Средства защиты информации

Тот факт, что информация нуждается в защите, уже давно не вызывает сомнения. С каждым годом все больше и больше предприятий считает необходимым выделять специальную статью расходов на закупку, установку и обслуживание систем защиты информации. Причем для многих уже стало очевидным, что проверка помещения – это не просто его обход с индикатором поля: каналов утечки информации гораздо больше, чем представляется с первого взгляда. Более того, бурное развитие современных технологий повлекло за собой и резкое увеличение числа мест, где циркулирует информация, в том числе и сугубо конфиденциального характера.

В данной статье мы остановимся на основных каналах утечки информации, а также предложим меры по их закрытию.

Слово — не воробей...

Существует два основных канала утечки речевой информации из помещений: акустический и виброакустический.

В первом случае информация снимается с помощью микрофонов воздушной проводимости, которые регистрируют звуковые колебания воздуха. Такие микрофоны могут быть установлены на окна, в воздуховоды вентиляций, по которым акустические колебания могут распространяться на большие расстояния, в отверстия электропроводки, трещины в строительных конструкциях и другие полости, размеры которых значительно меньше длины волны. Заметим, что акустические колебания могут быть переизлучены от стен, пола, потолка или окна, попадая таким образом за пределы помещения.

В качестве защиты от микрофонов для акустического съема используют генераторы акустического шума, например, WNG 023 и ЛГШ-302, но следует заметить, что помеха в акустическом диапазоне создает определенные неудобства при переговорах.

Кроме съема акустических колебаний, речевую информацию можно получать, регистрируя виброколебания строительных конструкций, вызванные попаданием на них акустических волн. Виброколебания обычно «снимают» с пола, потолка, стен, окон, с железобетонных конструкций, кирпичной кладки и других строительных элементов с малым коэффициентом затухания, а также с таких волноводов вибрационных колебаний, как трубы отопления, водопровода и электропитания.

В этом случае для защиты также используют генераторы шума в акустическом диапазоне, а также пьезокерамические и электромагнитные излучатели, возбуждающие вибрационные колебания в ограждающих конструкциях. Следует отметить, что уровень акустической шумовой помехи в этом случае невысок, а поэтому слышимость при разговоре не ухудшается. К наиболее известным системам виброакустической защиты относятся «Соната АВ», «Шорох-1,2,3», SEL SP-55, «Барон», «ЛГШ-40х» и ряд других.

Существует еще один вид утечки речевой информации — запись разговора на диктофон. Хотя использование этого способа и сопряжено с определенными трудностями, связанными с обеспечением скрытности установки, ограниченными ресурсами для записи и наличием общих акустических шумов, влияющих на качество записи, диктофоны достаточно широко применяются в шпионской деятельности.

Вместе с тем, при использовании кинематических и цифровых диктофонов производимая ими запись поддается подавлению. На сегодняшний день известны подавители «Сапфир», «Шумотрон-6», «Барсетка», «Бастион-GN04», «Шторм», «РаМЗес-II Соло», принцип действия которых заключается в искажении записываемой на диктофон информации до неузнаваемости путем генерации высокочастотной помехи. Для подавления записи может применяться и воздействие на магнитную ленту диктофона мощным магнитным полем, размагничивающим устройство звукозаписи, а также воздействие на микрофоны диктофона путем генерации помех в ультразвуковом или акустическом диапазоне. Тем не менее, последний способ применяется достаточно редко, так как акустическая помеха вносит достаточно высокий дискомфорт в процесс проведения переговоров.

«Алло, Вы меня слышите?»

Одним из наиболее удобных устройств для переговоров по-прежнему является телефон. Но одновременно телефон является и наиболее доступным для прослушки прибором — ведь закладку можно установить на любом участке телефонной линии между абонентами.

Любую телефонную линию можно разделить на несколько зон, в которых возможно расположение закладки. Во-первых, это сам телефонный аппарат, затем следует участок линии до распределительной коробки, откуда сигнал по магистральным кабелям попадает на АТС, где происходит коммутация сигнала, а далее сигнал идет по многоканальным кабелям или по радиоканалу до следующей АТС.

Обычно закладку устанавливают на участке от телефонного аппарата до распределительной коробки. В зоне магистрального кабеля это тоже теоретически возможно, но такой способ используется крайне редко, так как для обнаружения нужного кабеля необходимо проникнуть в систему телефонной канализации и среди сотен проводов выбрать нужный.

Существует три основных способа съема информации, циркулирующей в телефонной среде. Первый — это установка в телефонную линию подслушивающего устройства, передающего затем информацию на высокой или низкой частоте, при этом прослушивание может происходить как при поднятой, так и при положенной трубке. Защита в этом случае производится путем отсекания низко- и высокочастотной составляющих.

