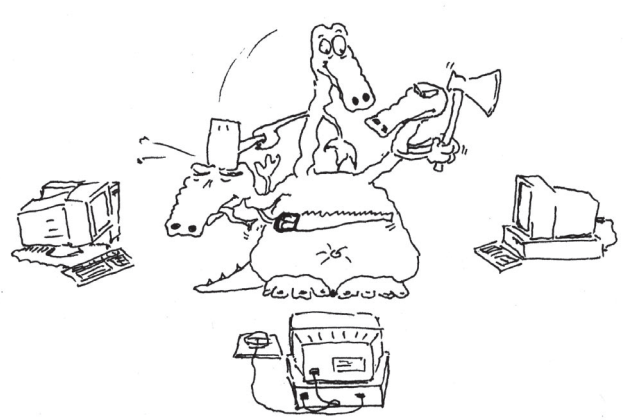
ЧАСТЬ III

Направления создания систем защиты информации



В этой части

- *Техническая защита информации на объектах ИС*
- *Защита информационных и физических объектов ИС*
- *Защита процессов и программ*
- *Технологии брандмауэров*
- *Защита каналов связи*
- *Подавление побочных электромагнитных излучений*
- *Управление системой защиты*

Техническая защита информации на объектах ИС

10

В этой главе

- *Что понимают под объектами ИС*
- *Техническая защита информации на объектах ИС*
- *Поиск каналов утечки информации*
- *Поиск радиозакладок с помощью носимых многофункциональных поисковых приборов СРМ-700 "Акула" и ST-031 "Пиранья"*
- *Общая методология поиска радиозакладок*
- *Защита речевой информации*
- *Направленное подавление радиоэлектронных устройств*
- *Организация проверки объектов ИС на наличие "жучков"*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Что понимают под объектами ИС

Предлагаем рассмотреть типы объектов ИС:

- информационные
- ресурсные (программно-аппаратные)
- физические
- пользовательские
- логические

Определение

Информационные объекты ИС – любая информация (сообщения, сведения, файлы базы данных и т.д.) в любых формах ее представления (аналоговая, цифровая, виртуальная, мысленная и др.)

В понятие *ресурсные (программно-аппаратные) объекты ИС* входят все компоненты ИС, ее аппаратное и программное обеспечение, процедуры, протоколы, управляющие структуры и т.п. (начиная с операционных систем и заканчивая выключателем сети компьютера). Отсюда следует, что понятие ресурсного объекта определяется в общем виде.

К физическим объектам ИС относятся:

территории, здания, помещения, техническое оборудование, электронные устройства, компьютерная техника, средства связи и многое другое;

Пользовательские объекты ИС – это в первую очередь люди, которые используют ресурсы ИС, имея доступ через терминалы или рабочие ЭВМ (например: пользователи информации, лица, о которых информация накапливается и обрабатывается, собственники информации, органы управления, администрация ИС).

Логические объекты ИС – это логические операции или процедуры, результатом выполнения которых является определенный вывод или признак (например: некая логическая операция формирует сообщение "Опасность" при выполнении условия совпадения ряда установленных признаков "Угроза").

Роль и место вопросов защиты объектов ИС в общей структуре системы защиты информации условно показаны на рис. 10.1.

Техническая защита информации на объектах ИС (101)

Техническая защита информации (ТЗИ) предполагает наличие методик определения угроз и утечки информации и знание средств добывания (снятия) информации, а также многое другое. В дальнейшем, для упрощения изложения, под технической защитой информации на объектах ИС будем понимать именно использование технических средств.

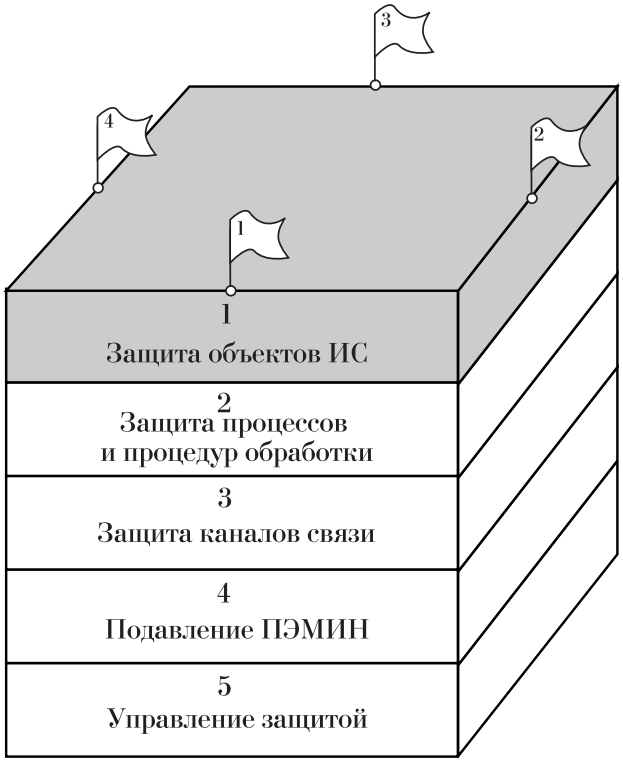


РИС. 10.1. *Защита объектов ИС в общей структуре СЗИ.*

Определение

Под *технической защитой информации на объектах ИС* обычно подразумевается совокупность организационно-технических мер, средств и правовых норм, призванных защищать объекты ИС от нанесения вреда.

Утечка информации по техническим каналам (210)

***Рассмотрим некоторые типичные каналы утечки информации*:**

- снятие информации, передаваемой по телефонным линиям, по линиям радио- и пейджинговой связи;
- снятие речевой информации с последующей передачей ее по радиоканалу ("жучки"), по проводным линиям (по сети или по пожарной сигнализации);
- снятие речевой информации через конструкции зданий (стетоскопы), с оконных проемов (лазерный микрофон или направленный микрофон);
- запись переговоров в шумных местах (направленный микрофон);
- снятие и дешифрация побочных излучений с компьютера или другой оргтехники;
- запись на диктофон переговоров. Кроме перечисленных, существуют другие варианты и методы получения информации. Классификация закладных устройств представлена на рис. 10.2.

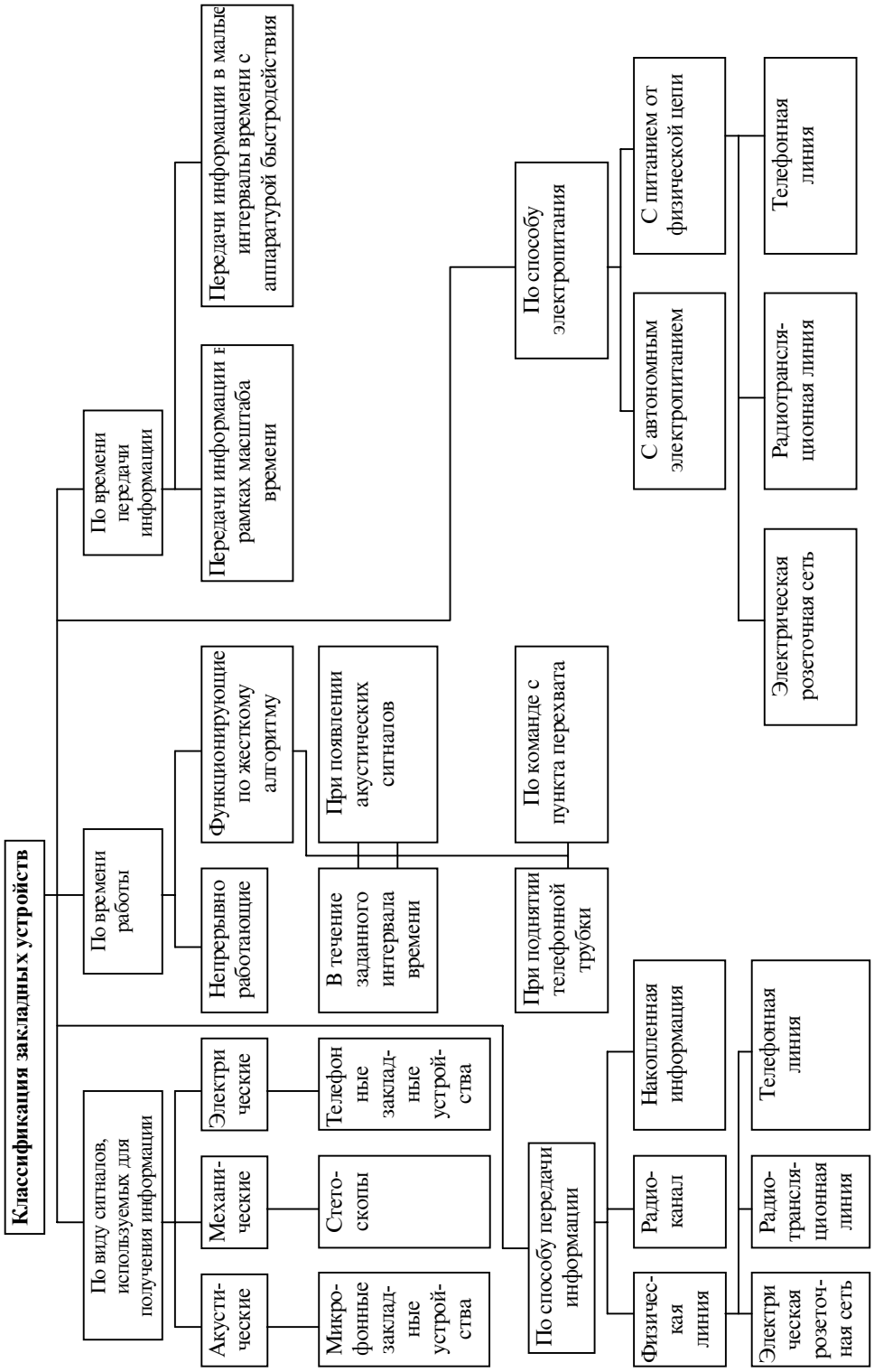


РИС. 10.2. *Классификация закладных устройств.*

Снятие информации с помощью микрофонов (214)

В том случае, если имеется постоянный доступ к объекту контроля, могут быть использованы простейшие миниатюрные микрофоны, соединительные линии которых выводят в соседние помещения для регистрации и дальнейшего прослушивания акустической информации. Такие микрофоны диаметром 2.5 мм могут улавливать нормальный человеческий голос с расстояния до 10–15 м.

Вместе с микрофоном в контролируемом помещении, как правило, скрытно устанавливают миниатюрный усилитель с компрессором для увеличения динамического диапазона акустических сигналов и обеспечения передачи акустической информации на значительные расстояния. Эти расстояния в современных изделиях достигают до 500 метров и более, то есть служба безопасности фирмы, занимающей многоэтажный офис (или злоумышленник), может прослушивать любое помещение в здании. При этом проводные линии чаще всего от нескольких помещений сводятся в одно на специальный пульт и оператору остается лишь выборочно прослушивать любое из них и, при необходимости, записывать разговоры на магнитофон или жесткий диск компьютера для сохранения и последующего прослушивания. Для одновременной регистрации акустических сигналов от нескольких помещений (от 2-х до 16-ти) существуют многоканальные регистраторы созданные на базе ПК. Такие регистраторы чаще всего используются для контроля акустической информации помещений и телефонных разговоров. Они имеют различные дополнительные функции, такие как определение входящих и исходящих номеров телефонов, ведение журналов и протоколов сеансов связи и др.

Интересно

Передача информации по специально проложенным проводам.

В качестве примера можно привести случай, когда советские власти заподозрили, что одно из посольств прослушивается. В связи с этим они направили в страну, о которой идет речь, бригаду чернорабочих, снабдив их дипломатическими паспортами. Местные власти немало позабавились, наблюдая на протяжении нескольких недель, как эти "дипломаты" в спецовках лопатами рыли вокруг здания посольства ров глубиной в несколько метров. Они искали зарытые в землю провода, которые, по их мнению, должны были идти из здания наружу (ничего обнаружено не было). Но часто подозрения подтверждались.

В доме, где проживали семьи советских дипломатов в Вашингтоне, стержни крепления металлического потолка были заменены пустотелыми трубками, содержавшими микрофоны для прослушивания разговоров.

Недостатком проводов является возможность их обнаружения и проверки назначения при визуально-техническом контроле. В более современных системах используются тончайшие (не толще волоса) оптические волокна, которые возможно вплести в ковровое покрытие, и т.д.

Разумеется, микрофон в его привычном понимании отсутствует.

Несмотря на видимую простоту, специалисты не очень любят подобные средства, поскольку по проводу можно обнаружить пункт прослушивания, со всеми вытекающими отсюда неприятными последствиями.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Микрофоны могут быть введены через вентиляционные каналы на уровень контролируемого помещения, которое может прослушиваться с другого помещения, чердака здания или с крыши в местах выхода вентиляционного колодца. При этом не обязательно, как Карлсону сидеть на крыше, достаточно установить диктофон с возможностью записи на несколько часов и имеющему возможность управления записью по уровню акустического сигнала и все разговоры в контролируемом помещении будут записываться довольно длительное время без смены кассет.

Кроме непосредственного перехвата звуковых колебаний отдельные микрофоны (т.н. микрофоны-стетоскопы) могут воспринимать звуковые колебания, распространяющиеся из контролируемого помещения по строительным конструкциям здания (стены, трубы

Снятие информации с помощью микрофонов...

отопления, двери, окна и т.п.). Их используют для прослушивания разговоров сквозь стены, окна, двери. Контрольный пункт для прослушивания разговоров с помощью микрофонов-стетоскопов может быть оборудован в безопасном месте здания на значительном удалении от контролируемого помещения.

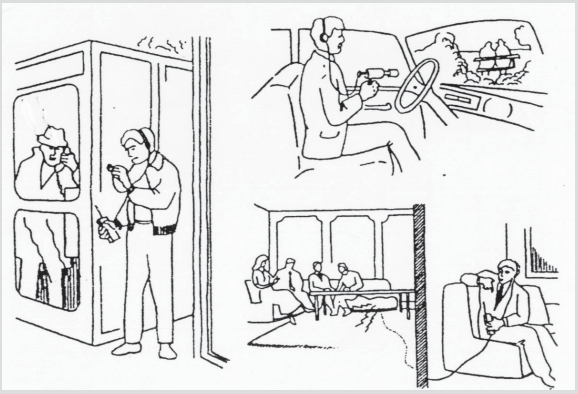
Современной промышленностью выпускаются модификации микрофонов направленного действия, которые воспринимают и усиливают звуки, идущие из одного направления и ослабляют все другие звуки. Конструкции узконаправленных микрофонов — от формы трости до микрофонов, использующих параболические концентраторы звука.

Направленные микрофоны

Обычные микрофоны динамического или электретного типа способны регистрировать голос человека с нормальной громкостью на расстоянии до 15 метров, а ночью, в тихую погоду, – 200 м.

Интересно

Для средств разведки этого мало, так как в некоторых случаях требуется дальность действия примерно в десять раз больше. Существует несколько модификаций направленных микрофонов, воспринимающих и усиливающих звуки, идущие только из одного направления, и ослабляющих все остальные звуки. В простейших из них узкая диаграмма направленности формируется за счет использования длинной трубки. В более сложных конструкциях могут использоваться несколько трубок разной длины. Высокие параметры имеют также узко направленные микрофоны, в которых диаграмма направленности создается параболическим концентратором звука.



Из западных систем подобного типа широко представлены трубчатые микрофоны, закамуфлированные под зонт "в английском стиле". В него встроен усилитель и имеется выход на наушники. Реальная дальность действия не более 30 м.

В реальных городских условиях невозможно проводить съем информации с расстояний, превышающих 100 м. Сотни метров могут быть достигнуты в исключительных случаях типа: заповедник, раннее утро, туман, над озером.

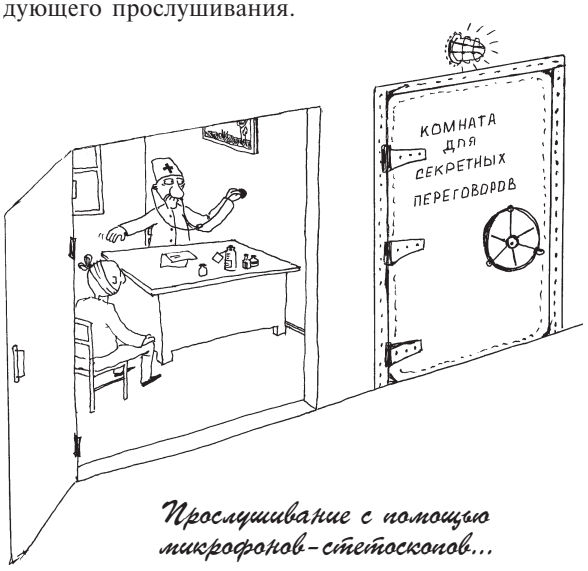
(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Диктофоны и магнитофоны (214)

Если агенты не имеют постоянного доступа к объекту, но имеется возможность его кратковременного посещения под различными предлогами, то для акустической разведки используются радиомикрофоны, миниатюрные диктофоны и магнитофоны закамуфлированные под предметы повседневного обихода: книгу, письменные приборы, пачку сигарет, авторучку. Кроме этого, диктофон может находиться у одного из лиц, присутствующих на закрытом совещании. В этом случае часто используют выносной микрофон, спрятанный под одеждой или закамуфлированный под часы, авторучку, пуговицу. Скрыто установленный в атташе-кейс малогабаритный магнитофон может незаметно включаться с помощью простой шариковой ручки.

Современные диктофоны обеспечивают непрерывную запись речевой информации от 30 минут до нескольких часов, они оснащены системами акустопуска (VOX, VAS), то есть управлением по уровню акустического сигнала, автореверса, индикации даты и времени записи, дистанционного управления. Выбор диктофонов сегодня очень большой. С описанными функциями можно подобрать модель диктофона фирм OLYMPUS, SONY, Pansonic, Uher, и др.

В некоторых моделях диктофонов в качестве носителя информации используются цифровые микрочипы и мини-диски, записанную на таком диктофоне речевую информацию можно переписывать на жесткие диски компьютеров для хранения, архивации и последующего прослушивания.



Прослушивание с помощью микрофонов-стетоскопов...

Серьезным преимуществом цифровых диктофонов является то, что они имеют малые габариты и вес, могут записывать до 20 часов речи, имеют хорошую чувствительность встроенного микрофона (до 8 м) и широкий динамический диапазон. Время непрерывной работы от одного элемента питания может составлять до 80 часов в режиме записи и до 2-х лет в дежурном режиме (счёт времени).

Из-за отсутствия движущихся частей диктофоны работоспособны в широком диапазоне температур, в условиях тряски, запылённости.

Как правило цифровые диктофоны оснащены системой голосовой активации (VAS), позволяющей эффективно сжимать паузы в сообщениях, увеличивая таким образом реальное время записи. Каждая произведенная запись маркируется временем и датой с помощью встроенных часов реального времени.

Диктофоны имеют мощную систему навигации при прослушивании ранее записанных сообщений: можно быстро переходить к следующему/предыдущему/первому/последнему сообщению, к началу/концу текущего сообщения, осуществлять перемотку вперед/назад в пределах текущего сообщения с переменной скоростью, а также стирать сообщения из памяти диктофона.

В отличие от кассетных диктофонов, цифровые хуже обнаруживают себя при работе, в отличие от кассетных, которые обнаруживаются специальными приборами типа TRD-800, PTRD-18, PTRD-19 и др. по электромагнитным излучениям, работающего двигателя лентопротяжного механизма. Цифровые диктофоны обнаруживаются с значительно меньших расстояний. В частности портативный прибор ST-041 обнаруживает цифровые диктофоны на расстоянии 20–30 см, а стационарный комплекс ST-0110 на расстоянии 50–70 см.

Снятие информации, передаваемой по телефонным линиям

Это простейший, один из самых результативных и наиболее дешевый способ. Прослушивание разговора на телефонной линии, как правило, осуществляется на отрезке “станция — абонент” или же сразу с аппарата (кроме случаев, когда этим занимаются спецслужбы, которые подключаются после АТС и технику которых в этом случае практически невозможно обнаружить).

Телефонные контролеры...

Телефонные абонентские линии обычно состоят из трех участков: магистрального (от АТС до распределительного шкафа (РШ)), распределительного (от РШ до распределительной коробки (КРТ)), абонентской проводки (от КРТ до телефонного аппарата). Последние два участка — распределительный и абонентский являются наиболее уязвимыми с точки зрения перехвата информации. Подслушивающее устройство может быть установлено в любом месте, где есть доступ к телефонным проводам, телефонному аппарату, розетке или в любом месте линии вплоть до КРТ.

Наиболее простой способ подслушивания это подключение параллельного телефонного аппарата или “монтерской” трубки. Используются также специальные адаптеры для подключения магнитофонов к телефонной линии. Адаптеры сделаны таким образом, что диктофон, установленный на запись в режиме акустопуска, включается только при поднятой трубке телефонного аппарата. Это дает возможность экономно расходовать пленку на кассете, не сматывая ее вхолостую.

Подключение к телефонным линиям осуществляется не только гальванически (прямым подсоединением), а и с помощью индукционных или емкостных датчиков. Такое подсоединение практически не обнаруживается с помощью тех аппаратных средств, которые широко используются для поисковых целей.

Самыми распространенными из подобных средств прослушивания являются телефонные контроллеры радиоретрансляторы которые чаще называются телефонными передатчиками или телефонными “закладками”.

Телефонные закладки подключаются параллельно или последовательно в любом месте телефонной линии и имеют значительный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне.

Большинство телефонных “закладок” автоматически включается при поднятии телефонной трубки и передают разговор по радиоканалу на приемник пункта перехвата, где он может быть прослушан и записан. Такие “закладки” используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть очень небольшими. Часто в качестве антенны используется телефонная линия. Для маскировки телефонные “закладки” выпускаются в виде конденсаторов, реле, фильтров и других стандартных элементов и узлов, входящих в состав телефонного аппарата.

