любого телефонного аппарата. Она выполняет функции кодирования и декодирования разговора. Каждый из собеседников должен иметь такую трубку.

В скремблере устанавливается код. Не зная установленного кода невозможно подслушать разговор даже имея такой же скремблер т. к. комбинаций установки кодов – несколько десятков миллионов. Имея два скремблера на концах телефонной линии, например, «ACS2» вы надежно защитите свои речевые сообщения.

Прослушивание телефонных линий

Обычно прослушивание телефонной линии осуществляется с помощью параллельно подключенного телефонного аппарата. Более совершенные методы используют подключение к линии через согласующие устройства.

Прослушивание телефонных линий с помощью диктофона не вызывает трудностей. На пути к телефонной станции линии не защищены и доступ к ним открыт. Диктофон подключается через делитель напряжения непосредственно к телефонной линии.

В разрыв телефонной линии также могут включаться ретрансляторы. Ретранслятор представляет собой передатчик, использующий телефонный провод как антенну. На расстоянии до 500 метров можно принимать сигналы передатчика и записывать телефонные разговоры. Питается передатчик напряжением телефонной линии и имеет небольшие размеры.

Такие передатчики могут быть обнаружены по радиоизлучению в момент работы. При попытке обнаружить такой передатчик следует снять телефонную трубку, так как в большинстве моделей передатчик отключается при положенной трубке.

Совместно с передатчиками могут использоваться ретрансляторы, которые устанавливаются в безопасном месте. При этом уменьшается мощность передатчиков, что затрудняет их обнаружение.

Анализаторы телефонных линий предназначены для сигнализации подключения к линии. Они контролируют наиболее простые методы несанкционированного доступа, но не могут идентифицировать прослушивание телефонных разговоров без гальванического подключения к линии.

Недорогое и достаточно эффективное устройство «TS2», американской фирмы Personal Protection Product. Оно позволяет идентифицировать подключение к линии по падению напряжения и обнаруживать сигналы радиомикрофонов.