Для съема информации может использоваться контактное и бесконтактное подключение к телефонной линии. Существует несколько способов контактного варианта в зависимости от места подключения: это может быть уста-

новка параллельного телефона, временное подсоединение «монтерской» трубки или же подключение к воздушной линии. В последнем случае прокладывается пара очень тонких проводков от телефонной жилы по трещине деревянного столба к месту, где находится оператор. Однако такое подключение очень легко обнаружить из-за сильного падения напряжения в линии, происходящего вследствие дополнительной нагрузки. Тем не менее, сейчас известны способы контактного подключения с компенсацией нагрузки.

Может также применяться бесконтактный (индуктивный) съем информации с последующей передачей данных на головные телефоны или записью на магнитофон. Индукционный контакт датчика не вносит изменений в телефонную линию, с чем связаны сложности в выявлении такого устройства. Однако установка датчика в случае экранированной линии нарушает экранирующую оплетку, что уже является демаскирующим признаком.

Для защиты телефонной линии применяются самые разные устройства: генераторы шума, подавители закладных устройств, системы, обеспечивающие контроль состояния телефонной линии и др. Например, многофункциональный модуль SEL SP-17/D и устройство защиты «Цикада-М» обеспечивают снижение эффективности работы подслушивающих устройств, контроль телефонной линии, защиту от высокочастотного навязывания. Системы «Референт» и «Грот» позволяют передавать информацию по телефонным каналам в зашифрованном виде, а прибор «Кобра» выжигает все гальванически подключенные закладные устройства.

Капканы в сотовых сетях

Широкое распространение сотовых телефонов привело к появлению большого количества устройств для прослушивания разговоров по «мобильникам».

Для того чтобы понять, каким образом осуществляется перехват разговоров по сотовому телефону, необходимо в общих чертах представлять структуру сетей сотовой связи. Стандартная сеть состоит из трех компонентов: радиопередатчика (то есть самого мобильного телефона), базовых станций и коммуникационного центра (Mobile Telephone Switching Office).

Коммуникационный центр назначает частоты для радиосвязи базовым станциям и радиотелефонам. Базовая станция управляет работой мобильных телефонов в пределах определенной «соты». Станция подключается к обычной проводной телефонной сети и имеет встроенные в нее преобразователи высокочастотного сигнала сотового телефона в низкочастотный сигнал обычного проводного аппарата. Раз в 30-60 минут базовая станция излучает служебный сигнал, который принимается затем телефоном, находящимся в зоне покрытия данной станции. Телефон прибавляет к сигналу свой идентификационный номер ESN и отправляет его обратно на базовую станцию, которая фиксирует положение телефона, состояние его счета и т.д. Базовая станция также выделяет свободную частоту для разговора, изменяет состояние счета и передает вызов по назначению. В том случае, если объект переходит из одной соты в другую, базовая станция автоматически ищет свободную частоту в новой соте и переключает частоту. Таким образом, на базовой станции хранятся данные о положении мобильного радиотелефона, о состоянии счета и другая информация.

Перехват сигнала сотового телефона обычно происходит на участке между мачтой, на которой установлена антенна, и движущимся телефоном. Такой перехват осуществить достаточно легко, однако в том случае, если объект в процессе разговора переходит из одной соты в другую, требуется аппаратура более высокого класса сложности, которая существует и применяется в процессе разведки.

Следует отметить, что сотовый телефон может использоваться как радиопередатчик — при проведении важных переговоров он включится на передачу, и вся информация будет поступать злоумышленнику. Также радиопередатчик может быть встроен в сотовый телефон, а передача информации будет осуществляться на частоте сотовой связи. Для противодействия таким устройствам широко применяются акустические сейфы производства компании «HEPA-C» — «Кокон» и «Ладья», которые представляют собой контейнеры, в которые помещаются сотовые телефоны. В случае изменения напряженности электромагнитного поля при включении телефона на передачу активируется генератор акустического шума и до абонента не доходит никакой речевой информации.

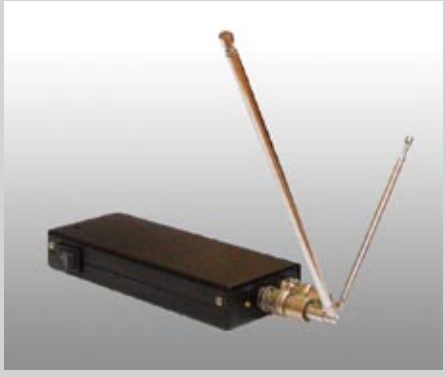
Применяются и различные блокираторы сотового телефона и подслушивающих устройств, работающих в диапазоне сотовой связи. Примерами таких устройств служат приборы «Октава-БС», «Мозаика», «Бархан», «Завеса», «С Guard», «Квартет», ЛГШ-701 и др. Такие блокираторы используются также в общественных

Система активной защиты SEL SP-21 «Баррикада»

Система активной защиты SEL SP 21 «Баррикада» предназначена для исключения перехвата информативных побочных электромагнитных излучений и наводок при обработке закрытой информации средствами офисной техники.