Чаще всего телефонные “закладки” стараются устанавливать за пределами офиса или квартиры, что существенно снижает риск. Для упрощения процедуры

подключения подслушивающих устройств и уменьшения влияния на телефонную линию используются изделия с индуктивным датчиком съема информации. Особенностью подобных устройств является то, что требуется автономный источник питания и устройство должно иметь схему автоматического включения при снятии телефонной трубки. Качество перехватываемой информации практически всегда хуже.

Использование телефонных линий для дистанционного съема аудио- информации из контролируемых помещений (214)

Отдельное место занимают системы, которые предназначены не для подслушивания телефонных переговоров, а для использования телефонных линий при прослушивании контролируемых помещений, где установлены телефонные аппараты или проложены провода телефонных линий.

Примером такого устройства может служить “телефонное ухо”. “Телефонное ухо” представляет собой небольшое устройство, которое подключается параллельно к телефонной линии или розетке в любом удобном месте контролируемого помещения. Для прослушивания помещения необходимо набрать номер абонента, в помещении которого стоит “телефонное ухо”. Услышав первый гудок АТС необходимо положить трубку и через 10−15 секунд повторить набор номера. Устройство дает ложные гудки занято в течение 40−60 секунд, после чего гудки прекращаются и включается микрофон в устройстве “телефонное ухо” — начинается прослушивание помещения. В случае обычного звонка “телефонное ухо” пропускает все звонки после первого, выполняя роль обычной телефонной розетки и не мешая разговору.

Кроме того, возможно использование телефонной линии для передачи информации с микрофона, скрытно установленного в помещении. При этом используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи существенно зависит от качества линии, прокладки телефонных проводов, наличия в данной местности радиотрансляционной сети, наличия вычислительной и оргтехники и т.д.

Из числа, так называемых “беззаходовых” систем съема речевой информации с контролируемых помещений, когда используются телефонные линии, следует отметить возможность съема за счет электроакустического преобразования, возникающего в телефонных аппаратах и за счет высокочастотного (ВЧ) навязывания. Но эти каналы утечки используются все реже. Первый из-за того, что современные телефонные аппараты не имеют механических звонков и крупных металлических деталей, а второй из-за своей сложности и громоздкости аппаратуры. Но тем не менее меры защиты от утечки информации по этим каналам применяются, они общеизвестны и не дорогие.

Перехват факсимильной информации

Перехват факс-сообщений принципиально не отличается от перехвата телефонных сообщений. Задача дополняется только обработкой полученного сообщения.

Обычно комплексы перехвата и регистрации факсимильных сообщений состоят из:

- ПК с необходимыми, но вполне доступными ресурсами;
- пакет программного обеспечения;
- стандартный аудио контроллер (SoungBlaster);
- устройство подключения к линии (адаптер).

Комплексы обеспечивают автоматическое обнаружение (определение речевое или факсимильное сообщение) регистрацию факсимильных сообщений на жесткий диск с последующей возможностью автоматической демодуляции, дескремблирования зарегистрированных сообщений и вывода их на дисплей и печать.

Перехват разговоров по радиотелефонам и сотовой связи (234)

Перехват разговоров по радиотелефонам не представляет трудности. Достаточно настроить приемник (сканер) на частоту несущей радиотелефона, находящегося в зоне приема и установить соответствующий режим модуляции.

Для перехвата переговоров, ведущихся по мобильной сотовой связи необходимо использовать более сложную аппаратуру. в настоящее время существуют различные комплексы контроля сотовой системы связи стандартов AMPS, DAMPS, NAMPS, NMT-450, NMT-450i, разработанных и изготовленных в России и странах Западной Европы.

Комплексы позволяют обнаруживать и сопровождать по частоте входящие и исходящие звонки абонентов сотовой связи, определять входящие и исходящие номера телефонов абонентов, осуществлять слежение по частоте за каналом во время телефонного разговора, в том числе при переходе из соты в соту. Количество задаваемых для контроля абонентов определяется составом аппаратуры комплекса и версией программного обеспечения и может достигать до 16 и более.

Имеется возможность вести автоматическую запись переговоров на диктофон, вести на жестком диске ПК протокол записей на диктофон, осуществлять полный мониторинг всех сообщений, передаваемых по служебному каналу, а также определять радиослышимость

всех базовых станций в точке их приема с ранжировкой по уровням принимаемых от базовых станций сигналов.

Стоимость подобных комплексов в зависимости от стандарта контролируемой системы связи и объемов решаемых задач может составлять от 5 до 60 тысяч долларов.

Перехват GSM-связи следует рассмотреть отдельно. ***Цифровая сеть GSM использует два вида связи***: для связи мобильного телефона с базовой радиостанцией используется радиоэфир, другие элементы сети (например связь базовой станции с городскими АТС) соединяются с помощью проводной связи.

Данные, передаваемые по проводной части сети GSM, не шифруются. Прослушивание этой части сети можно осуществлять, как на обычных телефонных линиях.

Система радиосвязи сети GSM имеет двухуровневую защиту. Первый уровень гарантирует анонимность и аутентификацию абонента и реализуется центром аутентификации сети при вводе абонентом секретного кода. Второй уровень защиты гарантирует засекречивание данных и передач. В нем применяется шифрование информации. Алгоритмы шифрования и аутентификации сложные, но по данным зарубежной печати, не обладают абсолютной гарантией относительно невозможности расшифровки данных.

Поэтому системы перехвата переговоров сотовой GSM-связи значительно сложнее других и сейчас на рынке СНГ предлагаются только комплексы перехвата сотовой GSM-связи активного действия (комплекс подставляет себя в качестве активной базовой станции) производства Германии и Англии. Стоимость таких комплексов составляет порядка 350–650 тысяч долларов. Но по информации, поступившей с выставки “Технологии безопасности”, проходившей в Москве в феврале 1999 года, российскими разработчиками созданы комплексы перехвата сотовой GSM-связи пассивного типа и эти комплексы на порядок дешевле.

Перехват GSM-связи...

Интересно

"Ассоциация независимых разработчиков смарт-карт (Smartcard Developer Association, и двое исследователей из Университета Беркли сообщили, что им удалось клонировать сотовые телефоны стандарта GSM. Стандарт GSM (Groupe Speciale Mobile), разработанный Европейским институтом телекоммуникационных стандартов (European Telecommunications Standard institute), на сегодняшний день является самым распространенным в мире – он используется в 79 млн. сотовых аппаратов, преимущественно в странах Европы и Азии. До сих пор считалось, что телефоны GSM обладают столь надежной защитой, что их нельзя не только прослушать, но и размножить, то есть сделать несколько аппаратов, одновременно пользующихся одним и тем же номером. Один из рекламных плакатов компании Pacific Bell, например, изображает клонированную овцу и утверждает, что с телефонами GSM такого проделать нельзя.

Взлом защиты GSM еще раз показал, что единственная гарантия надежности криптографических алгоритмов — это их абсолютная открытость. Засекреченные системы (использующиеся в GSM, и не только) практически неизбежно оказываются уязвимыми. Тайное, рано или поздно становится явным.

Зашифрованные данные абонента GSM хранятся в небольшой SIM-карте, которая вставляется в телефон. Без карты, называемой также модулем идентификации пользователя (SIM — Subscriber Identification Module), аппарат представляет собой бесполезную оболочку. Карту, идентифицирующую владельца, можно использовать с любым стандартным телефоном. Обнаруженная дыра в безопасности позволяет извлечь секретную информацию из одного SIM и переписать ее в другой, создав точную копию первого телефона. Клонировать телефон, перехватывая информацию в эфире, пока еще нельзя, но SDA не исключает такой возможности в будущем.

Какие выводы можно сделать из громкого взлома еще одной защиты? Прежде всего, владельцам сотовых телефонов пока не следует особо беспокоится. Без физического доступа, по крайней мере, на несколько часов, их аппарат никто не сможет клонировать (однако гарантий на будущее никаких нет). Операторы же сотовых сетей оказываются в очень неприятной ситуации. Хотя существует несколько альтернатив COMP128, сегодня этот протокол поддерживается во всех сетях

GSM. Более того, уверенность в защите от клонирования была столь высока, что, по данным SDA, большинство операторов даже не производит проверку на одновременное включение одинаковых телефонов.

Поиск каналов утечки информации (213)

Осмотр объекта (213)

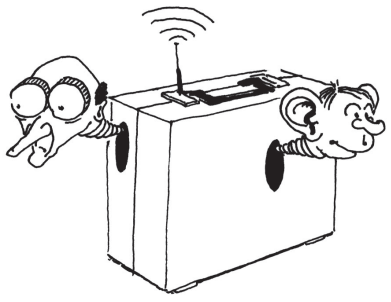
Поиск в конкретном помещении начинается с осмотра. Вначале проводится сравнение с планами, идентификация предметов мебели и интерьера. По возможности все устройства, содержащие электронику, должны быть вынесены из помещения и обследованы отдельно.

Во время осмотра основное внимание уделяется посторонним предметам. Тщательно осматриваются все полости и щели в плинтусах, полах и за батареями отопления, труднодоступные места на шкафах, карнизах и т.п. Вся мебель отодвигается, вынимаются и осматриваются ящики, внутренние полости. Вскрываются и осматриваются электророзетки и выключатели, разбирается электроустановочная арматура, просматриваются стояки и вводы коммуникаций в помещении и около него. По возможности все провода и коммуникации прослеживаются визуально. При этом необходимо строго придерживаться правил безопасности работы с электросетью — отключать электрощиты, пользоваться индикаторами сети, резиновыми перчатками и защитными ковриками.

Подготовка к поиску может осуществляться в обычное рабочее время с соответствующим прикрытием. Исследование объекта проводится без шума, никакой демаскирующей работу активности, ничего, что может насторожить ведущего прослушивание.

Контроль радиоэфира (213)

Поиск начинается с изучения оперативной обстановки вокруг объекта:



Следует знать оперативные и технические возможности по проникновению на объект с целью съема информации...

- определение вероятного расположения контрольных пунктов (КП) приема информации от спецтехники, возможно установленной на объекте;
- фиксирование подозрительных автомашин, стоящих подолгу с пассажирами, появляющихся и исчезающих вместе с владельцем проверяемого помещения, ведение конспиративного наблюдения за ним;
- организация работы пункта контроля радиоэфира (ПКР). Вначале ПКР должен быть развернут в здании объекта или рядом с ним, но не в проверяемом помещении.

Основная задача ПКР:

- составление карты занятости эфира в районе проведения мероприятия;
- выделение и исключение из дальнейшего анализа сигналов легальных (известных) радиостанций;
- статистический анализ работы подозрительных станций.

Такой радиоконтроль может продолжаться 2–7 дней, затем ПКР переносится в проверяемые помещения и принимаемые в нем сигналы сравниваются с полученной ранее статистикой.

Контроль радиоэфира или, как иначе называется — радиомониторинг и обнаружение радиомикрофонов удобнее всего осуществлять с помощью автоматизированного комплекса построенного на базе сканирующего приемника, управляемого с помощью компьютера.

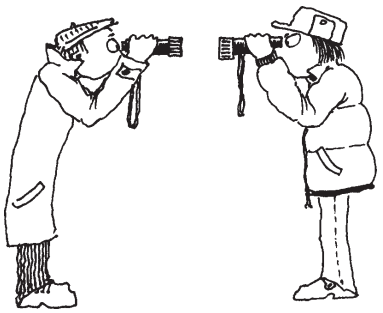
После преноса ПКР в контролируемое помещение его необходимо озвучить для активизации радиомикрофонов, имеющих режим акустопуска. Для этого включают контрольный источник звука, чаше всего это магнитофон или генератор звуковой частоты. Радиоприемник для этой цели использовать нежелательно, так как не исключены захваты сканером комбинационных частот, что напоминает по характеру наличие передающего устройства.

Если поиск осуществляется вручную с помощью сканирующего приемника, то в процессе сканирования приемник будет делать “остановки” на частотах работающих радиостанций, телевизионных программ и других источников излучений; “остановка”, при которой прослушивается контрольный сигнал, свидетельствует о наличии “закладки” (радиомикрофона) в помещении.

Совет

Указанную проверку выполнить выполнить в трех режимах:

- при полностью отключенных электроприборах, имеющихся в помещении;
- при включенных электроприборах;
- при снятых с рычагов телефонных трубках



Осмотр объекта...

В случае выявления сигнала, соответствующего созданной акустической обстановке, необходимо провести работы по индентификации и локализации источника излучений наиболее доступным путем, используя детекторы раиочастоты, частотомеры или любые другие приборы, предназначенные для этого.

При обнаружении "закладки" не следует прекращать поиски, так как не исключено, что установлены и другие.

Интересно

Можно запитать радиомикрофон и напряжением телефонной линии или от солнечных батареек как это сделано в изделии типа SIPE MT. Это ЧМ-передатчик с питанием от солнечной батареи, выполненный в виде стакана для виски. Элементы солнечной батареи расположены на дне стакана в виде оригинального орнамента. Для повышения скрытности передатчик имеет два режима: он включен если стакан стоит на столе, и отключается если его поднять и изменить положение в пространстве. Дальность действия передатчика в диапазоне 130—150 МГц составляет 100 м.

Так, в новом здании американского посольства элементы радиозакладок были "рассредоточены" по бетонным блокам, представляя собой кремневые вкрапления, арматура использовалась в качестве проводников, а пустоты — в качестве резонаторов и антенн. К счастью, подобные изделия пока по карману только спецслужбам, и коммерсантам опасаться их нет необходимости.

Классическим образцом западной технической мысли является изделие HR560 LIGHT WULD. Это передатчик, встроенный в цоколь обыкновенной лампочки накаливания с дальностью передачи до 250 м.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Контроль эфира должен продолжаться в течение всего мероприятия и еще несколько дней после его окончания. Вполне возможно, что злоумышленник расшифровал работу бригады и выключил на это время устройства съема информации, а после окончания поиска попытается возобновить работу.

Если обследуется телефонная линия, то контрольным сигналом является сигнал тональной частоты АТС (длинный или прерывистый гудок). В этом случае поиск ведется при снятой телефонной трубке.

Проверка электронной техники

Основа работы в этом случае — сравнение с эталоном. Электронные устройства вскрывают и осматривают с целью выявления изменений схемы и появления дополнительных конструкций, сделанных не на заводе.

Особое внимание следует уделять подпайкам к проводам питания. Полностью внедрить устройство съема информации в промышленное изделие можно только в заводских условиях, поэтому более быстрым, относительно простым и поэтому наиболее реальным способом внедрения является подсоединение устройства съема к цепи питания с помощью проводников.

При внимательном рассмотрении можно определить следы элементов, установленных вне заводского цикла: следы паек, изменение цвета покрытия в местах подпаек и прочие отметки вмешательства. Наличие эталона упрощает исследование, поэтому необходимо заранее узнать марки всех электронных изделий и подобрать их эталоны.

Контроль радиоизлучений электронной техники (240)

Перед разборкой электронных приборов, например современных телефонных аппаратов, их проверяют с помощью индикатора поля и частотомера на наличие излучений как во включенном (телефонные аппараты со снятой трубкой), так и в выключенном (с положенной трубкой) состоянии.

ИК-передатчики

Интересно

Для повышения скрытности, в последние годы стали использовать для передачи перехваченной микрофоном информации инфракрасный канал. В качестве передатчиков используются маломощные полупроводниковые лазеры и светодиоды. В качестве примера рассмотрим закладку TRM-1830. Дальность действия ее днем 150 м, ночью – 400 м. Ток потребления – 8 мА, время непрерывной работы – 20 часов. Габариты не превышают 26x22x20 мм. К недостаткам можно отнести необходимость прямой видимости между закладкой и приемником и влияние фоновой засветки. Все это резко ограничивает оперативные возможности подобных средств. Самое же громкое дело в США, связанное с применением оптических закладок – Уотергейт.

При наличии подозрительных излучений, регистрируемых индикатором и частотомером на расстоянии 60–80см от прибора, необходимо настроить комплекс радиоконтроля на эту частоту и, облучая проверяемый прибор акустическим сигналом, искать признаки модуляции в принимаемом радиосигнале.

В качестве облучающего сигнала лучше всего использовать генератор с резко меняющимся уровнем (типа сирены), а наблюдать принимаемый сигнал — на анализаторе спектра или осциллографе, подключенном к приемнику ПКР.

Указанный способ проверки радиосигналов дает положительный эффект даже в том случае, когда в радиомикрофоне используется необычный вид модуляции или шифрация. В этом случае акустический сигнал модуляции как бы “перегружает” передатчик, и в его радиосигнале это можно выявить.

Если “под рукой” нет анализатора спектра, можно воспользоваться и наушниками, но оценка будет менее объективной. В этой ситуации целесообразно повторить исследование обнаруженного радиосигнала без проверяемого устройства — его необходимо убрать в соседнее помещение. Такую проверку целесообразно проводить и при наличии анализирующих приборов. Если обследование проводится в большом помещении, то возможна ситуация, когда облучая акустическим сигналом один проверяемый прибор, обнаруживается канал утечки от другого устройства.

Как показывает практика, не обязательно в нем обнаруживается внедренная спецтехника. Чаще всего канал утечки информации создается в электронных устройства за счет конструктивных особенностей или даже дефектов. Проверяемые электронные устройства, в которых обнаружены паразитные каналы утечки информации необходимо из помещения удалить.

Вся электронная техника в кабинете шефа требует особо тщательной проверки...

Классификация характерных признаков радиозакладок

Наиболее полную классификацию из восьми характерных признаков радиозакладок приводит в статье "Поисковый радиомониторинг. Проблемы, методики, аппаратура" независимый эксперт В.И. Скребнев (Журнал "Системы безопасности, связь и телекоммуникации" – январь-февраль 1999 года).

Первый признак – радиозакладка, какая бы она ни была, с точки зрения поиска удобна тем, что сигнал с нее должен излучаться за пределы контролируемого помещения и, если она установлена в этом помещении, то уровень сигнала в нем всегда выше, чем за пределами. Это наиболее характерный признак радиозакладки.

Второй признак – наличие гармоник. Ослабление излучений на гармониках составляет не более 40–50 дБ. Регистрация гармоник возможна без проблем с помощью связных сканеров на расстоянии до 10 метров и ограничивается только частотным диапазоном сканера.

Третий признак – в подавляющем большинстве случаев закладка использует диапазон не занятый в данной местности радиовещательными станциями, телевизионными, системами мобильной и транкинговой связи. Появление в свободном диапазоне нового источника излучений является признаком радиозакладки.

Четвертый признак – в большинстве радиозакладок используются сосредоточенные антенные системы, что приводит к сильной локализации излучения. Этот признак хорошо использовать при поиске с помощью индикаторов поля, но затруднен при использовании связных приемников. В этом случае спад уровня сигнала

можно зарегистрировать только для гармоник (чем выше гармоника, тем лучше эффект). Использование этого признака существенно облегчается при использовании для поиска многоантенных автоматизированных систем, которые могут вести сравнение уровней сигнала поступающего от различных антенн, разнесенных на значительное (до 20 метров) расстояние.

Пятый признак – связан с пространственным распределением излучения и с поляризацией. При изменении пространственного положения или ориентации зондирующей антенны наблюдается изменение видимого уровня всех источников, причем однотипные удаленные источники одного диапазона (если осуществлять поиск с помощью спектр-анализатора) ведут себя примерно одинаково в отличие от сигнала радиозакладки.

Шестой признак – состоит в том, что уровни чувствительности применяемых в радиозакладках микрофонов достаточно велики и поэтому даже естественный уровень шумов помещения приводит к размыванию спектра радиоизлучения. Таким образом, если закладка работает без кодирования, то независимо от того используется маскирование или нет, спектр излучения всегда расширяется в соответствии с увеличением уровня звука. Это хорошо видно на спектрограмме сигнала радиозакладки, если вы издаете резкие звуки или хлопаете в ладоши в помещении, где установлена радиозакладка.

Седьмой признак – связан со способностью человека различать акустические сигналы. Так, если закладка работает без маскирования, то мы слышим шум помещения или тестовый акустический сигнал, которым мы озвучили помещение. При применении маскированного спектра сигнал напоминает неразборчивую речь или какофонию, если в качестве тестового сигнала используется музыка. При применении кодирования, слышится белый шум и никакой корреляции со звуком не наблюдается.

Восьмой признак – связан со временем работы радиозакладки. Так самые простые из них, то есть не оборудованные схемами акустопуска (VOX) или не имеющими дистанционного управления работают непрерывно в течение времени определяемом источником питания. Закладки с VOX будут работать прерывисто днем и “молчать” ночью, то есть когда нет акустических шумов. Устройства с дистанционным управлением будут иметь несколько коротких сеансов днем особенно в момент проведения важных, для установивших радиозакладку переговоров.

Таким образом, зная перечисленные характерные признаки радиозакладок можно сказать, что поиск не представляет особых трудностей. Но надо учитывать, что выделить те или иные из перечисленных или других не перечисленных признаков под силу профессионалу, имеющему необходимую для этого аппаратуру и обладающему необходимыми навыками работы с ней, а кроме того, знающему если не весь парк современных закладных устройств, то хотя-бы наиболее распространенных.

Поиск радиозакладок с помощью средств оперативного контроля (254)

Для успешного поиска необходимо прежде всего обеспечить необходимые условия для работы радиозакладки, которую вы ищете.

Для этого необходимо:

- как уже отмечалось ранее, озвучить помещение, в котором производится поиск, т.е. создать разумный естественный шум (звук), чтобы включить закладки с VOX;
- по возможности включить в сеть бытовую радиоэлектронную аппаратуру и оргтехнику;
- избежать шумов, характерных для поиска и демаскирующих процесс поиска (различные разговоры по теме, выдача зондирующих звуковых сигналов). В противном случае злоумышленник, установивший радиозакладку, если она имеет дистанционное управление может просто отключить ее.

К средствам оперативного контроля, то есть простейшим средствам обнаружения факта использования радиозакладки, а иногда и ее локализации относятся индикаторы или детекторы поля, частотомеры и некоторые поисковые приемники. Основное их преимущество – способность находить источники излучения или передающие устройства независимо от режима применения в них модуляции. Принцип поиска заключается в выявлении максимума уровня излучения в помещении.

Индикаторы поля, как правило, снабжены звуковой и световой индикацией уровня принимаемого сигнала. Многие из них имеют акустический динамик для реализации режима "акустозавязки". Хорошие индикаторы поля снабжены частотомерами.

Поиск радиозакладок может происходить в различных условиях, и различной электромагнитной обстановке. Труднее осуществлять поиск, когда уровень радиочастотного фона от расположенных вблизи радиовещательных станций, ретрансляторов или телевизионных станций очень высок, многие приборы при этом просто "зашкаливают". Для работы в такой обстановке в индикаторах поля предусмотрена возможность изменения чувствительности вручную, как например в таких приборах, как Д006, Д008, РИЧ-2 и многих других, или автоматически, как например в RD-14, в котором осуществляется вычитание фона после нажатия

соответсвующей кнопки, и далее отсчет уровня принимаемого сигнала выполняется с новых установленных значений.

Обычно поиск радиозакладок с использованием приборов оперативного контроля осуществляется следующим образом. Оператор становится на середине проверяемого помещения, то есть в месте, где предполагается отсутствие радиозакладок, включает прибор, фиксирует уровень поля в данной точке или исключает фон, затем медленно перемещаясь по помещению переносит прибор вблизи предметов мебели, электронной техники, элементов конструкции стен, потолка и т. д., фиксируя изменения уровня поля индицируемого прибором. При этом стараются проверять постоянно изменяя ориентацию антенны прибора, чтобы не пропустить закладку с определенной поляризацией антенной системы. Если находятся места, в которых уровень поля высокий, то исследуют их меняя чувствительность прибора, сокращая размеры антенны и т.д.

Демодуляция сигнала радиозакладки, как правило, происходит за счет неравномерности частотной характеристики индикатора и неизбежной небольшой амплитудной модуляции, характерной для большинства радиозакладок. При работе с индикаторами поля следует учитывать, что обнаружение большинства радиозакладок осуществляется с расстояния до 10 см. При обследовании всех возможных мест размещения закладки при расстоянии до 40-50 см., вероятность пропуска может быть значительной.

Если используется индикатор поля с частотомером (РИЧ-2, ИПФ-Ч и др.) или просто частотомер, то это дополнительная возможность убедиться, что есть радиозакладка или полученный уровень на индикаторе другого происхождения, но при этом надо учитывать, что большинство частотомеров работают при любых уровнях сигналов, но при малых уровнях нет на индикаторе фиксированного значения (цифры "бегут"), поэтому на частотомер следует обращать внимание, когда он показывает одно фиксированное значение частоты.

Хороший результат дает поиск закладок с использованием частотомера и подключенного к нему сканирующего приемника, частота настройки которого может устанавливаться командами от частотомера. Такими свойствами обладают частотомеры типа “SCOUT”, RFM-31(32) с приемниками AR8000, AR8200 и др. Частотомер выдает на приемник команду на установку фиксированного значения частоты, приемник перестраивается на эту частоту и появляется возможность прослушать полученный сигнал в наушниках подключенных к приемнику с целью идентификации принятого сигнала, сравнивая его с акустической обстановкой обследуемого помещения. Однако надо иметь в виду, что осуществлять поиск только с частотомером без индикатора поля не рекомендуется ввиду низкой чувствительности частотомеров.

Функция акустозавязки, реализованная во многих индикаторах поля связана с возникновением положительной обратной связи, которая зависит от фазовых соотношений для звуковой волны и уровней звукового сигнала. Для гарантированного возникновения завязки на расстоянии до полуметра необходимо максимально повысить уровень звука на индикаторе медленно перемещать его в пространстве, так как для завязки требуется не менее 1−2 секунды.

Если контроль помещения осуществляется регулярно, то целесообразно составить карту уровней, зафиксировав характерные уровни поля для каждой точки пространства.

Иногда индикаторы поля используют для постоянного контроля помещений. Например, если это кабинет руководителя или комната переговоров, то для постоянного контроля могут быть использованы комплексы, состоящие из нескольких датчиков уровня поля, которые размещаются в наиболее уязвимых, с точки зрения установки радиозакладок местах. Сигналы от датчиков сводятся на один блок, в котором микшируются и выдается информация о состоянии электромагнитного поля на блок индикации, который размещается на столе или, при скрытной установке, в ящике стола руководителя. Если на индикаторе фиксируется постоянный или в течение длительного времени повышенный уровень поля, это может свидетельствовать о появлении закладки. Повышение уровня на короткое время может происходить от работающего вблизи мобильного телефона, радиостанции или радиотелефона. Отключая поочередно датчики поля, можно приблизительно определить, в каком месте помещения появилась радиозакладка.

В ряде приборов оперативного контроля реализована функция быстрого прохода диапазона, на который расчитан прибор с запоминанием всех встретившихся частот радиоизлучений от радиовещательных, телевизионных станций систем радиосвязи и т.д. Пример такого прибора − "Скорпион". Весь диапазон 2 ГГц поисковый приемник радиосигналов проходит, при отсутствии сигналов, за 10 секунд. Если сюда включить время прослушивания, то на это уйдет до 6-8 минут. Предусмотрена возможность исключения из всего диапазона до 128 зарегистрированных приемником частот. Оператору для этого необходимо лишь нажать кнопку ПРОГР после прослушивания на частоте "остановки" приемника. И тогда на следующем проходе на запомненных частотах приемник не будет останавливаться. Помимо этого цифровой сканер прибора "Скорпион" функционально связан с перестраиваемым генератором прицельной помехи, который включает-

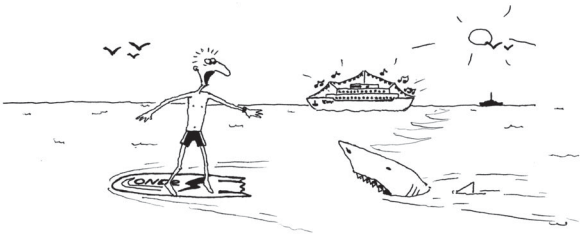
ся кнопкой РЕЖИМ на панели прибора. Мощности помехи (не менее 20 мВт) достаточно, чтобы осложнить прием не слишком мощных радиозакладок.

Поиск радиозакладок с помощью носимых многофункциональных поисковых приборов СРМ-700 "Акула" и ST-031 "Пиранья" (250)

Из носимых многофункциональных приборов, предназначенных для поиска средств несанкционированного съема и обнаружения каналов утечки информации, наиболее популярными сегодня являются такие, как СРМ-700 "Акула" и ST-031 "Пиранья". Причем оба эти прибора относительно не дороги их стоимость примерно одинакова (около 2500 долларов США), но комплектность "Пираньи" полнее. По своим возможностям в этот список следовало бы отнести и знаменитый OSCOR-5000, но его трудно назвать носимым из-за больших габаритов и веса, поэтому о нем пойдет речь в следующей статье при рассмотрении многофункциональных программно-аппаратных комплексов.

Прибор СРМ-700 "Акула" — производства фирмы Research Electronics (США) давно и широко распространен среди многих пользователей.

Предназначен для оперативного обнаружения и определения местонахождения электронных устройств съема и контроля информации. Диапазон частот 200 Гц—3 ГГц. Прост в обращении и эффективен в работе. Высокая чувствительность и автоматическая регулировка усиления, а также наличие различных входов и комплектация разнообразными датчиками — зондами превращает прибор в многофункциональное устройство. В частности при наличии дополнительных датчиков может осуществляться режим детектора инфракрасных излучений и режим виброакустического приемника.



"Акула" прост в обращении и эффективен в работе...

Предусмотрена возможность использования СРМ-700 в стационарном варианте для непрерывного контроля помещений или линий связи. Возможна запись регистрируемых сигналов на магнитофон. Имеется вход дополнительного усилителя для "прослушивания" цепей с напряжением до 52 вольт, подозрительных с точки зрения передачи звуковых сигналов. Симметричный вход позволяет тестировать телефоны и телефонные цепи на вторжение извне или отслеживать такое вторжение в режиме мониторинга и записи на внешний магнитофон.

Мнение специалистов

Надо знать

- Простота в обращении и эффективность в работе делает этот прибор действительно популярным даже среди пользователей, которые не имеют больших профессиональных знаний и опыта.
- Высокая чувствительность прибора, с одной стороны хорошо, но при этом нет эффективной возможности исключить фон и поэтому прибором очень сложно пользоваться в условиях наличия электромагнитного поля высокого уровня (если близко находятся теле или радиовещательная станция, ретранслятор и др).
- Что касается комплектации разнообразными датчиками – зондами превращающими прибор в многофункциональное устройство, то такая возможность есть, но те кто хочет прибрести себе "Акулу", должны знать, что дополнительные датчики и зонды надо покупать отдельно и стоят они не дешево.
- Серьезным недостатком СРМ-700 является отсутствие частотомера, что снижает объективность контроля. Кроме того высокочастотный детектор позволяет прослушивать сигналы только амплитудной модуляции или "паразитной" амплитудной модуляции в частотно-модулированном сигнале.
- Есть еще один серьезный эксплуатационный недостаток СРМ-700 состоит в том, что его радиочастотный зонд очень боится статического электричества, потому в инструкции записано:

"ВНИМАНИЕ: в РЧ-зонде содержится высокочувствительный усилитель, который может выйти из строя от электрического разряда через антенну. В условиях возможности появления статического электричества (сухие помещения, ковры) по возможности коснитесь исследуемого объекта сначала рукой, а только потом антенной. Не касайтесь зондом цепей с включенным питанием!"

И тем не менее многие пользователи этого прибора, несмотря на осторожность при обращении с прибором, вынуждены часто обращаться к специалистам с просьбой отремонтировать ВЧ-зонд после очередного "пробоя".

"Пиранья"

ST-031 "Пиранья" — многофункциональный прибор нового поколения производства российской компании "СмерШ Техникс" (г. Санкт-Петербург), появился на рынке поисковой техники сравнительно недавно, но сразу завоевал уважение среди специалистов. Многие ставят его по своим функциональным возможностям между СРМ-700 и знаменитым, но дорогим комплек-

сом OSCOR-5000, той же упомянутой фирмы Research Electronics (США).

Конструкция, комплектность, характеристики и возможности ST-031 "Пиранья" позволяют, в сочетании с общим радиомониторингом, физическим поиском и визуальным осмотром, реализовать фактически полную методику выявления специальных технических средств.

В ST-031, в отличие от CPM-700, появились новые возможности и режимы.

Режим высокочастотного детектора, в котором обеспечивается прием радиосигналов в диапазоне от 30 до 2500 МГц, их детектирование и вывод для слухового контроля в виде чередующихся тональных посылок (щелчков), либо в виде фонограмм при их прослушивании как на встроенный громкоговоритель, так и на головные телефоны. В каждый конкретный момент времени на фоне реальной помеховой обстановки принимается и детектируется наиболее мощный из всех радиосигналов в рабочем диапазоне. Его уровень относительно установленного порога детектора, отображается на ЖКИ, одновременно, в отличие от CPM-700, осуществляется измерение текущих значений частоты принимаемого сигнала и определение ее наиболее устойчивого значения с индикацией на экране дисплея.

Режим сканирующего анализатора проводных линий, в котором обеспечивается прием и отображение параметров сигналов в проводных линиях различного назначения (электрической сети, телефонной, пожарной и охранной сигнализации и т.д.), в таком виде в приборе CPM-700 отсутствует. В ST-031 прием сигналов осуществляется путем автоматического или ручного сканирования в диапазоне частот до 15 МГц. Спектрограмма принятого сигнала выводится на дисплей и может быть прослушана оператором. "Прослушивание" проводных линий может осуществляться с использованием дифференциального анализатора проводных линий ДАПЛ-031, которым прибор, к сожалению пока не комплектуется, а приобретается дополнительно.

Режим детектора низкочастотных магнитных полей, в котором осуществляется прием на внешнюю магнитную антенну и отображение сигналов от источников низкочастотных магнитных полей с преобладающей магнитной составляющей поля в диапазоне частот от 300 до 5000 Гц.

Режим акустического приемника обеспечивает прием на внешний выносной микрофон и отображение параметров акустических сигналов в диапазоне от 300 до 6000 Гц. Используется при оценке состояния звукоизоляции помещения.

Дополнительные возможности – использование встроенного спектроанализатора, встроенного осциллографа для анализа сигналов и запись в энергонезависимую память.

Благодаря появлению в приборе ST-031 этих новых режимов и дополнительных возможностей по сравнению с CPM-700, особенно встроенного частотомера, осциллографа и спектроанализатора, этот прибор пользуется все большей популярностью у профессионалов – поисковиков.

К концу 2000 года, появилась новая модель "Пираньи" – ST-031P, которая дополнена следующими возможностями:

- управление сканирующим приемником (типа AR8000, AR8200 и т. п.);
- работа с IBM PC совместимым компьютером (создание базы данных графической и звуковой информации).

Как отмечалось выше, многофункциональные приборы CPM-700 "Акула" и ST-031 "Пиранья" обладают большими возможностями, в частности они позволяют осуществлять поиск:

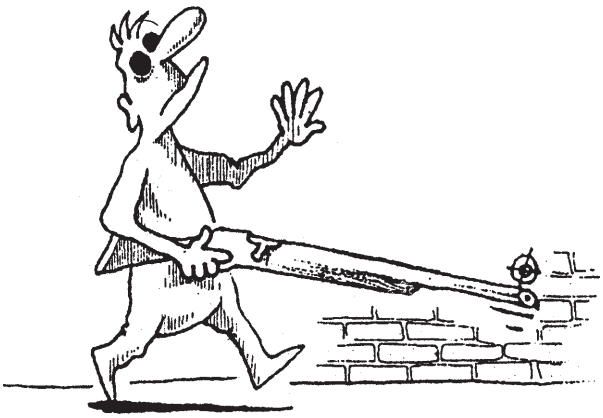
- высокочастотных передатчиков аудио и видео сигналов;
- телефонных "жучков";
- проводных микрофонов;
- инфракрасных передатчиков;
- эвукозаписывающих устройств;
- проводить анализ виброакустических утечек.

Общая методология поиска радиозакладок (250)

Общая методология поиска радиозакладок с помощью многофункциональных поисковых приборов не намного отличается от поиска средствами оперативного контроля.

Для обеспечения скрытности проводимых работ в контролируемом помещении не должны находиться посторонние люди. Следует закрыть двери и окна, а также шторы или жалюзи. Обычно для выявления радиоизлучающих средств несанкционированного съема информации проводят проверку в условиях максимальной активизации всех технических средств, находящихся в контролируемом помещении. При этом принимаются меры активизации разведки противника, предусмотренные легендой: озвучивают помещение воспроизведением "деловых переговоров", снятия телефонных трубок для перевода в режим занято, включения всех источников света, бытовой и оргтехники.

Некоторые специалисты, напротив, для уменьшения фона электрического поля выключают оргтехнику, сетевые адаптеры, трансформаторы, базовые станции беспроводных телефонов, люминесцентные



Общая методология поиска...

осветительные лампы (используют для освещения лампы накаливания) и другие электронные устройства и электроприборы — потенциальные источники повышения фона. Проверку этих устройств, проводят отдельно, включая их поочередно.

Если проверяемое помещение или смежные оборудованы системами активной радиотехнической маскировки (радиочастотные генераторы шума и т.п.), их необходимо выключить на время проведения проверки. Следует отключить радиотелефоны и другие радиопередающие средства. Не допускается совместная работа приборов СРМ-700 и ST 031 с нелинейными локаторами.

Для активации радиозакладок с акустопуском и обеспечения классификации обнаруживаемых радиосигналов, в контролируемом помещении и включают идентификационный источник звука, в качестве которого можно использовать магнитофон или CD-плеер в режиме воспроизведения музыки или речевой фонограммы. Не рекомендуется использовать в этих целях радиоприемник или телевизор, так как звуковой сигнал, создаваемый ими может коррелировать с соответствующим радиосигналом, на котором ведется данная передача, принятым поисковым прибором.

Подготовка и настройка приборов для работы в режиме высокочастотного детектора (214)

Подготовка прибора заключается в том, что, несмотря на то, что СРМ-700 построен на современной элементной базе, дополненной температурной компенсацией параметров схемы, что обеспечивает стабильную и точную работу прибора, из-за большого коэффициента усиления иногда требуется подстройка параметров, обусловленная старением элементов, изменений температуры и влажности среды. Калибровка выполняется подключением ОНЧ-зонда к зондовому входу и настройки блока калибровки на боковой стороне прибора так, чтобы показания дисплея составляли от 2 до трех сегментов при усилении high.

Подготовка прибора ST-031 "Пиранья заключается в установке "нулевого" порога детектора, а это происходит автоматически по включению питания прибора.

Подготовку приборов следует производить в одном из ближайших к проверяемому помещений, в котором, предположительно, уровень фона существенно не отличается, а установка "радиозакладок" либо невозможна, либо нецелесообразна. В качестве таких помещений обычно рассматривают помещения другого предназначения, но расположенные на том же этаже и с оконными проемами, выходящими на ту же сторону здания.

После калибровки СРМ-700 или установки "нулевого" порога ST-031, прибор перемещают в контролируемое помещение (к контролируемому объекту) БЕЗ ВЫКЛЮЧЕНИЯ ПИТАНИЯ. Ибо каждое последующее его включение приводит к автоматической установке порога уже применительно к новым условиям электромагнитной обстановки.

При работе с приборами СРМ-700 и ST 031 используют раздельно или в сочетании два основных метода поиска и локализации источников опасных радиосигналов. Ими являются так называемые "Амплитудный метод" и метод "Акустической завязки".

"Амплитудный метод" основан на резком возрастании уровня принимаемого сигнала при приближении приемной антенны прибора к месту расположения его источника. Радиус зоны обнаружения источника зависит от мощности излучаемого им сигнала, направленности его антенны и уровня фона электрического поля в точке расположения приемной антенны прибора. Контроль за уровнем принимаемого сигнала осуществляется по показаниям индикаторов уровня на экране дисплея, а для прибора ST-031 и по частоте щелчков звуковой сигнализации в режиме "TONE".

Метод **"Акустической завязки"** основан на возникновении положительной акустической обратной связи между микрофоном "радиозакладки" и динамиком прибора, в результате чего возникает "писк" тон и интенсивность которого изменяются при приближении динамика прибора к микрофону "радиозакладки". Эффект "акустической завязки" возникает только в отношении "радиозакладки", в которой применены обычные виды модуляции — амплитудная и частотная (узкополосная или широкополосная). Причем в случае частотной модуляции эффект основан на наличии "паразитной" амплитудной модуляции в частотно-модулированном сигнале.

При этом следует учитывать, что наличие характерного звука при использовании данного метода демас-

кирует проведение работ. Поэтому в случае применения "радиозакладок" с дистанционным управлением они могут быть выключены "противником" на время проверки.

И еще необходимо помнить, что эффект "акустозавязки" и отчетливое прослушивание демодулированного сигнала наблюдаются не всегда. Например, если закладки имеют маскированный радиоканал.

Поиск осуществляется путем планомерного обхода помещения (объекта) с движением вдоль стен и обследованием мебели и других расположенных в нем предметов. При обходе антенну необходимо ориентировать в разных плоскостях, совершая плавные, медленные повороты основного блока и добиваясь максимального уровня сигнала. Антенну прибора целесообразно держать на расстоянии не более 20–25 см от обследуемых поверхностей и предметов. При отсутствии ограничений на использование метода "акустозавязки" динамик встроенного громкоговорителя прибора следует ориентировать в сторону обследуемых поверхностей и предметов.

При приближении антенны прибора к месту размещения "радиозакладки" напряженность электромагнитного поля возрастает, соответственно повышается и уровень сигнала на его входе. С превышением уровнем сигнала установленного "нулевого" порога, в зависимости от вида сигнала, увеличивается количество окрашенных секторов индикаторов уровня. При работе с ST-031 возрастает частота щелчков звуковой сигнализации в режиме "TONE", а при включении режима "AUD" и динамика громкоговорителя возникает "акустозавязка". В случае нахождения источника с частотномодулированным сигналом будет увеличиваться количество окрашенных секторов верхнего индикатора уровня сигнала. При достаточном приближении к источнику радиочастотомер осуществляет "захват" частоты и показывает в последней строке экрана ее значение по результатам нескольких измерений. Путем уменьшения громкости, изменения границ динамического диапазона, увеличения вручную порога срабатывания детектора, наблюдения за показаниями частотомера сужается зона обследования и, тем самым, локализуется место установки "радиозакладки".

Особенности поиска радиомикрофонов (210)

Радиомикрофоны с кварцевой стабилизацией частоты и узкополосной частотной модуляцией. Основные их особенности заключаются в небольших пределах изменения несущей частоты (до десятка килогерц) и слабом звуковом сигнале на выходе амплитудного детектора приемника прибора. Последнее определяет значительно меньшие размеры зоны возникновения "акустозавязки". Поэтому для поиска и локализации такого типа источников наиболее целесообразно использование амплитудного метода.

Радиомикрофоны с вынесенным передатчиком. Их основная особенность — разнос мест установки микрофона и собственно радиопередатчика (вплоть до выноса в другое помещение). В этом случае необходимо сочетание метода "акустозавязки" и амплитудного метода. Причем для локализации микрофона необходимо использовать метод "акустозавязки", а радиопередатчика (в проверяемом помещении или за его пределами) — амплитудный метод.

Радиомикрофоны с закрытым или маскированным радиоканалом. Их основная особенность в том, что принятый и демодулированный сигнал не несет в себе информации об акустическом фоне помещения. Это определяется использованием для закрытия (маскирования) радиоканала методов инверсии спектра, цифровых методов передачи и сложных видов модуляции. Следовательно, в основе их обнаружения и локализации должен лежать амплитудный метод, а при работе с "Пираньей" с дополнением его анализом осциллограмм и спектрограмм в режимах "OSC" и "SA", соответственно. Дополняющим здесь может быть простой прием. Если выключить источник тестовой фонограммы и создать в проверяемом помещении короткий резкий звук (сильный хлопок, удар по крышке стола или металлическому предмету), то можно зафиксировать характерные изменения демодулированного сигнала "на слух" в режиме "AUD", изменения осциллограммы в режиме "OSC" и спектрограммы в режиме "SA".

Поиск камуфлированных радиомикрофонов, питающихся от электросети, и локализация места их установки осуществляется теми же методами, которые были охарактеризованы выше. Поочередно включить имеющиеся осветительные приборы с лампами накаливания и подключить к розеткам электросети шнуры питания санкционированных потребителей. Последовательно провести обследование каждого из вновь подключенных средств.

Поиск телефонных радиоретрансляторов (210)

Телефонные радиоретрансляторы, по способу подключения к элементам телефонной линии – могут быть с гальваническим контактом и без него. При этом гальваническое подключение может осуществляться как последовательно, так и параллельно.

Телефонные радиоретрансляторы последовательного включения характеризуются появлением в эфире модулированного сигнала только при поднятой трубке телефонного аппарата. Локализацию телефонных ретрансляторов данного типа наиболее целесообразно осуществлять амплитудным методом.

Это обусловлено тем, что телефонные аппараты, используемые в настоящее время, имеют достаточно чувствительные микрофоны и, часто, режим громкоговорящей связи. Применение метода "акустозавязки" может привести к ложным выводам о наличии установленного телефонного радиоретранслятора.

Телефонные радиоретрансляторы параллельного включения могут иметь две разновидности.

Первая из них предусматривает реализацию только функции ретранслятора. При этом в режиме поднятой трубки на радиочастоте прослушиваются сигналы АТС ("вызов", "занято"), щелчки набора номера и разговор абонентов. При положенной трубке модуляция радиосигнала отсутствует, может отсутствовать и сама несущая частота. Для локализации закладок такого типа предпочтителен амплитудный метод с их активизацией путём поднятия трубки телефонного аппарата.

Во второй разновидности часто совмещают функции телефонного радиоретранслятора и радиомикрофона, питающегося от телефонной линии и обеспечивающего контроль акустики помещения в режиме положенной трубки. Такие закладки устанавливаются на элементах телефонной линии в пределах интересующего помещения. Для их локализации при положенной трубке используется метод "акустозавязки" с применением тестового звукового сигнала. В режиме поднятой трубки для локализации таких закладок предпочтителен амплитудный метод.

Телефонные радиоретрансляторы не гальванического включения (индуктивного съёма информации) могут быть установлены на любом участке телефонной линии, как правило, вне интересующего помещения на абонентской проводке без нарушения изоляции. Они формируют модулированный радиосигнал только при поднятии трубки телефонного аппарата. При этом прослушиваются сигналы АТС ("вызов", "занято"), щелчки набора номера, разговор абонентов после установления соединения. Их локализация осуществляется амплитудным методом по мере обследования телефонной линии на всём её доступном протяжении.

При поиске телефонных радиоретрансляторов для их активизации необходимо снять трубки всех телефонных аппаратов. Собственно поиск проводится в два этапа.

Сначала на наличие закладных устройств проверяются сами телефонные аппараты. Установленный в аппарате радиоретранслятор проявляется точно так же как и радиомикрофон. При приближении антенны прибора к такому телефонному аппарату реагируют средства звуковой (в режиме "TONE") индикации, индикатор уровня сигнала и частотомер. При переключении в режим "AUD" в динамике или в головных телефонах прослушивается либо непрерывный, либо прерывистый тональный сигнал телефонной станции. В ряде случаев при приближении микрофона телефонной трубки к динамику поискового прибора может возникнуть эффект "акустозавязки". Не рекомендуется проверять телефонные аппараты в режиме громкоговорящей связи (если он предусмотрен), так как в этом случае может возникнуть ложная "акустозавязка" между микрофоном и динамиком самого аппарата.

Далее поиск телефонных радиоретрансляторов осуществляется путем обхода помещения вдоль абонентской телефонной линии и выявления на ней мест с возрастанием (максимумом) уровня радиосигнала. При обходе антенну прибора необходимо ориентировать в разных плоскостях на минимально возможном расстоянии от линии. Практически всегда существует необходимость проверки линии вплоть до основного распределительного щита. Особое внимание следует обращать на распределительные коробки и места, где линия проложена скрытой проводкой. Установленные на линии телефонные радиоретрансляторы локализуются, в основном, амплитудным методом.

Особенности поиска радиостетоскопов, видеопередатчиков и радиозакладок в ПК (210)

Основная особенность радиостетоскопов состоит в том, что они устанавливаются только с внешней стороны поверхностей, ограждающих контролируемое помещение, или на выходящих за его пределы трубах систем отопления, водопровода и других коммуникациях. Для обнаружения их сигналов можно использовать режим анализа и классификации "на слух", а для локализации источников радиоизлучения — амплитудный метод с перемещением прибора в смежные, выше и ниже расположенные помещения. Поскольку средой распространения виброакустических колебаний могут являться трубы отопления и водоснабжения, то проверке подлежат и эти коммуникации.

Скрытые видеокамеры с радиоканалом передачи информации отличаются тем, что сигнал, излучаемый в радиодиапазоне, по структуре схож с сигналом канала яркости передатчиков телевизионного вещания. При обнаружении такого сигнала первой является задача его распознавания по критерию "внешний-внутренний". Для распознавания необходимо закрыть окна шторами или жалюзи, оставив включенным внутреннее освещение. Произвести несколько раз включение и выключение искусственного освещения. При включенном режиме "AUD" должны прослушиваться отчетливые изменения тона продетектированного сигнала. Для повышения надежности распознавания включить режим "OSC" и убедиться в изменении структуры сигнала по осциллограмме при включении и выключении освещения.

Принципиально передатчики видеокамер могут работать на частотах до 2300МГц. Обнаружение сигнала (похожего на сигнал яркости) на частотах вне диапазона телевизионного вещания практически однозначно свидетельствует о работе передатчика скрытой видеокамеры. Локализация таких средств осуществляется амплитудным методом.

Радиозакладки в ПК предназначены для передачи изображения монитора и цифровых сигналов системного блока и других элементов физической архитектуры компьютера. Основная их особенность заключается в том, что сигнал, передающий изображение монитора, по структуре похож на сигнал передатчика скрытой видеокамеры, а в других случаях содержит все признаки цифровой передачи. Основой для их обнаружения и локализации служит амплитудный метод, дополняемый анализом изображений в режимах "OSC" и "SA" при работе с ST-031.

Поиск радиозакладок с помощью программно-аппаратных комплексов (740)

Использование компьютера существенно расширяет возможности поисковой аппаратуры. Это связано с тем, что появляется возможность хранения, вызова неограниченного объема снятой с эфира и накопленной информации, визуального представления снятой спектрограммы и ее анализа по уровням сигналов, наличием гармоник, частотных, фазовых и амплитудных характеристик сигналов, полученных при сканировании приемника, ширины полосы и т.д.

Широкие сервисные возможности программных оболочек большинства комплексов в решении задач по накоплению и анализу информации о принимаемых радиосигналах позволяют с успехом их применять для выявления излучений технических средств негласного получения информации и их локализации. В большинстве комплексов хорошо проработаны процедуры выполнения акустических тестов, графика для локализации источников излучения.

Поиск радиозакладок с помощью программно-аппаратных комплексов...

Программы дают возможность проводить поиск не только средств, передающих перехваченную информацию по эфиру, (радиомикрофонов, телефонных ретрансляторов, устройств видеонаблюдения, устройств несанкционированной передачи компьютерной информации по радиоканалу и т.п.), но и закладок, передающих информацию по проводным линиям, как низковольтным, так и по сети 220В.

Общие принципы (240)

Общая методика выявления таких устройств заключается в использовании сканирующего приемника, управляемого программной оболочкой, одной или нескольких антенн, позволяющих изменять условия приема радиосигналов и сравнении спектрограмм сигналов, снятых в различных условиях приема. В автоматизированных комплексах используются сканирующие приемники, имеющие возможность управления с ПК. Чаще всего применяются такие, как AR8000, AR8200, AR3000A, AR5000 (фирмы AOR − Япония) , IC-R10, IC-R7100, IC-R8500, IC-R9000, IC-PC R1000 (фирмы ICOM − Япония) и др.

Для выявления радиозакладок различные программные оболочки используют различные принципы. Но общим является тот, что в контролируемом помещении, для активизации радиомикрофонов снабженных режимом VOX вклю чается источник звука и проводится съем группового спектра шумов и сигналов, оцениваются амплитудно-частотные характеристики отдельных сигналов, проводится их классификация и идентификация с сигналами известных источников электромагнитных излучений.

Особое внимание при этом обращается на участки диапазона, типичные для применения в них современных радиомикрофонов и других закладных устройств, использующих для передачи информации радиоканал (специалисты, которые профессионально занимаются поисковыми мероприятиями, знают эти диапазоны радиочастот и постоянно отслеживают их изменения).

Последующий анализ снятых спектрограмм может осуществляться следующими общепринятыми методами.

Сравнение текущих или запомненных спектров сигналов с типовыми спектрограммами радиозакладок различных типов, если создана библиотека образов таковых спектрограмм и она находится в памяти компьютера.

Навязывание предполагаемой радиозакладке тестового звукового сигнала, анализа на текущей спектрограмме изменений исследуемого сигнала и установления корреляции между акустическим сигналом и изменениями радиосигнала. В процессе анализа проводится прослушивание принятого сигнала через наушники, подключенные к выходу сканирующего приемника или, если предусмотрено программой – запись полученного сигнала для последующего прослушивания и анализа.

Проведение так называемой пространственной селекции сигналов, полученных от нескольких, удаленных на значительное расстояние антенн (не менее 20 метров) и вынесенных в различные помещения. Иногда одну из антенн устанавливают снаружи (на крыше здания). При этом сравниваются уровни сигналов, принятых на одной и той же частоте различными антеннами. Сигналы радиовещательных или телевизионных станций будут иметь примерно одинаковый уровень на входах от всех антенн. Сигнал же от радиозакладки имеет незначительную мощность и уровень сигнала принятого на антенну размещенную в контролируемом помещении будет значительно выше, что позволяет эту частоту отнести к разряду "опасной" с тем чтобы подвергнуть дальнейшей идентификации методом акустической корреляции, исследованию гармоник и т.д.

Последующее уточнение месторасположения радиозакладки может осуществляться в режиме "локализация". Этот режим основан на выдаче звуковых тестовых сигналов от разных акустических колонок, расположенных в помещении и измерении времени распространения звука от источника до радиозакладки. Координаты радиозакладки отмечаются на плане помещения, выведенном на экран ПК, точкой пересечения двух окружностей с радиусами, равными расстояниям до закладки от двух точек расположения излучателей акустического сигнала или, если программа и звуковая карта ПК предусматривает выдачу координат в трех плоскостях, то используется 4 акустических колонки. Точность измерения таким методом не превышает 5–10 см.

Уточнение местоположения радиозакладки может быть проведено также по максимальной амплитуде радиосигнала при перемещении выносной антенны радиоприемника по контролируемому помещению.

Следует особо подчеркнуть высокую эффективность применения программно-аппаратных комплексов для обнаружения радиозакладок с инверсией спектра и другими способами закрытия канала передачи информации, ибо поиск таких закладных устройств техническими комплексами с использованием тестовых акустических сигналов не всегда дает положительные результаты. Последние разработки таких комплексов, как "АКОР-1" (Украина), "Крона-6000" (Россия), АРК-Д1 (Россия) позволяют идентифицировать закладные устройства, использующие режим дельта-модуляции и даже ШПС.

Программно-аппаратные комплексы позволяют осуществлять еще одну серьезную функцию в плане обеспечения технической защиты информации. Если обнаружена радиозакладка, но ее изъятие по каким-то причинам невозможно, то есть возможность программно управлять генераторами прицельной помехи, позволяющей на необходимое время нейтрализовать установленную радиозакладку.

Программно-аппаратный комплекс АКОР-1 (244)

Более подробно возможности автоматизированных комплексов рассмотрим на примере комплекса АКОР-1 который позволяет осуществлять:

- проверки помещения, электросети, телефонных линий и других коммуникаций на наличие устройств негласного съема речевой информации;
- контроль рабочего места руководителя, отдельных кабинетов или всего офиса от появления устройств съема, использующих дистанционное включение или кратковременную работу, а также вносимых на время проведения совещания, переговоров и др. закрытых мероприятий;
- выявлять каналы утечки информации от средств оргтехники, связи и другой аппаратуры по электромагнитному полю.

Благодаря внедрению оптимальных методов обнаружения и анализа сигналов (быстрое свиппирование по диапазону, пространственная селекция сигналов, корреляционная обработка по тест-сигналу или звуковому фону, анализ сигналов на гармоники, звуковое зондирование, ведение по контролируемым объектам архивов данных по сигналам) *комплекс обеспечивает*:

- гарантированное обнаружение любых средств съема информации, использующих в т.ч. закрытые виды модуляции (инверсия спектра, дельта модуляция, шумоподобный сигнал, цифровая передача) и скачкообразное изменение частоты;
- автоматическую работу без ее демаскирования и без ложных срабатываний на посторонние сигналы;
- подключение генератора автоматического подавления устройств съема информации.

Комплекс позволяет осуществлять в автоматическом режиме или по команде оператора следующие функции:

- обнаружение и регистрацию на контролируемом (проверяемом) объекте вновь появляющихся источников радиоизлучения (ИРИ);

- идентификацию обнаруженных и зарегистрированных ИРИ на принадлежность к устройствам негласного съема речевой информации (радиомикрофонов, радиостетоскопов, сетевых и телефонных передатчиков и т.п.), использующих различные в т.ч. закрытые виды модуляции;
- локализацию (определение местоположения) ИРИ в трехмерном пространстве;
- адаптацию комплекса к радиоэфиру и помеховой обстановке в районе расположения контролируемого объекта с возможностью обнаружения вновь появляющихся сигналов;
- ввод сетки "запрещенных" частот с возможностью их редактирования;
- визуальный просмотр в окнах анализа осциллограмм и спектра сигналов после их квадратурной обработки, а также их изменений амплитуды и фазы;
- прослушивание интересующих сигналов с возможностью выбора типа демодулятора и полосы пропускания приемника;
- просмотр в различных ракурсах и масштабе схемы контролируемого помещения с установленными в нем акустическими датчиками и определение в трехмерном пространстве координат обнаруженных ИРИ;
- локализацию на обнаруженной "опасной частоте" ИРИ при помощи цифрового индикатора поля, аппаратно-программно реализованного в комплексе;
- возможность цифровой записи интересующих сигналов с последующим анализом их радиотехнических характеристик и аудиоконтроля;
- автоматическое подавление "опасных сигналов" при помощи специального генератора, поставляемого по желанию клиента в составе комплекса;
- поиск и локализацию возможных каналов утечки речевой информации по электромагнитному полю, возникающих за счет акустического воздействия на аппаратуру связи, оргтехнику и другие устройства, установленные в контролируемом помещении.

При использовании АКОР-1 для автоматического контроля одновременно нескольких помещений в его состав дополнительно включают блоки ВЧ- и НЧ-коммутаторов, антенн с ВЧ-усилителями и соединительными кабелями, звуковыми колонками с соответствующей разводкой.

Для выявления сигналов со скачкообразным изменением частоты используется дополнительная программа, ведущая предисторию всех подозрительных, отсортированных методом пространственной селекции сигналов.

Обнаружение сигналов (244)

В комплексе реализовано два вида обнаружителей:

- обнаружение всех сигналов принимаемых антенной;
- обнаружение сигналов, появляющихся только в контролируемом помещении.

В первом случае прием сигналов осуществляется на одну антенну. Во втором случае на две или более антенны — рабочие и опорную. При этом используется метод пространственной селекции.

Обнаружитель осуществляет автоматический прием сигналов через широкополосную антенну на сканирующий приемник, обеспечивающий двойное преобразование частоты в полосе пропускания по второй промежуточной частоте (ПЧ) равной 10,7 МГц и переключение в контролируемом диапазоне частот с шагом 3–4 МГц. С выхода 2-ой ПЧ сигналы в полосе пропускания 4 МГц поступают на вход БПО, который производит третье преобразование частот, быстрое свиппирование в полосе 4 МГц с шагом 20 КГц и квадратурную обработку сигналов. Затем сигналы с двух квадратур БПО подаются через двухканальный линейный вход на звуковую плату SB, установленную в ПК, с помощью которой производится оцифровка сигнала. Оцифрованные сигналы, обработанные при помощи специальных алгоритмов, выводятся на экран монитора в виде Общей и Детальной панорам. Панорама изображается в виде зависимости амплитуды сигнала от его частоты в условных единицах SB (рис. 10.3).

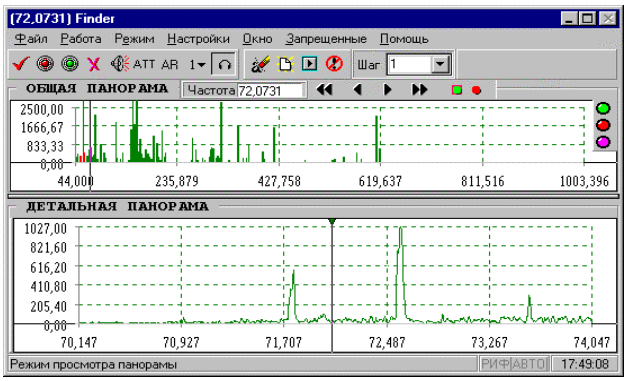


РИС. 10.3. *Главное окно программы*

Возможен вывод протокола с указанием ОПАСНЫХ ЧАСТОТ или отдельных Списков частот всех сигналов, превышающих порог или только вновь обнаруженных сигналов. Максимальное количество контролируемых частотных каналов в диапазоне 1000 МГц составляет 50000 за время не превышающее 30 секунд (рис. 10.4).

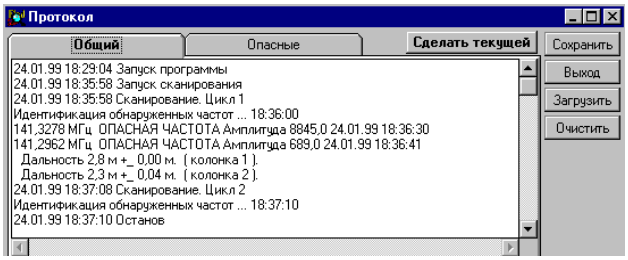


РИС. 10.4. *Окно Протокол/Общий*

Идентификация сигналов

Идентификация осуществляется после обнаружения сигналов, превышающих порог обнаружения в автоматическом режиме или оператором.

После первого прохода Общей панорамы идентификация сигналов происходит на всех частотах, не попавших в заранее задаваемый (при необходимости) Список запрещенных частот. На втором проходе контролируемого диапазона идентифицируются только вновь появившиеся сигналы и т.д. Таким образом с каждым циклом обзора происходит автоматическая адаптация комплекса к помеховой и сигнальной обстановке. Это позволяет процесс выявления включаемого во время работы комплекса ИРИ свести практически до нескольких секунд.

Идентификация происходит путем настройки комплекса на частоту сигнала при помощи специального синтезированного на звуковой карте акустического тестового сигнала, который поступает на одну из активных колонок, выбранную заранее оператором. В комплексе реализован универсальный очень чувствительный алгоритм (универсальный коррелятор), который позволяет выявлять корреляцию между акустическим тестом и модулируемой функцией практически любого из используемых в настоящее время подслушивающих устройств. Те частоты, для которых коэффициент корреляции превысил порог, попадают в список Опасных частот, которые оператор может проанализировать в окнах Анализа внутренней структуры Квадратура, Амплитуда, Фаза и Спектр сигналов, или прослушать через динамик приёмника комплекса или наушники, вызвав режим Прослушивания.

Кроме универсального коррелятора по звуковому тесту в комплексе реализован метод анализа сигналов на гармоники, который совместно с универсальным коррелятором приводит к практически полному отсутствию ложных срабатываний комплекса.

В режиме идентификации сигналов оператором происходит пошаговая проверка Всех обнаруженных или только Вновь появившихся сигналов с анализом их

Локализация источников радиоизлучения

Локализация производится после обнаружения идентификатором Опасной частоты.

Локализатор предназначен для определения местоположения ИРИ в двух- или трехмерном пространстве после его идентификации как Опасная частота. Для этого в окне Локализация задается план контролируемого помещения с его размерами (длиной, шириной и высотой) с точностью не хуже 0.2 м. Кроме того на плане наносятся координаты 4-х звуковых колонок в пространстве с их номерами. Колонки рекомендуется размещать по углам помещения таким образом, чтобы они не находились в одной плоскости.

В автоматическом режиме работы комплекса локализация осуществляется после обнаружения идентификатором опасной частоты корреляционным методом. Для этого специальный тестовый сигнал подается последовательно на одну из 4-х колонок и методом акустической локации определяется местоположение (координаты) ИРИ. Полученные результаты запоминаются и процесс продолжается на других частотах. Оператор в любой момент может остановить обнаружение и идентификацию сигналов и посмотреть результаты локализации ИРИ. Просмотр результатов локализации выбирается в любой удобной плоскости.

Локализация может производиться также оператором как при помощи тех же четырех колонок путем подачи команд на их излучение, так и при помощи режима Индикатор поля. Уточнить местоположение ИРИ можно перемещая приемную антенну в контролируемом помещении. Точность локализации в этом случае возрастает до единиц сантиметров.

Поиск возможных каналов утечки речевой информации за счет акустического воздействия на аппаратуру связи, оргтехнику и другие устройства (210)

Поиск возможных каналов утечки речевой информации производится комплексом с подключенной широкодиапазонной антенной по электрической составляющей поля в диапазоне 0.15—1000 МГц или рамочной антенны по магнитной составляющей поля в диапазоне 0.15—30 МГц (поставляется по отдельному заказу). При этом антенна устанавливается на расстоянии 1 м от исследуемой аппаратуры. Включается режим Обнаружение, при котором производится снятие радиопортрета эфира при выключенном исследуемом устройстве путем сканирования диапазона не менее 10 раз. Затем устройство включается в штатный режим и производится снятие электрической и магнитной составляющих его спектра. Далее перед исследуемым устройством на расстоянии 1

Акустическое воздействие...

м устанавливается звуковая колонка, включается режим Идентификация и производится проверка частот спектра ПЭМИ на наличие паразитной модуляции в автоматическом режиме или оператором при помощи окон анализа.

Классификация (211)

В настоящее время рынок технических средств поиска и нейтрализации средств негласного съема информации настолько велик, что можно сказать, что он близок к насыщению. Знакомясь с рекламно-справочными материалами, полученными с выставок, журналов, по сети интернет даже подготовленному специалисту зачастую бывает трудно разобраться в преимуществах одного средства перед другим. Особенно это характерно для таких наукоемких видов устройств обнаружения каналов несанкционированного съема информации, как автоматизированные программно-аппаратные комплексы поиска, обнаружения и локализации средств негласного съема акустической информации.

Поэтому можно предложить следующую упрощенную классификацию современных программно-аппаратных поисковых комплексов:

- комплексы мобильные;
- комплексы стационарные.

Такие характеристики и мобильных и стационарных комплексов, как диапазон рабочих частот, динамический диапазон, чувствительность определяются в основном типом используемых в них сканирующих радиоприемников.

Но ряд характеристик, принципиально важных для решения задачи обнаружения радиоизлучающих средств съема информации целиком зависят от разработчика комплекса. Прежде всего к таким характеристикам относится показатель производительности комплексов, а именно скорость панораммного обзора загрузки радиодиапазона, с учетом времени, затрачиваемом комплексом на надежное определение принадлежности обнаруженного сигнала к классу сигналов подслушивающих устройств. Характеристики производительности важны для обнаружения дистанционно управляемых или кратковременно излучаемых радиозакладок.

Исходя из этого, ***множество существующих программно-аппаратных комплексов можно еще разделить на две группы: с обычной производительностью,*** определяемой технической скоростью сканирования используемых приемников и *с* ***повышенной производительностью*** в состав которых входит специальная аппаратура аналогово-цифровой обработки сигналов (обычно на базе процессора быстрого преобразования Фурье) многократно повышающая скорость панораммного анализа.

Стационарные комплексы, как правило, имеют высокую производительность, кроме того в стационарных комплексах используются быстродействующие высокочастотные и низкочастотные коммутаторы, обеспечивающие анализ одновременно нескольких помещений в режиме реального времени. ***В стационарных и мобильных комплексах высокой производительности*** есть возможность ручного анализа оператором динамических характеристик обнаруживаемых сигналов в реальном масштабе времени. Эта возможность важна для проведения пользователем детального анализа акустически некоррелируемых сигналов, относимых аппаратурой комплекса к разряду вероятных сигналов радиомикрофонов и принятия оператором правильного решения о принадлежности сигнала к средству несанкционированного съема информации.

Исходя из приведенной классификации можно дать рекомендации покупателю по приобретению программно-аппаратного комплекса. Конечно для полной уверенности лучше всего приобрести многофункциональный высокопроизводительный комплекс, позволяющий работать стационарно и имеющий мобильную комплектацию. Стоимость такого комплекса будет составлять не менее 10–15 тысяч долларов.

Если бюджет ограничен, то можно рекомендовать приобрести недорогой мобильный комплекс, обладающий возможностью последовательного наращивания своих функций. Минимальный набор: ПК (желательно Note book), сканирующий приемник, управляемый от ПК (из списка, приведенного выше) и программное обеспечение. Выбор программ сейчас очень велик. От простейших типа RS-1000, RST-1200, RST-2000, SEDIF 2.0 до более универсальных типа SCANAR, SEDIF SCOUT, FILIN-98, управляющей программы комплекса АКОР-1, и т.д.

К ***мобильным комплексам высокой производительности*** и имеющие широкие функциональные возможности можно отнести такие, как АКОР-1 (базовый комплект), КРК, КРОНА-5Н, КРОНА-6Н, АРК-Д1-12 стоимость которых составит от 6 до 8 тысяч долларов.

Проверка электронной техники (244)

Основа работы в этом случае — сравнение с эталоном. Электронные устройства вскрывают и осматривают с целью выявления изменений схемы и появления дополнительных конструкций, сделанных не на заводе.

Особое внимание следует уделять подпайкам к проводам питания. Полностью внедрить устройство съема информации в промышленное изделие можно только в заводских условиях, поэтому более быстрым, относительно простым и поэтому наиболее реальным способом внедрения является подсоединение устройства съема к цепи питания с помощью проводников.

При внимательном рассмотрении можно определить следы элементов, установленных вне заводского цикла: следы паек, изменение цвета покрытия в местах подпаек и прочие отметки вмешательства. Наличие эталона упрощает исследование, поэтому необходимо заранее узнать марки всех электронных изделий и подобрать их эталоны.

Контроль радиоизлучений электронной техники

Перед разборкой электронных приборов, например современных телефонных аппаратов, их проверяют с помощью индикатора поля и частотомера на наличие излучений как во включенном (телефонные аппараты со снятой трубкой), так и в выключенном (с положенной трубкой) состоянии.

ИК-передатчики (214)

Для повышения скрытности, в последние годы стали использовать для передачи перехваченной микрофоном информации инфракрасный канал. В качестве передатчиков используются маломощные полупроводниковые лазеры и светодиоды. В качестве примера рассмотрим закладку TRM-1830. Дальность действия ее днем 150 м, ночью — 400 м. Ток потребления — 8 мА, время непрерывной работы — 20 часов. Габариты не превышают $26 \times 22 \times 20$ мм. К недостаткам можно отнести необходимость прямой видимости между закладкой и приемником и влияние фоновой засветки. Все это резко ограничивает оперативные возможности подобных средств. Самое же громкое дело в США, связанное с применением оптических закладок — Уотергейт.

При наличии подозрительных излучений, регистрируемых индикатором и частотомером на расстоянии 60−80см от прибора, необходимо настроить комплекс радиоконтроля на эту частоту и, облучая проверяемый прибор акустическим сигналом, искать признаки модуляции в принимаемом радиосигнале.

В качестве облучающего сигнала лучше всего использовать генератор с резко меняющимся уровнем (типа сирены), а наблюдать принимаемый сигнал — на анализаторе спектра или осциллографе, подключенном к приемнику ПКР.

Указанный способ проверки радиосигналов дает положительный эффект даже в том случае, когда в радиомикрофоне используется необычный вид модуляции или шифрация. В этом случае акустический сигнал модуляции как бы “перегружает” передатчик, и в его радиосигнале это можно выявить.

Если “под рукой” нет анализатора спектра, можно воспользоваться и наушниками, но оценка будет менее объективной. В этой ситуации целесообразно повторить исследование обнаруженного радиосигнала без проверяемого устройства — его необходимо убрать в соседнее помещение. Такую проверку целесообразно проводить и при наличии анализирующих приборов. Если обследование проводится в большом помещении, то возможна ситуация, когда облучая акустическим сигналом один проверяемый прибор, обнаруживается канал утечки от другого устройства.

Как показывает практика, не обязательно в нем обнаруживается внедренная спецтехника. Чаще всего канал утечки информации создается в электронных устройства за счет конструктивных особенностей или даже дефектов. Проверяемые электронные устройства, в которых обнаружены паразитные каналы утечки информации необходимо из помещения удалить.

Исследования возможности утечки речевой информации от оборудования, установленного на объекте исследования посредством акустоэлектрических преобразований (213)

Исследованиям подвергается оборудование, находящееся в обследуемом помещении, на которое воздействуют акустические сигналы, содержащие конфиденциальную информацию (беседы, совещания и т.д.).

Проверка наличия наведенных сигналов, вызванных акустоэлектрическими преобразованиями, проводится во всем исследуемом диапазоне частот (определяется техническими характеристиками оборудования) во всех проводах или линиях связи, подключенных к

исследуемому оборудованию (цепи питания, линии связи, шины заземления, служебные цепи и т.д.).

Подслушивание

Интересно

Наиболее простым способом перехвата разговора является обыкновенное подслушивание, причем, очень часто, случайное. Достаточно распространенной является ситуация, когда находящиеся в приемной посетители достаточно отчетливо слышат все, что происходит в кабинете; в курилке сотрудники фирмы, не обращая внимания на присутствие посторонних продолжают обсуждать важные проблемы; летом совещания, в том числе на нижних этажах, ведутся при открытых окнах или форточках. В этих ситуациях, как говорится, не хочешь, а услышишь.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Исследования проводятся следующим образом:

На расстоянии 0,5 м от исследуемого оборудования устанавливается источник акустического поля, спектр акустических сигналов которого должен перекрывать весь речевой диапазон.

Производится идентификация наведенных сигналов посредством преобразования электрических сигналов, присутствующих в исследуемой линии, в акустические. Преобразование выполняется путем подключения к исследуемой линии входа микрофонного усилителя, при этом оценка наведенных сигналов выполняется на слух через головные телефоны, подключаемые к выходу микрофонного усилителя. При наличии сигналов, вызванных электроакустическим преобразованием исследуемого оборудования на проводах и линиях связи, необходимо принять меры по защите.

Методы выявления закладных устройств, подключаемых к телефонным линиям (233)

Прежде чем говорить о методах контроля телефонных линий, следует оценить параметры входных цепей технических средств (ТС) съема информации, включаемых в телефонную линию.

Параметры входных цепей ТС, включенных в телефонную линию для перехвата информации с питанием от линии (234)

Напряжение питания в телефонной линии связи при поднятой трубке постоянно и лежит в пределах 5—15В, величина разговорных токов в линии при поднятой трубке равна 35 мА. Следовательно, для обеспечения питания ТС мощностью 5 мВт входные цепи ТС могут быть представлены только эквивалентным сопротивлением, включенным параллельно линии $R_{тф\text{-}паралл}$ или в разрыв одной из жил рабочей пары телефонной линии связи $R_{тф\text{-}посл}$. Величина $R_{тф\text{-}паралл}$ не может быть более 5 кОм при поднятой трубке. Такое подключение может привести к переходу линии в режим вызова. Для исключения этого эффекта необходимо, чтобы сопротивление ТС было не менее 50 кОм, что соответствует потребляемой ТС мощности 2 мВт. Ток в линии при положенной трубке должен быть порядка 1,2 мА. Сопротивление $R_{тф\text{-}посл}$ не должно быть меньше 140ом. Вносимое падение напряжения при поднятой трубке не менее 5 В.

Параметры входных цепей ТС, включенных в телефонную линию для перехвата информации с автономным питанием (234)

Уровень сигнала наводимого микрофонами современных телефонных аппаратов в телефонной линии связи при акустическом воздействии, соответствующем речевому сигналу на расстоянии 6 см от рта говорящего (97 дБ) лежит в пределах 40—700 мВ. Величина собственного шума, вносимого телефонным аппаратом в линию, не может превышать 0.5мВ. При эквивалентном сопротивлении телефонной линии связи равном 600ом, ток вызванный работой ТА в режиме передачи речевого сообщения не менее 1 мка.

Входные цепи ТС включенные параллельно телефонной линии с целью перехвата передаваемого сообщения не могут содержать только индуктивность и должны состоять из сопротивления $R_{тфс}$ или емкости Стфс либо последовательно включенных емкости и сопротивления. Применение индуктивности в такой цепи не исключено, но не обязательно.

При минимальном сигнале в телефонной линии равном 0,5 мВ величина модуля входного сопротивления может достигать 5 ГОм. Для обеспечения высокого качества перехватываемого сообщения необходимо соблюдать соотношение сигнал/шум не менее 10, граничные значения сопротивления и емкости ТС перехвата информации подключенного параллельно линии в этом случае имеют следующие значения $R_{тфс.гр.}$ = 50 мОм, $C_{тфс.гр}$ = 3.3 пф. Для обеспечения достаточного качества перехвата на любом участке линии (на ближнем и на дальнем конце), для линий с наихудшими параметрами оптимальная величина модуля входного сопротивления 130ком. Реально можно ориентироваться на величину в пределах 1−5 МОм. При подключении ТС возможно увеличение тока утечки при положенной трубке на величину 0,5 мкА—0,5 мА.

Входные цепи средства включенного в разрыв телефонной линии не могут иметь в своем составе емкости, включенные последовательно, т. к. это приведет к

прекращению связи. В разрыв линии можно включать только сопротивления и индуктивности. Величина сигнального тока в линии не менее 1 мкА. Тогда минимальная величина сопротивления входных цепей, с которого можно снять сигнал достаточного качества, равна 0.00005 Ом, величина индуктивности 0,01 мкГн. Учитывая то, что ТС наверное должно быть универсальным и сохранять работоспособность независимо от места включения в линию, можно ожидать, что при разработке учитывается реальное ослабление сигнала (допустимо ослабление на 28 дБ). Устройство, рассчитанное на перехват сигнала, передаваемого током равным собственному шуму микрофона телефонной трубки должно включаться в разрыв линии через сопротивление не менее 20 Ом или индуктивность не менее 4 мГн. Демаскирующим признаком может служить дополнительное падение напряжения на участке линии на 0,7 В и более.

Методы выявления закладных устройств, подключаемых к проводным линиям (244)

Исходя из изложенного выше, методы контроля телефонных линий основаны на том, что непосредственное подключение к ним вызывает изменение электрических параметров линий: напряжения, тока, активного и реактивного сопротивлений, а также емкости и индуктивности. В зависимости от способа подключения закладного устройства (ЗУ) к телефонной линии (последовательного или параллельного) влияние его на изменение параметров линии будет различным.

Наиболее информативным и легко измеряемым параметром телефонной линии является напряжение в ней при положенной и поднятой трубке. Для большинства ГАТС напряжение 60–64 В при положенной трубке и 8–15 В (в зависимости от модели телефонного аппарата) при поднятой трубке. Но эти параметры могут изменяться не только при подключении закладного устройства, но и из-за плохой линии (изменения состояния атмосферы, время года, осадки, плохие контакты и т.д.). Поэтому контроль напряжения в линии следует вести постоянно. Некоторые устройства защиты телефонных переговоров ("Барьер-3", "Аккорд-200" и др.) постоянно индицируют напряжение в линии и можно набрать статистику от различных условий, учитывая при этом, что резкое изменение напряжения должно настораживать, нет ли постороннего подключения?

При подключении к линии ЗУ с питанием от телефонной линии изменяется и величина потребляемого тока, который зависит от мощности передатчика закладки и его КПД. Но не всегда этот параметр информативен, например при подключении к телефонной линии адаптера с внешним питанием и большим входным сопротивлением, ток потребляемый устройством незначителен.

Возможен также анализ переменной составляющей сигнала на линии. Например, при появлении сигнала с частотой более 50 кГц может быть сделан вывод о том, что к линии, возможно подключена аппаратура ВЧ-навязывания, или по линии передается модулированный высокочастотный сигнал. Появление на линии низкочастотного сигнала в то время, когда линия находится в отбое, может свидетельствовать о возможной попытке перехвата информации из помещения.

Телефонные радиопередатчики или так называемые ретрансляторы могут использовать в качестве антенны телефонную линию или просто наводить ВЧ-сигнал в линию, который также может быть обнаружен специальными приборами.

Индуктивное подключение характеризуется тем, что практически не вносит изменений в характеристики линии, но позволяет перехватывать ее побочные излучения, методы обнаружения посредством измерения параметров линии в настоящее время неизвестны.

Средства контроля проводных линий (234)

Средства контроля проводных линий, предназначенные для выявления несанкционированных подключений к ним с целью организации каналов утечки информации, условно можно разделить на три группы:

1 – средства контроля сигналов в линиях – усилители НЧ-сигналов, широкополосные индикаторы ВЧ-сигналов, перестраиваемые приемники модулированных ВЧ-сигналов;

2 – средства контроля нормализованных параметров линий (как действующих, так и отключенных от потребителей и источников; как по постоянному, так и по переменному току) – контроль импеданса, напряжения, тока;

3 – средства контроля параметров линий, основанные на принципе активного воздействия на линию и выявления аномалий, вызванных реакцией на него подключенных к линии устройств.

Средства контроля проводных линий могут быть выполнены как “сторожевые”, так и “поисковые”. Как те, так и другие могут сочетать в себе функции приборов разных групп предлагаемой классификации.

К приборам 1-й группы могут быть отнесены такие изделия, как ST 031 “Пиранья” (Россия), “Облако” (Россия), СРМ-700 “Акула” (США). К приборам 2-й группы могут быть отнесены Winkelman Model 200/B (США), КТЛ-3, КТЛ-400 (Россия). К средствам, сочетающим в себе функции 1-го и 2-го классов, относятся ТСМ-03 (США), ТПУ-5 (Россия), SP-18T “Багер-01” (Россия) и др.

Средства, относящиеся к первой группе, *выявляют сигналы устройств, несанкционированно подключенных к линиям, и позволяют:*

- прослушивать НЧ-сигнал в линии, выявляя его связь с акустическим сигналом в помещении (наличие подключенных микрофонов, устройств, обладающих микрофонным эффектом и т.д.);
- выявить наличие так называемого сигнала ВЧ-зондирования или постоянно действующего передатчика сигнала в линию с уровнем, превышающим в месте подключения средства контроля уровень собственных сигналов в линии или естественный фон ВЧ-наводок;
- выявить наличие ВЧ-сигнала, модуляция которого связана с акустическим сигналом в помещении;
- выявить наличие модуляции зондирующего ВЧ-сигнала, которая связана с акустическим сигналом в помещении.

Средства второй группы, выявляют отличия нормализованных параметров линий при наличии и отсутствии подключений к ним. Основная масса средств контроля, условно, второй группы – это пассивные измерители величин сопротивлений, емкостей, напряжений, токов, адаптированные к изменениям в проводных линиях с введенной в схему измерений необходимой коммутацией, автоматизацией, интерпретацией показаний и т.д. Приборы, предназначенные для измерения и анализа параметров телефонных линий так и называют анализаторами телефонных линий. Для того, чтобы противодействовать анализатору, злоумышленнику придется использовать системы перехвата, которые не изменяют или незначительно изменяют параметры линии. Возможно использование систем перехвата с компенсацией изменений. В любом случае это повышает стоимость оборудования для перехвата информации, снижает удобство и повышает риск операции.

Достоинства применения анализаторов телефонных линий состоит в том, что, установка такого прибора на городскую линию позволит своевременно зафиксировать попытку подключения к линии. Появляется возможность отследить изменения параметров линии и вовремя принять меры для осмотра и очистки линии.

Недостатки применения анализаторов телефонных линий:

- ***отсутствуют четкие критерии оценки несанкционированного подключения.*** Телефонные линии не идеальны. Даже в спецификации на стандартные параметры сигналов городских АТС предусмотрен большой разброс. Параметры линий могут меняться в зависимости от загруженности АТС, колебаний напряжения в энергосети. Температура и влажность окружающей среды существенно влияют на качество контактных соединений, которые всегда есть на любой телефонной линии, и приводят к окислительным процессам на этих контактах. Промышленные наводки дают посторонние сигналы на линии. Даже при комплексном анализе большого количества параметров речь может идти о свершении события с некоторой вероятностью;
- ***высока вероятность ложных срабатываний и невозможность определить все виды подключений.*** В частности, хотя и существует теоретическая возможность определить устройство бесконтактного подключения к линии (емкостной или индуктивный датчик), практически на реальной линии с ее "плывущими" параметрами и паразитными наводками сделать это чрезвычайно сложно;
- ***существенное снижение вероятности определения факта подключения, если линия заранее не проверена на "чистоту".*** Многие анализаторы требуют при установке на линию балансировки под ее конкретные параметры. Если при балансировке на линии уже было установлено некое устройство перехвата информации, то оно не будет обнаружено.

Более совершенные и более дорогие анализаторы не требуют чистой линии, но тем не менее все-таки склонны к ложным срабатываниям, обладают низкой вероятностью определения подключения с внесением незначительных изменений параметров линии, и совсем не определяют наличие бесконтактного подключения.

Следует отметить, что применение сравнительно новых, универсальных приборов высокого класса, таких как КТЛ-400 или SP-18/T "Багер-1" на некоторых современных АТС невозможно без имитатора АТС, так как искусственное изменение тока и напряжения в линии с целью анализа нелинейности импеданса, АТС воспринимает как неисправность и отключает линию.

Применение средств первого и второго классов может дать ощутимый эффект при постоянном (в “сторожевом” режиме) или периодическом контроле конкретных линий.

К третьей группе средств контроля проводных линий в предлагаемой классификации могут быть отнесены рефлектометры и, так называемые, нелинейные локаторы проводных линий.

Определение

Рефлектометры – устройства, предназначенные для выявления неоднородностей волнового сопротивления анализируемой линии. К ним относятся выпускаемые промышленностью стандартные измерители неоднородностей линий типа Р5-10, Р5-11 (Россия) и приборы, рассчитанные на контроль проводных коммуникаций при их комплексной проверке на утечку информации, такие как “Бор-1” (Россия).

Рефлектометры основаны на подаче в линию импульсного сигнала и приеме отраженного от неоднородности линии сигнала. По запаздыванию отраженного сигнала, зная параметры линии, можно определить расстояние до неоднородности ("дефекта" линии). Возможности рефлектометров, как любой аппаратуры, ограничены их чувствительностью. Наилучшим образом выявляются дефекты типа "обрыв" и "короткое замыкание", а, например, подключения к линиям, имеющие входной импеданс резистивного характера в несколько десятков кОм ими принципиально не выявляются. Кроме того, сильно затруднен контроль разветвленных проводных коммуникаций, так как требует контроля каждого ответвления отдельно.

Нелинейные локаторы проводных линий – приборы, основанные на выявлении в линии гармонических составляющих испытательного сигнала, вызванных подключением к ней устройств с нелинейным входным импедансом.

Интересно

Обнаружительная способность нелинейных локаторов проводных линий, реализующих "осциллографический метод" (АТ-2, АТЛ, ОК-1 и др.), приборов серии КОМ, "Визир" (все – Россия) и др. составляет величину от 1 мВт и более (обнаружительная способность "пассивных измерителей" ниже, как минимум, на порядок и более). Для примера, обнаружительная способность прибора КТЛ-2, выраженная в тех же единицах, составляет величину порядка 100 мВт, прибора ТПУ-5 – 10-30 мВт.

Анализатор линий LBD-50 (Россия) представляет собой комплексный прибор, в котором реализовано несколько взаимно дополняющих методов проверки проводных линий.

Анализатор линий LBD-50 представляет собой нелинейный локатор проводных коммуникаций, в котором достигнута обнаружительная способность, выраженная в тех же единицах, 10 мкВт — для параллельно подключенных блоков питания и 100 мкВт — для последовательно подключенных.

Кроме того, в LBD-50 применен режим контроля импеданса линии в режиме "холостого хода" методом измерения переходных процессов при подаче импульсного сигнала, что позволяет выявлять параллельные подключения, содержащие RC-цепи с постоянной времени 100 мкс и более.

Таким образом, обнаружительная способность LBD-50 на один-два порядка выше, чем у других нелинейных локаторов проводных линий и, как минимум, на два-три порядка выше "пассивных измерителей".

Проверка параметров телефонных линий связи (213)

Для анализа возможности подключения к телефонной линии несанкционированных потребителей, которыми являются закладные устройства, необходимо проверить:

- напряжение в телефонных линиях при пассивном телефонном аппарате — ТА (при положенной трубке) и его отличие от напряжений стандартного ряда;
- напряжение в телефонных линиях при активном ТА (при снятой трубке) и его отличие от обычного для исследуемого типа телефонных аппаратов;
- ток в телефонной линии при активном и пассивном ТА.

Причем указанные параметры необходимо проверять как минимум в двух точках: возле ТА и на распределительном щитке. При обнаружении отклонений от нормы необходимо проверить напряжение в телефонной линии — ТЛ, отключив ее на щитке от ТА.

Телефонные линии обследуются под нагрузкой индикатором поля или другим средством контроля эфира. Для этого имитируется разговор на линии, а поисковик перемещается вдоль проводки с индикатором поля или другим средством контроля эфира. В случае обнаружения подозрительных излучений имитируется многократное рассоединение. Если в этом случае уровень подозрительного сигнала меняется синхронно с рассоединением, то обнаруженный сигнал необходимо поставить на контроль ПКР для дальнейшей дешифровки. При необходимости ПКР можно перемещать вдоль ТЛ для определения места расположения источника излучения. Этот метод позволяет выявлять подключение подслушивающих устройств с передачей по радиоканалу, находящихся также и вне проверяемого участка, поскольку будет иметь место "наводка" сигнала на телефонную линию.

Передача информации по телефонным линиям (213)

Широкое распространение в последнее десятилетие за рубежом получили системы акустического прослушивания помещений через телефонную линию. Рассмотрим алгоритм работы подобных систем на примере TELE-MONITOR. На телефонной линии (внутри телефонного аппарата) устанавливаются специальные датчики (подключаются параллельно). При необходимости прослушать разговор производится звонок с любого телефона, в том числе и по междугородней связи, и выдается в телефонную трубку специальный сигнал. Звонки в этом случае не проходят на телефон и датчик TELE-MONITOR начинает передавать в линию разго-

воры, происходящие в помещении. Таких датчиков можно установить до четырех, скажем, для контролирования четырех комнат квартиры, при этом инициировать их в любой последовательности.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Проверка телефона на наличие "жучков" с помощью прибора СРМ-700 (754)

Выполняется посредством измерения уровня сигнала на линии при снятой трубке. Верификация телефонного "жучка" выполняется прослушиванием номеронабирания через наушники.

Поиск осуществляется в следующей последовательности:

1. СРМ-700 расположить рядом с телефоном, при этом телефонная трубка — на рычаге, длина антенны сокращена до 10 см, чтобы ослабить прием радиочастот окружающей среды; шнур, идущий от телефонной трубки 4 раза следует обернуть вокруг антенны.

2. Сравнить предыдущие уровни шумов в помещении и измеренный уровень в телефоне (при опущенной трубке), и если наблюдается значительное увеличение, необходимо произвести верификацию звука для определения, безопасен ли этот сигнал.

3. Измерьте минимальный р.ч. уровень на шкале, снимите трубку и посмотрите на увеличение р.ч. уровня (обычно это составляет более 2 сегментов). Прослушайте тональный сигнал готовности через наушники. Если уровень на шкале увеличится или тональный сигнал готовности слышен через наушники СРМ-700, значит возможно наличие телефонного "жучка". Обычный телефон вызывает только небольшой звук и моментальный скачок на шкале.

4. Проверьте телефон, повторив тестирование, перемещая зонд в стороны от телефона, измеряя при этом разницу показаний при поднятой и опущенной трубке.

5. Повторить процедуру на КРТ и за пределами комнаты, где линия входит в здание. Пусть кто-нибудь снимает и кладет трубку во время проверки. Обычный телефонный аппарат без "жучков" ответит моментальным щелчком и незначительным изменением уровня радиочастот без слышимого тонального сигнала готовности через наушники.

Проверка телефонной линии с помощью прибора ST 031 (754)

Основными видами проводных линий, для анализа которых предназначен прибор ST -031 "Пиранья", являются линии электросети (высокопотенциальные линии), а также абонентские телефонные линии и линии систем пожарной и охранной сигнализации (низкопотенциальные линии).

В целом приёмы и методы, применяемые для проверки проводных линий названных видов, одинаковы. Подключение к ним осуществляется с использованием единого, универсального адаптера. Анализу методом сканирования подвергается общий диапазон от 0 до 15МГц. Вывод результатов сканирования производится в виде изображения панорамы с однотипным представлением (отображением) измеренных параметров. Функции органов управления прибором одинаковы (вне зависимости от вида проверяемой линии).

Шаг перестройки фиксированный и составляет 5 кГц и 1 кГц при автоматическом и ручном сканировании, соответственно.

Для адаптации настройки прибора к условиям и задачам контрольно-поисковых работ предусмотрена возможность выбора направления и скорости автосканирования, а так же два варианта установки необходимых границ диапазона перестройки (задание начальной и конечной частоты или задание центральной частоты перестройки и ширины диапазона).

Классификация сигналов в контролируемых проводных линиях осуществляется на основе анализа автоматически выводимой на экран дисплея панорамы (диаграммы), отображающей частотные составляющие спектра принятого сигнала и его уровень на каждой из них. При осуществлении ручного сканирования (точной настройки) дополнительно обеспечивается возможность непосредственного слухового контроля принятого сигнала путём вывода его на встроенный громкоговоритель или головные телефоны.

Проведение подготовки контролируемого помещения заключается в проверке соответствия количества и назначения реально существующих в нём проводных линий ранее изготовленным (представленным) схемам их прокладки.

Подготовка самого прибора ST 031 "Пиранья" (после проверки его работоспособности в данном режиме) фактически состоит только в выборе наиболее удобных наконечников к щупам, применительно к типу и особенностям имеющихся проводных линий.

Наибольшее внимание следует уделять диапазону 40-2500 кГц, как наиболее типичному для использования закладками, питающимися от напряжения проводных линий и передающих перехваченную информацию по их проводам. Значительно реже встречаются закладные устройства с частотами около 7 МГц и выше. Для обеспечения гарантированной надёжности не пропуска сигналов закладок по частоте верхняя граница диапазона сканирования в приборе ST 031 "Пиранья" определена на уровне 15 МГц.

Рекомендуется следующий порядок действий оператора

Включить прибор. Дождаться начала сканирования в диапазоне до 10.450 МГц и после завершения 2-3-х циклов установить верхнюю границу диапазона на уровне 15 МГц. Внимательно изучив наиболее характерные особенности изображения панорамы определить наличие частотных составляющих, превышающих уровень общего фона.

При необходимости разбить диапазон на отдельные интервалы и просканировать их подробно, останавливаясь, прежде всего, на частотах наиболее интенсивных составляющих.

Границы интервалов задаются последовательным нажатием кнопок "SET", "4", кнопок с цифровой маркировкой и кнопки "ENTER" (либо альтернативнй вариант с заданием центральной частоты и ширины полосы).

Установить нижний порог индикации уровня сигнала порядка 10−15%. Для этого нажать кнопку "SET", кнопкой "3" вывести надпись "3 — > THRESHOLD level", нажать кнопку "ENTER" и кнопками "5" и "6" добиться установки этого порога индикации. В последующем, в зависимости от характера изображения панорамы, выбрать наиболее удобный для анализа уровень порога.

Запуск и остановка сканирования осуществляется нажатием кнопки "RUN/STOP".

После прохода нескольких циклов сканирования можно обоснованно установить порог "автостопа" для чего нажать кнопку "SET", выбрать кнопкой "3" режим "SQUELCH LEVEL", подтвердить выбор кнопкой "ENTER" и, манипулируя кнопками "5" и "6", поставить курсор на необходимый уровень. После остановки на частоте того или иного сигнала следует произвести точную настройку кнопками "3" и "4", одновременно анализируя сигнал "на слух" поочерёдным включением детекторов "AM" и "FM" кнопкой "ENTER". Для анализа слабых сигналов можно выбрать кнопками "SET", "5" и "ENTER" более удобный амплитудный диапазон (0,1-1мВ).

Можно дополнить проверку используя режим осциллографа.

Встроенный в прибор ST-031 осциллограф обеспечивает выполнение тех же основных функций по измерению амплитудных, частотных и временных параметров анализируемых сигналов, которые характерны и для промышленных осциллографов общего назначения.

Он может работать в одно- и двухканальном режиме. Штатным является одноканальный режим с подключением входа осциллографа к выходу амплитудного детектора основного тракта прибора.

Включение в него осуществляется автоматически при использовании прибора в режимах детектора низкочастотных магнитных полей, виброакустического и акустического приёмника. При работе прибора в режимах высокочастотного детектора-частотомера и детектора инфракрасных излучений − вручную через кнопку "OSC".

Двухканальный режим осциллографа является вспомогательным и может использоваться, например, для сравнения сигнала, принятого по основному тракту прибора, с некоторым внешним эталонным сигналом, поданным на дополнительный вход через разъём "OSC2". Его включение производится только вручную через кнопку "ENTER (CH S)".

В осциллографе на программно-технической основе заложена возможность выбора параметров вертикальной развёртки и управления перемещением "луча" вдоль вертикальной оси, выбора пределов горизонтальной развёртки, методов оцифровки сигналов и вариантов синхронизации, а также реализации процедуры курсорных измерений.

Это позволяет, фактически оптимальным образом, формировать осциллограммы и проводить оценку параметров сигналов в различных условиях проведения контрольно-поисковых работ.

Проверка отсутствия сигналов от закладных устройств в сети 220В

С целью обнаружения слабых сигналов необходимо использовать осциллограф, подключив его к сети 220В через согласующее устройство, обеспечивающее возможность анализа сигналов более высокочастотного диапазона на фоне сигналов с частотой 50 Гц.

Для подобных проверок можно использовать прибор ST-031 или Д-008 в режиме анализатора проводных линий или режиме осциллографа, а также прибор СРМ-700 с зондом ОНЧ (VLF), предназначенным для подсоединения к стенным розеткам переменного тока и отфильтровывания напряжения переменного тока 50Гц и пропускания полосы частот от 15КГц до 1МГц ко входу СРМ-700.

Можно также протестировать другие провода, кабели или телефонные линии на наличие VLF сигналов, подсоединяя проводник напрямую от каждого входного терминала зонда VLF к подозрительному соединению проводов. Оборудование с переключением питания (компьютеры, ксероксы, электронные пишущие машинки и т.д.) могут производить сигналы очень низкой частоты. Выборочно следует отключать такие приборы на время, чтобы изолировать себя от помех до тех пор, пока не обнаружится прибор, дающий сигнал не связанный с переключением питания. Необходимо произвести осмотр подозреваемого предмета.

Проверка отсутствия сигналов от закладных устройств, передающих информацию в звуковом и надтональном диапазонах (214)

Проверка выполняется путем включения в разрыв исследуемой линии резистора сопротивлением порядка 1КОм и анализа снятых с него сигналов в звуковом и надтональном диапазонах. Анализ может проводится как на слух с помощью малогабаритного магнитофона, так и визуально с помощью осциллографа. В рамках этой же проверки целесообразно проверить отсутствие и более высокочастотных сигналов в исследуемых линиях (до 30 МГц). Исследованиям должны подвергаться также телефонные линии, линии охранной и пожарной сигнализации и другие проводные коммутации, выходящие за пределы проверяемых помещений.

Проверка объектов ИС с помощью нелинейного локатора (754)

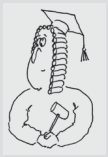
Принцип нелинейной локации состоит в том, что информация об обнаруживаемом объекте определяется его способностью спектрального преобразования зондирующего сигнала и переотражения его на гармониках частоты зондирования. Эта способность возможна при наличии в составе объекта элементов с нелинейными вольтамперными характеристиками. Такие элементы по природе своего возникновения делят на "искусственные" и "коррозийные". "Искусственные" — полупроводниковые приборы искусственного происхождения, содержащие *p-n* переход (диод, транзистор и т.п.). "Коррозийные" – нелинейные элементы, образованные в результате механического контакта металлических поверхностей через тонкую окисную пленку.

Особенность обнаружения "искусственного" полупроводника состоит в том, что уровень второй гармоники сигнала отклика на 20 дБ выше, чем третьей. "Коррозийный" полупроводник наоборот из-за малой толщины окисной пленки дает отклик более высокого уровня на третьей гармонике. Существенной особенностью вольт-амперной характеристики контактных полупроводников является ее неустойчивость при механическом воздействии (изменении давления на контакт).

Проверка мебели и интерьера (книги, карнизы, сувениры, папки с бумагами, пепельницы и т.д.) начинается с их тщательного осмотра.

Особое внимание следует уделить всякого рода укрепляющим брускам-подставкам и способам их крепления, поскольку аппаратура подслушивания, закамуфлированная под элементы мебели, крепится, как правило, на шипах или подобных устройствах, позволяющих при необходимости установить спецтехнику в течение нескольких секунд. Затем готовится площадка для проведения аппаратурной проверки с использованием нелинейного локатора. Сначала площадка проверяется на наличие помеховых сигналов. Определяются источники помех и, по возможности, устраняются, например переносятся, или идентифицируются по направлению так, чтобы при обследовании была возможность развернуть поисковый аппарат в противоположном направлении.

Полуактивная система акустической разведки (214)



Определение

Самым оригинальным, простейшим и малозаметным до сих пор считается полуактивный радиомикрофон, работающий на частоте 330 МГц, разработанный еще в середине 40-х годов. Он интересен тем, что в нем нет ни источника питания, ни передатчика, ни собственно микрофона. Основой его является цилиндрический объемный резонатор, на дно которого налит небольшой слой масла. В верхней части цилиндра имеется отверстие, через которое внутренний объем резонатора сообщается с воздухом помещения, в котором ведутся переговоры. Верхняя часть сделана из пластмассы и является радиопрозрачной для радиоволн, но препятствием для акустических колебаний. В указанное отверстие вставлена металлическая втулка, снабженная четвертьволновым вибратором, настроенным на частоту 330 МГц. Размеры резонатора и уровень жидкости в нем подобраны таким образом, чтобы вся система резонировала на внешнее излучение на частоте 330 МГц. При этом собственный четвертьволновый вибратор внутри резонатора создает внешнее поле переизлучения. При ведении разговоров вблизи резонатора на поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора. Этих изменений достаточно, чтобы влиять на поле переизлучения, создаваемого внутренним вибратором, которое становится модулированным по амплитуде и фазе акустическими колебаниями. Работать такой радиомикрофон может только тогда, когда он облучается мощным источником на частоте резонатора, т.е. 330 МГц. Главным достоинством такого радиомикрофона является невозможность обнаружения его при отсутствии внешнего облучения известными средствами поиска радиозакладок.

Впервые информация об использовании подобной полуактивной системы была обнародована американским представителем в ООН в 1952 году. Этот резонатор был обнаружен в гербе посольства США в Москве. С тех пор для полуактивных систем применялись все более высокие диапазоны, вплоть до миллиметровых волн; современные резонаторы по форме напоминают пластмассовую блесну. Американцы жаловались, что в 60-е годы их представительства в СССР постоян-

но облучались высокочастотными сигналами с целью активизации встроенных резонаторов.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

Если, например, помеховый сигнал идет от стены, то при развороте антенны нелинейного локатора, т.е. при обследовании предмета в направлении "от стены", помеха значительно ослабнет. Убедиться в том, что сигнал ложный, можно и путем перемещения обследуемого предмета при неподвижном поисковом приборе. При этом если уровень сигнала от поискового прибора практически не меняется, то сигнал ложный.

Затем, убедившись в том, что сигнал исходит именно от обследуемого предмета, следует внимательно осмотреть источник сигнала. Если сигнал возникает в крепежных элементах (гвозди, болты и т.д.), то следует попытаться запомнить тембр сигнала, его уровень, характерные трески при простукивании места отклика.

Обследование мебели и интерьера следует проводить при минимально возможной чувствительности нелинейного локатора, предварительно проверив его работоспособность. Предмет проверяется с разных точек, чтобы зафиксировать точное направление на источник сигнала.

Дешифровка сигналов нелинейного локатора проводится на слух, например путем энергичного простукивания узлов соединений, поскольку в этих местах практически всегда существует нелинейность, образуемая контактом разнородных металлов и окисных пленок. Качество таких полупроводниковых свойств низкое, поэтому нелинейный локатор будет давать "хриплый" тон, который при простукивании модулируется или может вообще исчезнуть.

Электроакустические преобразования (213)

При разговоре акустические волны воздействуют на конструктивные элементы электронных приборов. Они, в свою очередь, влияют на электромагнитное поле излучающих элементов или создают микроскопические токи в проводниках. Все эти токи и поля оказываются промодулированы речью и при соответствующей обработке можно извлечь полезную информацию.

Проиллюстрировать сказанное можно на примере телефона со звонком электромеханического типа. Акустические волны воздействуют на маятник звонка, соединенного с якорем электромагнитного реле. Под воздействием речевых сигналов якорь совершает микроколебания, что, в свою очередь, вызывает колебание якорных пластин в электромагнитном поле катушек, следствием чего является появление микротоков, модулированных речью.Подобные преобразования происходят в большинстве электронных устройств (электрочасах, телевизорах, радиоприемниках и т.д.). Дальности перехвата подобных сигналов, как правило, невелики, но иногда превышают 100 м. Для усиления эффекта иногда применяется так называемое высокочастотное навязывание. В этом случае электронный прибор облучается извне мощным высокочастотным сигналом, и осуществляется прием промодулированного речью отраженного излучения.

После окончания проверки на всю мебель и предметы интерьера наносятся незаметные, видимые, например, только в ультрафиолетовых лучах, метки, которые потребуются при последующих проверках. Составляется опись предметов, находящихся в помещении, которая хранится вместе с уточненным планом помещения у лица, ответственного за его безопасность, или в учреждении, проводящем поисково-защитные мероприятия.

Проверка ограждающих конструкций является заключительным этапом аппаратурных обследований. Основным поисковым инструментом здесь также является нелинейный локатор, особенно в случае бетонных ограждающих конструкций.

Перед началом обследований нелинейным локатором осматриваются все смежные с проверяемым кабинетом помещения, в том числе и на прилегающих этажах, убираются как можно дальше от смежных стен или по возможности выносятся устройства, содержащие электронику: аудио и видео техника, оргтехника, электронные телефонные аппараты, факсимильные аппараты и т.д.

Затем проводится моделирование на каждой из обследуемых поверхностей, для чего модель крепится с одной стороны стены, а аппарат устанавливается с другой так чтобы приемо-передающая антенна вплотную прилегала к поверхности и определяется минимальный регулировочный уровень нелинейного локатора, при котором обнаруживается модель. После работы с моделью обследуется поверхность стены в соответствии с методикой использования нелинейного локатора. При обнаружении отклика фиксируется его местоположение с помощью клейкой ленты или другим способом.

При первом проходе стены нелинейным локатором, особенно на относительно небольших поверхностях, рекомендуется сначала пройти всю площадь стены и зафиксировать отклики, а уже затем приступать к их дешифровке. Это связано с тем что большинство откликов возникает от таких элементов, как арматура, сетка "Рабица", гвозди, проводка, трубы и т.п.

Портативный нелинейный радиолокатор "NR 900 E" (213)

Портативный импульсный нелинейный локатор NR 900E представляет IV поколение локаторов серии NR 900 E. Сохраняя все достоинства предыдущих версий (высокий энергетический потенциал, остро направленная антенная система, наличие режима огибающей — "20K"), локатор NR 900 E обеспечивает возможность сравнительного анализа сигналов откликов на 2 и 3 гармонике зондирующего сигнала . Таким образом в нелинейном локаторе NR 900 E реализован наиболее мощный на сегодняшний день арсенал возможностей для обеспечения эффективных поисковых мероприятий. С эргономической точки зрения NR 900 E выгодно отличается высоко интеллектуальной микропроцессорной системой обработки сигналов и управления. Все органы управления и ЖКИ табло отображения информации вы ведены на пульт управления, размещенный на штанге — держателе антенной системы.

Обследуя первоначально всю поверхность стены, можно заметить характерные отклики, прикинуть причины их возникновения, оценить количество ложных откликов. Для дешифрации откликов используется снижение чувствительности и мощности облучения нелинейного локатора — чем ниже эти потенциалы, тем точнее антенна указывает на место источника. Затем по характеру отклика определяется его природа, например, классический полупроводник дает "чистый", сильный тон. При работе нелинейным локатором можно разрушить коррозионный полупроводник сильным простукиванием стены резиновым молотком. Ложный полупроводник имеет "исчезающий" или "хриплый" отклик; при простукивании у него появляется модуляция и возможны резкие изменения уровня сигнала отклика.

Места в которых отклик вызывает сомнения, лучше всего вскрыть и найти причину срабатывания нелинейного локатора. Можно попробовать и другой способ — нелинейный локатор перенести на противоположную сторону стены и снова контролировать подозрительный отклик. Часто это приводит к исчезновению отклика, что свидетельствует о ложном (коррозионном) полупроводнике.

Своеобразные эффекты могут наблюдаться при обследовании металлических оконных рам, если рядом работает мощная телевизионная или радиостанция. Наличие разнородных металлических элементов превращает ее в "диполь с установленными между плечами диодами". Такая конструкция сильно переизлучает попадающие на нее сигналы и может имитировать подслушивающее устройство. Избавиться от такого эффекта (или снизить его) можно открывая рамы на 90 градусов и сильно их простукивая.

При анализе подозрительных мест, обнаруженных поисковыми приборами, следует учитывать выбранную на этапе подготовки модель вероятного противника, т.е. имеется ли у него возможность установить технику съема информации в стену или нет. Внедрение спецтехники в ограждающие конструкции требует большой подготовки и существенных материальных затрат, а также благоприятных условий для работы на объекте (капитальный ремонт, строительство и т.п.). Менее сложным является путь внедрения спецтехники с внешней стороны стены: иногда для этих целей используют естественные ниши в ограждающих конструкциях.

Защита речевой информации (750)

Надо знать, что дорогостоящие предварительные проверки помещений на наличие подслушивающей аппаратуры и технических каналов утечки информации оказываются бесполезными, если подслушивающая аппаратура попадает в помещение накануне проведения конфиденциальных переговоров или вносится непосредственно участниками этих переговоров.

Существует различная аппаратура для оперативного контроля службой безопасности участников переговоров. Это и металлообнаружители и средства обнаружения работающих диктофонов или жучков, но эта аппаратура дает часто ложные срабатывания или незначительный процент обнаружения (особенно это относится к диктофонам). Не всегда ее можно применять из этических соображений. Кроме того, надо всегда исходить из того, что "противник" умнее нас и пронесет технику в выключенном состоянии. Следует также учитывать, как уже отмечалось ранее, виброакустический канал утечки речевой информации и плохую звукоизоляцию помещений.

Исходя из этого, наиболее надежным направлением противодействия несанкционированному получению речевой информации является препятствование звукозаписи переговоров или ее ретрансляции из помещения путем создания акустических шумов или направленного подавления.

Каналы утечки речевой информации не обязательно только технические, но и естественные, такие как воздух, несущие конструкции, трубы отопления, водопровода, вентиляционные каналы и т.д.

Задача защиты от утечки состоит в перекрытии всех возможных каналов и нейтрализации средств перехвата (микрофоны, направленные микрофоны, диктофоны, стетоскопы, закладные устройства, лазерные системы, инфракрасные и т.д.)

Один из наиболее распространенных методов защиты состоит в создании шумовой акустической помехи, обеспечивающей скрытие информативного сигнала,

при этом соотношение величина шумового сигнала/величина информативного сигнала должны обеспечивать надежное скрытие информативного сигнала или снижение его разборчивости до достаточных пределов.

Возможности повышения звукоизоляции связаны со строительными работами по акустической защите выделенных помещений, но они не дают нужной защиты от внесенных в последующем средств съема акустической информации.

Существующие средства защиты акустической информации по вибрационным каналам представляют собой генераторы шума (белого или окрашенного) речевого диапазона частот в комплекте с вибропреобразователями пьезоэлектрическими или электромагнитными. Основное назначение их — создание шумовых помех средствам съема информации в стенах, окнах, инженерных коммуникациях. Основной критерий обеспечения защиты — превышение шума над уровнем наведенного в эти конструкции информативного сигнала. Нормы превышения определены соответствующими нормативно-техническими документами.

Прежде всего несколько определений:

Определение

- "белый" шум – имеет равномерный спектр в полосе частот речевого сигнала;
- "окрашенный" шум – формируется из "белого" в соответствии с огибающей амплитудного спектра скрываемого речевого сигнала;
- "речеподобные" помехи – формируются путем микширования в различных сочетаниях отрезков речевых сигналов и музыкальных фрагментов, а также шумовых помех, или формируется из фрагментов скрываемого речевого сигнала при многократном наложении с различными уровнями.

Помехи типа "белого" шума реализованы в большинстве существующих систем и средств защиты речевой информации, таких как "ПОРОГ-2М" (НИИСТ МВД РФ), ANG-2000 (Research Electronics, США), NG-006D (ИИКМЦ-1, Россия), "Базальт-4 ГА" (Укр-СпецТехника, Украина) и др.

Помехи типа "окрашенного" шума используются в таких системах, как "Кабинет" (Элерон, Россия), "Барон" (НЕЛК, Россия).

Формирование "речеподобной" помехи применено в изделиях "Эхо" (ЭНСАНОС, Россия), ПМ-2А (НИТ, Украина).

Сравнительная оценка эффективности различных видов помех, проведенная специалистами, натолкнула на ряд особенностей применения каждой из них. Исследования показывают, что ограждающие конструкции и поверхности обладают неодинаковым акустическим сопротивлением на различных частотах, кроме того, вибропреобразователи также имеют свои конструктивные особенности, влияющие на частотные характеристики. В результате оказывается, что для оптимальной настройки сигнала помехи, обеспечивающего заданный уровень превышения помехи над информативным сигналом на отдельных частотах из-за неправильно сформированной амплитудно-частотной характеристики приходится ставить достаточно высокий уровень помехи. Это приводит к тому, что уровень паразитных акустических шумов на отдельных частотах может быть очень высоким и приводить к дискомфорту для людей, работающих в выделенном помещении.

Этот недостаток прежде всего присущ помехе типа "белый" шум.

Для формирования "окрашенного" шума, сформированного из "белого" в соответствии с огибающей амплитудного спектра скрываемого речевого сигнала, в пяти октавных полосах диапазона 100 – 6000 Гц производится оценка параметров речевого сигнала и осуществляется корректировка уровня шума в тех же полосах с помощью встроенных эквалайзеров. Таким образом, обеспечивается энергетическая оптимальность помехи, при которой заданное нормированное соотношение "сигнал/помеха" выдерживается в пределах всего диапазона частот защищаемого речевого сигнала. В некоторых комплексах эта задача решается разделением уровней по каждому из выходов. Это позволяет использовать комплекс для одновременного зашумления различных ограждающих конструкций, инженерных коммуникаций, окон и т.п., обладающих неодинаковыми сопротивлением и звукопроводящими свойствами.

Наиболее перспективным оказалось формирование "речеподобной" помехи. ***Специалистами в основном предлагается создание трех видов такой помехи:***

- "речеподобная помеха — 1" — формируется из фрагментов речи трех дикторов радиовещательных станций при примерно равных уровнях смешиваемых сигналов;
- "речеподобная помеха — 2" — формируется из одного доминирующего речевого сигнала или музыкального фрагмента и смеси фрагментов радиопередач с шумом;
- "речеподобная помеха — 3" — формируется из фрагментов скрываемого речевого сигнала при многократном их наложении с различными уровнями.

Анализ исследований показал, что наибольшей эффективностью из всех существующих обладает именно "речеподобная помеха — 3" (см. рис.)

Кривая зависимости коэффициента разборчивости речи W, используемого в качестве показателя эффективности помехи, от отношения "сигнал/помеха" Q для "речеподобной помехи — 3" свидетельствует о воз-

можности значительного (на 6–10 дБ) по отношению к другим видам помех снижения требуемого уровня сигнала помехи для достижения заданной эффективности защиты речевой информации и, следовательно, повышения комфортности ведения конфиденциальных разговоров.

Интересно

Специалистами в области технической защиты информации В.М. Ивановым и А.А. Хоревым предложен способ формирования коррелированной по уровню, спектру и времени излучения со скрываемым сигналом "речеподобной" помехи, заключающейся в специальном преобразовании скрываемого речевого сигнала за счет сложной инверсии спектра и акустической псевдореверберации путем умножения и деления его частотных составляющих и многократного наложения принимаемых переотраженных акустических сигналов.

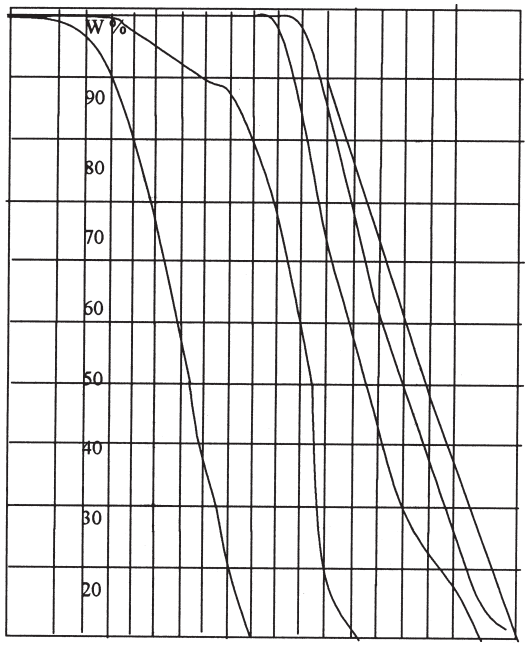


РИС. *Зависимость коэффициента разборчивости речи W от отношения "сигнал/помеха" Q для различных видов помех.*

В НПП "ЭНСАНОС" разработано устройство "Эхо", в котором реализован предложенный способ формирования "речеподобных" помех. Устройство содержит микрофонный модуль и активные акустические колонки со встроенным специальным блоком обработки речевых сигналов и предназначено для установки в выделенных для проведения конфиденциальных разговоров помещениях. Диапазон частот маскирующей помехи составляет 250-8000 Гц. Электропитание устройства осуществляется от электросети 220В или внешней батареи аккумуляторов (12В; 2,2 А/ч). Принцип действия устройства заключается в следующем.

Микрофон, как правило, устанавливаемый в центре стола, принимает акустические речевые колебания, возникающие при ведении переговоров, и преобразовывает их в электрические сигналы, которые по соединительному кабелю подаются на специальный блок обработки.

В блоке обработки эти сигналы путем умножения и деления частотных составляющих преобразовываются в шумовые "речеподобные", усиливаются и излучаются через акустические колонки, причем уровень излучаемых сигналов помех пропорционален уровню скрываемых речевых сигналов. Коэффициент усиления уровня громкости и тембра регулируется при установке устройства.

Излучаемые шумовые "речеподобные" акустические сигналы отражаются от ограждающих конструкций помещения (стен, оконных стекол, потолка пола), предметов мебели и интерьера и через некоторое время после излучения (время задержки) принимаются микрофоном и так же, как скрываемые речевые сигналы, обрабатываются и излучаются через акустические колонки. Этот процесс многократно повторяется.

Таким образом, устройством излучается "речеподобная" помеха, являющаяся результатом многократного наложения смещенных на различное время задержки разноуровневых сигналов, получаемых путем умножения и деления частотных составляющих скрываемого речевого сигнала.

Через несколько секунд после прекращения ведения разговоров в помещении генерация сигналов помех устройством прекращается.

Предварительные испытания устройства "Эхо" показали, что записанный на диктофон скрываемый речевой сигнал в условиях создаваемых устройством помех невозможно восстановить даже с использованием современных методов "шумоочистки".

К числу проблем, редко учитываемых при выборе средств защиты речевой информации, относится проблема текущего контроля эффективности виброакустического зашумления. Речь идет о непрерывной оценке качества создаваемых помех с выработкой сигналов тревоги в случае отключения помехи или снижения ее уровня ниже допустимого.

Данная проблема актуальна в связи с тем, что вибропреобразователи, излучая виброакустическую помеху, сами постоянно находятся под воздействием вибрации. Следствием этого является высокая вероятность разрушения элементов их крепления на ограждающих конструкциях защищаемых помещений, что влечет за собой снижение качества помехи.

Возможны также выходы из строя отдельных вибропреобразователей, нарушения контакта их подсоединения и другие причины, которые могут привести к снижению эффективности защиты.

Решением этой проблемы является создание распределенных систем, объединяющих как средства виброзашумления, так и средства контроля качества помех. Примерами таких систем могут служить комплекс "Барон", VNG-012.

Направленное подавление радиоэлектронных устройств (740)

Продолжаем начатый в предыдущем разделе разговор о защите речевой информации от внесенных в помещение средств несанкционированного съема информации. По периметру помещения мы защитились, применяя систему виброакустического зашумления, внутри помещения у нас издают разные неразборчивые звуки ("речеподобные" помеховые сигналы) динамики. Казалось бы, все прекрасно, но многие не любят дискомфорта, не хотят слушать доносящийся из динамиков шум или "квакающие" и "вякающие" звуки речеподобной помехи, их это раздражает, особенно это относится к несознательным руководителям высокого уровня. Кроме того, иногда хотят обеспечить защиту, не демаскируя факта применения технических средств защиты речевой информации.

Как быть в этом случае?

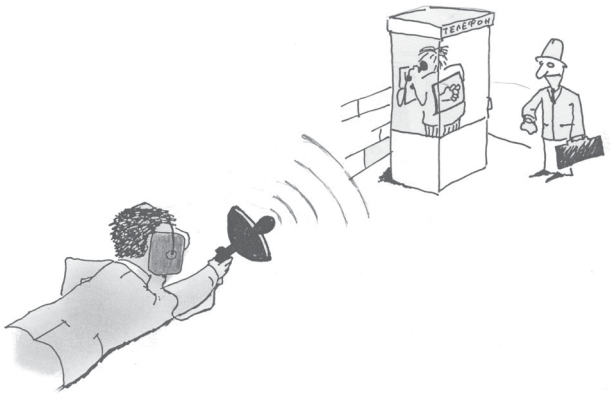
Существует великое множество генераторов высокочастотного "белого" шума, работающих в диапазоне от 10 МГц до 1200 МГц, но они могут воздействовать только на радиозакладки, да и то только широкополосные и если вам удастся разместить генератор вблизи от приемника, а это место, как правило, неизвестно. Арифметика здесь простая. Диапазон, на котором работают современные радиомикрофоны, очень велик — от 100 МГц до 1,8 ГГц. Таким образом, генератор шума должен перекрывать диапазон шириной 1,7 ГГц. Предположим, что радиозакладка имеет мощность 100 мВт, узкополосная – полоса около 2 кГц. Чтобы задавить такую закладку необходима мощность генератора в полосе 2кГц порядка 200 мВт (в два раза больше мощности радиозакладки), то на ширине полосы частот 1,7 ГГц – потребуется мощность 170кВт. Не уверен, что у Вас будет шанс выжить рядом с таким шумогенератором.

Большинство выпускаемых сегодня генераторов, работающих в данной полосе частот, имеют максимальную мощность 15–20 Вт при круговой поляризации антенной системы, но и при такой мощности после включения генератора начинают вблизи "шипеть" все бытовые радиоприемники, магнитолы и некоторые телефоны, "снежить" телевизоры, "моется" и дрожит изображение на мониторах компьютеров. Кроме того это не безвредно для здоровья окружающих. Поэтому применение таких шумогенераторов очень ограничено.

В силу изложенных объективных причин наиболее перспективным является препятствование функционированию звукозаписывающей и ретранслирующей аппаратуры с помощью направленного подавления. Этот метод реализован в таких изделиях, как "Шумотрон", "Шторм", "Буран", "Рамзес", "Бастион" и др.

Эти устройства позволяют скрытно сделать неразборчивой запись на аналоговые или цифровые диктофоны, но и подавить работу практически всех радиоэлектронных устройств, в том числе радиозакладок, попадающих в диаграмму направленности излучателя.

Идея направленного подавления заключается в формировании с помощью направленной антенной системы достаточно мощного СВЧ излучения, сфокусированного в некоторой области. Это позволяет не создавать помех окружающей радиоэлектронной аппаратуре вне этой области, и значительно снижает необходимость рассеивания больших энергетических мощностей. При внесении в эту область любого проводника на нем наводится ЭДС, пропорциональная напряженности электрического поля, создаваемого генератором. Излучаемый СВЧ сигнал промодулирован низкочастотным импульсным сигналом. В результате прямого детектирования на нелинейных элементах цепей радиоэлектронных устройств наведенный сигнал также будет иметь низкочастотную составляющую.



Направленное подавление...

Таким образом, в зоне подавления, в цепях любого электронного устройства наряду с полезным сигналом возникает превышащий его по мощности наведенный помеховый сигнал, который, проходя через цепи АРУ и усиливаясь, подавляет полезный сигнал. Следовательно, на выходе устройства записи или ретрансляции речевой информации получается помеховый сигнал.

Источником помехового сигнала подавителей типа "Шторм", "Шумотрон", "Буран" является импульсный генератор СВЧ излучения с рабочей частотой порядка 900 МГц, причем выходной сигнал генератора представляет собой псевдослучайную последовательность импульсов с переменной скважностью и минимальной частотой около 2 кГц. Такой способ формирования помехи, с одной стороны, практически не позволяет подобрав аналогичную последовательность импульсов и пустив ее в противофазе, выделить полезный сигнал; с другой стоны, импульсный сигнал, являясь широкополосным, надежно маскирует полезный сигнал и не допускает возможности отфильтровывания.

Выходная мощность генераторов составляет от 15 до 100 Вт в импульсе и длина волны помехового излучения, сопоставимая с размером проводников в цепях носимых звукозаписывающих и ретранслирующих устройств, позволяют навести на проводниках подавляемого устройства ЭДС, достаточную для снижения разборчивости речи практически до нуля.

Для обеспечения подавления звукозаписывающих устройств независимо от их расположения, вертикального или горизонтального и на достаточном удалении, в подавителях используются специальные антенные системы, которые позволяют формировать электромагнитную волну с эллиптической или круговой поляризацией, обеспечивающей диаграмму направленности 60-80 градусов в горизонтальной и вертикальной плоскости.

Уровень боковых лепестков значительно снижен до минус 12−минус 16 дБ, ось главного лепестка диаграммы направленности перпендикулярна к плоскости антенной системы (для подавителей типа "Шумотрон", "Шторм").

При этом дальность подавления оказывается даже для диктофонов в металлическом корпусе не менее 2−4 метра. Любой дополнительный проводник, подключенный к диктофону, например, выносной микрофон, пульт ДУ, а также пластмассовый корпус устройства, только усиливают эффект подавления и дальность увеличивается.

Специальные медицинские исследования, проведенные в частности с подавителями "Шумотрон-3", "Шторм" показали, что плотность потока излучаемой энергии, в соответствии с санитарными нормами, допускают нахождение в области основного лепестка диаграммы направленности, на расстоянии до 1 метра в течение 45 минут, на расстоянии 1,5−2 метра до 1 часа в сутки, что с точки зрения оперативного применения вполне достаточно. В направлении боковых лепестков и сзади антенной системы плотность потока энергии не более 10 мкВ/кв.см, что совершенно безвредно для человека.

Кроме того, большинство подавителей имеют систему дистанционного управления, осуществляющего включение и выключение генератора по радиоканалу, что дает возможность скрытно включать и выключать его только в момент ведения конфиденциальных переговоров.

Конструктивно подавители выполняются обычно в виде отдельных блоков генератора и антенной системы, что позволяет использовать их как в стационарном, так и в мобильном вариантах (атташе-кейс, саквояж, портфель, и т.д.). Есть варианты камуфлированного исполнения, например музыкальный центр, ПК и др.

Снятие информации, передаваемой по линиям пейджерной связи

В настоящее время разработаны и изготавливаются в России и в Украине программно-аппаратные комплексы мониторинга пейджерных сообщений, действующих на территориях стран СНГ системах радиопейджинга стандарта POCSAG, FLEX, и др.

В состав комплексов входят: ПК, специальное программное обеспечение, устройство преобразования и приемное устройство. В качестве приемного устройства обычно используют доработанные сканеры (AR3000, AR8000, IC-7100 и др.), радиостанции или приемники пейджеров.

Комплекс позволяет осуществлять прием и декодирование текстовых и цифровых сообщений, передаваемых в системе радиопейджинговой связи и сохранять все принятые сообщения с указанием даты и времени передачи

на жестком диске персонального компьютера в архивном файле. При этом может производиться фильтрация потока сообщений, выделение данных, адресованных конкретно одному или ряду абонентов по априорно известным или экспериментально определенным кеп-кодам. Параметры списков контролируемых абонентов можно оперативно изменять.

Снятие речевой информации с последующей передачей ее по радиоканалу (радиомикрофоны) (210)

Радиомикрофоны являются самыми распространенными техническими средствами съема акустической информации. Их популярность объясняется простотой использования, относительной дешевизной, малыми размерами и возможностью камуфляжа. Разнообразие радиомикрофонов или, так называемых "радиозакладок" столь велико, что требуется отдельная классификация. Радиомикрофоны подразделяют на:

- радиомикрофоны с параметрической стабилизацией частоты;
- радиомикрофоны с кварцевой стабилизацией частоты;

Параметрическая стабилизация частоты не может претендовать на высокое качество передачи из-за ухода частоты в зависимости от места расположения, температуры и других дестабилизирующих факторов (особенно, если радиомикрофон выполнен как носимый вариант и размещается на теле человека). Кварцевая стабилизация частоты или как называют часто специалисты "кварцованные закладки" лишены этого недостатка.

Радиозакладки работают как обычный передатчик. В качестве источника электропитания радиозакладок используются малогабаритные аккумуляторы. Срок работы подобных закладок определяется временем работы аккумулятора. При непрерывной работе это 1–2 суток. Закладки могут быть весьма сложными (использовать системы накопления и передачи сигналов, устройства дистанционного накопления).

Простейшие радиозакладки включают три основных узла, которые определяют их тактико-технические возможности. Это: микрофон, определяющий зону акустической чувствительности радиозакладки; собственно радиопередатчик, определяющий дальность ее действия и скрытность работы; источник электропитания, определяющий время непрерывной работы.

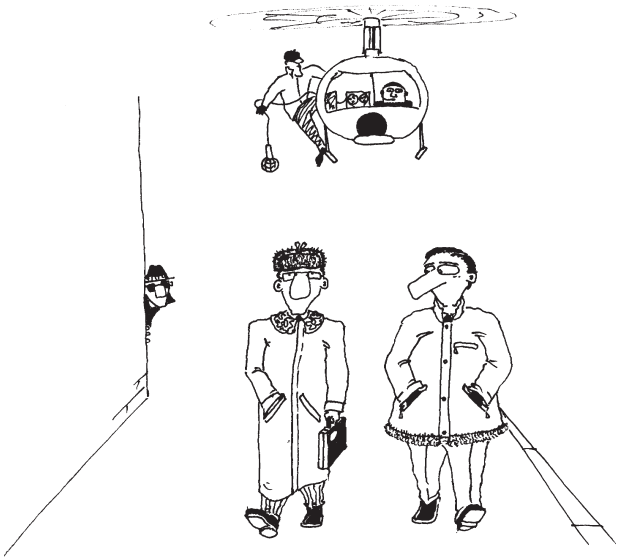
Скрытность работы радиозакладок обеспечивается небольшой мощностью передатчика, выбором частоты излучения и применением специальных мер закрытия. Часто рабочую частоту выбирают вблизи несущей частоты мощной радиостанции, которая своими сигналами маскирует работающую закладку

Из этого краткого описания следует, что дальность действия, габариты и время непрерывной работы очень взаимосвязаны. В самом деле, для увеличения дальности надо поднять мощность передатчика, одновременно возрастает ток потребления от источника питания, а значит сокращается время непрерывной работы. Чтобы увеличить это время, увеличивают емкость батарей питания, но при этом растут габариты радиомикрофона. Кроме того, следует учитывать, что увеличение мощности передатчика снижает его скрытность, то есть его легче обнаружить применяя даже не очень сложную и дорогую поисковую технику.

Закрытие радиоканала применяют различных видов: скремблирование (шифрование) передаваемого сигнала методом аналоговой маскировки сигнала в виде инверсии низко-частотного спектра или адаптивной дельта-модуляции информационного сигнала с добавлением цифрового псевдослучайного потока. Радиомикрофоны с закрытым каналом труднее обнаруживаются даже с применением дорогостоящих поисковых технических средств, но и цены на радиомикрофоны с закрытым каналом значительно выше.

Используемые в радиозакладках микрофоны могут быть встроенными или выносными.

Физическая скрытность радиозакладок определяется тщательной их маскировкой в контролируемом помещении. Однако в каждом помещении имеется целый ряд устройств, которые выглядят вполне безобидно и могут находится на видном месте, не вызывая даже малейшего подозрения, потому что чаще всего радиомикрофоны изготавливаются в камуфлированном виде (авторучки, зажигалки, картонки, предмет ы интерьера и т.д.)



Радиомикрофоны просты в использовании

Дальность действия радиомикрофонов в основном зависит от мощности передатчика, несущей частоты, вида модуляции и свойств приемного устройства.

Время непрерывной работы во многом зависит от организации питания изделия. Если радиомикрофон питается от сети 220 В, а такого типа “закладки” чаще всего выполняются в виде тройников, розеток, удлинителей, то время работы не ограничено. Если питание осуществляется от батареек или аккумуляторов, то выход из положения находят в применении режима акустопуска (управления голосом), использования дистанционного управления (ДУ) включением или увеличением емкости батарей.

Приемные устройства (214)

Прием сигналов с радиомикрофонов осуществляется на стандартные FM-радиоприемники или специально изготовленные контрольные пункты с возможностью звукозаписи.

Чаще всего для приема акустических сигналов от радиомикрофонов применяют сканирующие приемники (сканеры) типа AR3000A, AR2700, AR8000, IC-R10, IC-R2 и целый ряд других. Используют также бытовые радиоприемники с установленным конвертером для приема сигналов в нужном диапазоне частот. Предпочтительным является применение магнитол, т.к. появляется возможность одновременного одновременного прослушивания и ведения записи. Для приема от радиомикрофонов с закрытым каналом используют приемники с конвертером и демаскиратом типа инверсия или декодером сигнала с цифровой дельта-модуляцией.

Сканирующие приемники и создаваемые на их основе комплексы , кроме функций обычного радиоприема, выполняют радиомониторинг широкого спектра радиочастот. Совместно с программами управления они обеспечивают в автоматизированном и автоматическом режимах отображение радиообстановки на экране компьютера, накопление информации о принимаемых сигналах, анализ текущей и архивной информации с формированием отчетов о проделанной работе.

Они выполняют следующие задачи:

- выявление излучений специальных технических средств несанкционированного съема информации и их локализацию;
- выявление информативных побочных электромагнитных излучений и наводок, возникающих при работе вычислительной техники, средств связи, оргтехники;
- оценку эффективности использования технических средств защиты информации;
- контроль выполнения ограничений и соблюдения дисциплины связи при использовании открытых каналов радиосвязи радиоэлектронными средствами;
- контроль сеток частот различных систем радиосвязи;
- накопление данных по радиоэлектронной обстановке в точке приема и обнаружение новых сигналов;
- контроль списка фиксированных частот радиоэлектронных средств с различными параметрами излучаемого сигнала;
- оценку загруженности заданных диапазонов и интенсивности использования фиксированных частот;
- оценку электромагнитной совместимости РЭС;
- анализ индивидуальных особенностей спектра отдельного радиосигнала.

Лазерный съем речевой информации (214)

Для дистанционного перехвата информации (речи) из помещений иногда используют лазерные устройства. Из пункта наблюдения в направлении источника звука посылается зондирующий луч. Зондирующий луч обычно направляется на стекла окон, зеркала, другие отражатели.

Все эти предметы под действием речевых сигналов циркулирующих в помещении колеблются и своими колебаниями модулируют лазерный луч, приняв который в пункте наблюдения, можно путем несложных преобразований восстановить все речевые сигналы, циркулирующие в контролируемом помещении.

На сегодняшний день создано целое семейство лазерных средств акустической разведки. Такие устройства состоят из источника излучения (гелий-неоновый лазер), приемника этого излучения с блоком фильтрации шумов, двух пар головных телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Съем речевой информации с оконных рам с двойными стеклами с хорошим качеством обеспечивается с расстояния до 250 метров. Такой возможностью, в частности, обладает система SIPE LASER 3-DA SUPER производства США.

Однако на качество принимаемой информации, кроме параметров системы оказывают влияние следующие факторы:

- параметры атмосферы (рассеяние, поглощение, турбулентность, уровень фона);
- качество обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды — грязь, царапины и пр.);

- уровень фоновых акустических шумов;
- уровень перехваченного речевого сигнала.

Кроме того, применение подобных средств требует больших затрат не только на саму систему, но и на оборудование по обработке полученной информации. Применение такой сложной системы требует высокой квалификации и серьезной подготовки операторов.

Из всего этого можно сделать вывод, что применение лазерного съема речевой информации дорогое удовольствие и довольно сложное, поэтому надо оценить необходимость защиты информации от этого вида разведки.

Мероприятия по технической защите информации (640)

Мероприятия по технической защите информации можно условно разделить на три направления: пассивные, активные и комбинированные.

Пассивная защита подразумевает обнаружение и локализацию источников и каналов утечки информации. ***Активная*** — создание помех, препятствующих съему информации. *Комбинированная* — сочетает в себе использование двух предыдущих направлений и является наиболее надежной.

Однако пассивная и активная защиты уязвимы в некотором смысле. Например, при использовании исключительно пассивной защиты приходится проводить круглосуточный мониторинг, так как неизвестно, когда включаются средства съема, или теряется возможность использовать оборудование обнаружения при проведении деловой встречи.

Совет

Активная защита может заметно осложнить жизнь людям, ведущим наблюдение за вами, а вы можете использовать ее вхолостую, не зная точно, есть ли наблюдение. Комбинированная защита позволяет устранить эти недостатки.

Как правило, при выборе средств защиты информации нужно пользоваться услугами профессионалов, которые порекомендуют оптимальный комплект техники, гарантируют работоспособность, проконсультируют по применению и методам работы.

Приобретать сразу дорогостоящий комплект аппаратуры не стоит, тем более, если у вас нет сформированной службы безопасности. Достаточно приобрести недорогой комплект техники обнаружения и защиты, чтобы обезопасить себя от многих неприятностей.

Если же появляются подозрения в утечке информации, то можно пригласить специалистов для проведения аттестации и проверки помещения на каналы и технику утечки информации. Такая проверка, проведенная опытными специалистами с применением большого количества разных средств обнаружения с достаточно высокой степенью вероятности, гарантирует от наличия средств снятия информации.

Предупреждение: Помните, что лучший способ снятия информации — это установка “жучков” в средствах защиты.

Кто выловит у нас насекомых? (650)

К кому следует обращаться для получения услуг по проверке помещений на наличие закладок “жучков” и обнаружения каналов утечки информации?

Помните, что существует не много компетентных фирм, являющихся действительно специалистами по поисковым работам и вообще в области технической защиты информации, будьте терпеливы в поисках одной из них, которая сможет Вам помочь. Специалисты по чистке от закладок и контрразведке обычно не указываются в телефонных справочниках и редко рекламируют свои услуги, а если и рекламируют, то в специальных журналах, на специализированных выставках и через департаменты, выдающие лицензии на право проведения таких работ.

Специалисты по технической защите информации и поисковым работам должны иметь соответствующие лицензии, работать на договорной основе и проверены. Этот вид предпринимательской деятельности лицензируется в Украине Лицензионной палатой Департамента защиты телекоммуникаций и связи Службы безопасности Украины и этот вид деятельности находится под пристальным контролем.

Лицензии на право проведения работ по технической защите информации, в том числе на поисковые работы выдаются фирмам, имеющим необходимое техническое оснащение, подготовленных специалистов, которые являются инженерами в области электроники, связи и являются персоналом, получившим специальное обучение и большой опыт работы в этой области.

Если Вам предлагают свои услуги специалисты, не имеющие лицензии, а выдают себя за бывших работников Службы безопасности, имейте в виду, что можете

“нарваться” на частных детективов не получивших квалификацию, необходимую для чистки от закладок. Их учёба, базовая подготовка и оборудование могут быть нацелены на установку устройств подслушивания, а не на их выявление и удаление.

Если у них нет лицензии — вежливо (но быстро) укажите им на дверь.

Помните всегда, что чистка от закладок есть техническая услуга и что к этому ваши местные органы правопорядка не имеют ни малейшего отношения. Подразделения охраны правопорядка не осуществляют подобных услуг для коммерческих предприятий. У них просто нет необходимого оборудования и обученности этому делу.

Кого следует избегать?

Это важно

Остерегайтесь всякого, кто пытается рекламировать себя несколько сильнее, чем это принято или тех, кто, по-видимому, пользуется услугами рекламной фирмы или же пресс агентства. Они пытаются произвести на Вас впечатление, рассказывая обо всех статьях, которые о них написаны? Настоящие специалисты проводящие поисковые работы не ищут света рампы или широкой известности, поскольку их работа эффективна, если они остаются в тени.

Необходимо, кроме того, решительно избегать тех, кто пытается убедить Вас в том, что они являются или были шпионами корпораций. Эти люди доставляют одни только трудности и им совсем не следует доверять.

Постарайтесь выяснить, действительно ли лицо, с которым Вы говорите, оказывает TSCM услуги. Это важно, поскольку многие фирмы используют для этого дела продавцов, которые ничего не смыслят в TSCM (но кажутся знающими). TSCM команды этих фирм являются затем в составе плохо оснащённых техников, которые не имеют ни малейшего понятия о том, что они делают (часто они работают в лабораторных халатах с пистолетами в кобурах под мышкой, чтобы казаться более “устрашающим”). Используемое ими оборудование может выглядеть неплохо и сама команда может выглядеть искушённой,.но на самом деле они о TSCM не знают ничего.

Интернет: по материалам фирмы Granite Island Group, из сайта, созданного James M. Atkinson, Communications Engineer.

Ищите кого-нибудь с хорошей базовой технической подготовкой, а не с базовой подготовкой в сфере охраны правопорядка или проведения расследований.

Будьте готовы истратить значительную сумму денег за небольшую однодневную работу (плюс издержки), и конфиденциальную консультацию с разработкой рекомендаций по защите информации по результатам инспекции. Стоимость работ высока из-за высокой стоимости используемой при проверке аппаратуры и больших затрат на подготовку специалистов.

Организация проверки объектов ИС на наличие “жучков” (750)

Типовой план проверки объекта

1. Постановка задач обследования объекта:
   изучение объекта;
   определение вероятного злоумышленника, оценка его оперативных и технических возможностей по проникновению в объект с целью съема информации;
   составление плана проведения поиска, подготовка методик поисковых работ и необходимой аппаратуры;
2. Оценка системы защиты объекта:
   ознакомление с планом размещения и окружения объекта;
   оценка состояния охраны объекта, режима допуска и работы в здании, в помещениях; порядок ремонта помещений, мебели, оргтехники; оценка наличия и состояния защитной техники.
3. Контроль окружения объекта:
   определение места для организации контрольного пункта;
   контроль радиоэфира;
   контроль парковки автомашин и т.д.
4. Визуальный осмотр объекта:
   осмотр труднодоступных мест, полостей, плинтусов;
   разборка электро- и телефонной арматуры;
   осмотр электрощитов, стояков, вводов;
   вынос электронной техники.
5. Аппаратный контроль объекта:
   Поисковый радиомониторинг;
   Проверка проводных коммуникаций
6. Проверка электронной техники:
   поиск изменений в схеме, сравнение с эталоном;
   контроль радиоизлучений;
   исследование вероятности утечки конфиденциальной речевой информации от оборудования, установленного на объекте исследования посредством акустоэлектрических преобразований и паразитных ЭМИ.
7. Проверка мебели, интерьера:
   визуальный осмотр;
   проверка с помощью нелинейного локатора.

8. Проверка ограждающих конструкций:
   проверка смежных помещений;
   настройка на обнаружение модели;
   аппаратурная проверка.
9. Подготовка отчетной документации.

Подготовка поисковых работ (750)

Изучение объекта

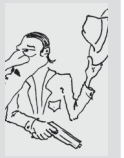
В понятие изучение объекта входит:

1. Физическое описание объекта, требующего услуг по проверке и ТЗИ, включая:
   название объекта, число комнат, число зданий, адрес и месторасположение.
2. Площадь объекта (с размером комнат и офисов).
3. Типы и число телефонов и компьютеров.
4. Список телефонных номеров (для привязки к конкретным АТС) основных и дополнительных.
5. Телефонный номер безопасных телефона и телефакса) по которому, в случае необходимости можно будет общаться представителям бригады поисковиков с клиентом.
6. Требования по форме допуска специалистов, выполняющих работы по ТЗИ.
7. Дата и номера предыдущих отчётов по поисковым работам и состояние выполнения предыдущих рекомендаций.
8. Информация, которая может повлиять на планирование выполнения работ (например, дата начала строительства здания, которое должно быть проверено, дата завершения строительства строящегося здания, выполнения ремонтных работ и т.п.)

Служебная информация (которая может дополнительно поставлена в фирму, которая будет выполнять работы по поиску закладных подслушивающих устройств и услуги в области ТЗИ):

1. Полный комплект чертежей проверяемого здания.
2. Месторасположение всех телефонных аппаратов, коммутационных коробок, шкафов и т.д. (указать на чертежах).
3. План размещения мебели в офисе/доме (обычно на чертежах).
4. Размещение всех электророзеток и выключателей
5. Тип потолков (подвесной, открытый, штукатурка и т.п.)
6. Тип телефонной системы в том числе внутренней связи (AT@T, Simens, Panasonic, Samsung, и т.п.)
7. Тип компьютерной системы (IBM, Apple, Compaq, Sun, HP, Silicon, Graphics)
8. Заметки, касающиеся последних работ по ремонту, доставки новой мебели или оборудования

Наиболее важные моменты



Если Ваш офис находится в состоянии риска, то это относится и к Вашему автомобилю и Вашей резиденции. Очень часто разведывательный агент не будет ставить закладок в офисе руководителя, а поставит их в доме или автомобиле руководителя. Это излюбленный способ действий агентов азиатской и французской разведки против бизнесменов и корпораций США.

Правильная TSCM инспекция должна включать в себя инспекцию автомобиля и частной резиденции клиента.

Интернет: по материалам фирмы Granite Island Group, из сайта, созданного James M. Atkinson, Communications Engineer.

Производится визуальный осмотр выявленных наиболее доступных мест возможной установки устройств съема информации — телефонные розетки, силовые розетки, пульты охранной сигнализации, осветительная аппаратура, блоки питания и т.д.

Виброканал

При воздействии акустического сигнала (речи) на поверхность твердых тел в них возникают вибрации, регистрируя которые можно прослушать интересующие разговоры. В качестве датчика используется вибродатчик, преобразующий вибросигналы в электрические.

Все "профи" очень любят стетоскоп, который избавил их от утомительного сверления, Он состоит

из вибродатчика с нанесенной на него мастикой для прикрепления к стене,

блока усиления с регулятором громкости и головных телефонов. Размер датчика – 2,2x0,8 см, диапазон принимаемых частот – 300...3000 Гц, вес – 126 г, коэффициент усиления – 20000. С помощью подобных средств можно прослушивать через стены толщиной до 1 м. Кроме свойств вибродатчика, на качество шума влияют толщина и материал изготовления стен, уровень шумов и вибраций в обоих помещениях, правильное место выбора расположения датчика и т.д.

Однако, так как не всегда возможно постоянно находиться в соседнем помещении, вибродатчик оснащается проводным, радио- и другими каналами передачи информации, которые аналогичны тем, которые используются с микрофонами. Преимущество вибродатчиков проявляется в том, что они могут устанавливаться не в самом, зачастую тщательно охраняемом помещении, а в соседних, на которые службы безопасности обращают гораздо меньше внимания.

(Лысов А.В., Остапенко А.Н. "Промышленный шпионаж в России. Методы и средства.")

При изучении объекта поиска следует уделить пристальное внимание расположению помещения и режиму его посещения и смежных с ним кабинетов, предполагая, что из смежного помещения, если стены не капитальные, можно просверлить слуховой канал и установить подслушивающую аппаратуру. Наличие стенных шкафов с коммуникациями в смежном помещении также дает хорошие возможности для внедрения спецтехники.

Необходимо провести осмотр помещения с целью обнаружения лишних проводов, выходящих за пределы проверяемых помещений, а также наличия устройств, в которых возможны акустоэлектрические преобразования.

Резюме

Мероприятия по технической защите информации, можно условно разделить на три направления: пассивные, активные и комбинированные. *Пассивная защита* подразумевает под собой обнаружение и локализацию источников и каналов утечки информации. *Активная* — создание помех препятствующих съему информации. *Комбинированная* сочетает в себе использование двух выше названных направлений и является наиболее надежной.

Целью изучения объекта перед проведением поисковых работ является определение вероятного злоумышленника, оценка его оперативных и технических возможностей по проникновению в объект с целью съема информации. Следует оценивать уровень злоумышленника, спецтехнику которого предполагается обнаружить.

Выбор технических средств для обнаружения закладных устройств съема акустической информации настолько разнообразен, что подобрать оптимально нужную технику не пол силу даже профессионалу. Поэтому все средства поиска делят на приборы оперативного поиска, многофункциональные приборы и на аппаратуру для непрерывного радиомониторинга и серъезного углубленного контроля.

Приборы оперативного поиска в большей степени ориентированы на конечного пользователя. Общий недостаток – наличие вероятности пропуска даже распространенных закладок.

Профессионалы работают, как правило с комплексами поисковой аппаратуры, позволяющие вести как оперативный контроль, так и радиомониторинг, а также вести поиск временно не работающих закладных устройств методами нелинейной локации, рентгеновской аппаратуры и т.д.

Выбирая средства защиты информации, необходимо руководствоваться не только их эффективностью, но и надежностью, а также уровнем комфортности их применения.

Гарантировать защищенность при приемлемых затратах могут системы, объединяющие собственно активные средства, многоканальные устройства дистанционного контроля и дистанционного управления аппаратурой виброзашумления.

Наибольшую комфортность обеспечивают средства, имеющие элементы коррекции амплитудного спектра (эквалайзеры) и использующие речеподобные помехи.

Поскольку в настоящее время задача оперативного обнаружения устройств несанкционированного получения речевой информации полностью не решена, для защиты речевой информации следует использовать направленное подавление. Аппаратура подавления должна эффективно противодействовать несанкционированному получению речевой информации на расстоянии как минимум 3–4 метров независимо от типа устройства записи или ретрансляции информации, положения его в пространстве м способа обработки сигнала, а также не создавать помех радиоэлектронным устройствам вне "зоны подавления".