Устройство генерирует широкополосный шумовой электромагнитный сигнал и обеспечивает маскировку побочных электромагнитных излучений средств офисной техники, защиту от подслушивающих устройств, передающих информацию по радиоканалу.

Область использования — помещения, в которых обрабатывается информация конфиденциального характера или содержащая сведения, составляющие государственную тайну.



Система обеспечивает:

- Маскировку информативных побочных электромагнитных излучений ПК и периферийного оборудования.
- Защиту от подслушивающих устройств с радиоканалом мощностью до 5 мВт (без кварцевой стабилизации).

Конкурентные преимущества:

- Малогабаритность и наличие телескопических антенн позволяют оперативно устанавливать систему, не требует прокладки рамочных антенн по периметру помещений.
- Возможность питания от аккумуляторов позволяет использовать систему вне помещений (например, в автомобиле).
- Регулировка выходной мощности.
- Повышенная надежность работы, новый дизайн корпуса, оптимизированная цена.

Система сертифицирована во ФСТЭК России.

Универсальный анализатор проводных коммуникаций «УЛАН-2» (третье поколение)

Предназначен для поиска устройств съема информации в двухпроводных линиях любого типа даже при наличии напряжения в них.

Скоростной поисковый приемник радиосигналов «Контур»

Портативное средство радиотехнического контроля для автоматического определения сигналов, излучаемых нелегальным передатчиком (подслушивающим устройством) в диапазоне частот 30–2500 МГц.

Анализатор электромагнитного поля второго поколения «АПП-7М»

Предназначен для выявления и определения места негласно установленных источников электромагнитного излучения.

«ОМЕГА» – комплекс радиоконтроля и поиска радиопередающих устройств

Комплекс позволяет организовать постоянный автоматический мониторинг электромагнитной обстановки в одном или нескольких служебных помещениях в целях выявления вновь появившихся в них сигналов.

местах — там, где нежелательно применение сотовых телефонов (в театрах, музеях, на лекциях и т.д.). Однако следует заметить, что в мобильные телефоны часто встроен диктофон, подавление которого на данный момент проблематично.

Через объектив размером в булавочную головку

В последнее время большое распространение получил съем информации путем скрытого видео- или телевизионного наблюдения.

Размер объективов современных микровидеокамер доходит в некоторых случаях до нескольких миллиметров, что намного усложняет задачу их обнаружения и нейтрализации. Структура микровидеокамеры достаточно сложна за счет того, что полученное изображение нужно разложить на составные части для его дальнейшей передачи к месту последующего восстановления. В состав камеры обычно входят объектив, фотоприемник, устройство формирования телевизионного сигнала, устройство синхронизации, видеоусилитель и устройство передачи сигнала, аналогичное радиопередатчику в закладных устройствах. В некоторые видеокамеры встраивается также система автоматической регулировка уровня сигнала. Некоторые стационарно установленные камеры оснащены устройством дистанционного управления для увеличения времени их автономной работы. Миниатюрные видеокамеры выпускаются и в закамуфлированном исполнении — например, под дверной глазок. Существуют бескорпусные видеокамеры, которые прячутся в одежде, элементах интерьера и т.д.

На сегодняшний день существуют устройства обнаружения микровидеокамер практически любых типов, например, размещенных в стенах, потолке, сумках, причем обнаружение достигается и в том случае, если камера выключена. Таким прибором является, например, устройство «Алмаз», применяемое также для поиска оброненных драгоценных камней. Существуют и более сложные по функциональным особенностям системы, например, «Мираж-1200», которая позволяет производить круглосуточное наблюдение за объектом и подает сигнал в случае появления видеокамеры. Такие устройства также активно применятся при проведении антитеррористических операций, так как позволяют выявлять винтовки снайперов, снабженные оптическим прицелом.

Не указан класс устройств, которые могут выявлять работающие видеокамеры не по оптическому признаку, а по признаку наличия электромагнитного излучения (изделие «Амулет»). Это удобно, когда надо определить наличие работающих камер, не заходя в помещение, или засечь начавшую работать камеру во время переговоров и т.п. Подробнее можно почитать в прилагаемой статье.

«Жучки» с неограниченным ресурсом

Одним из основных каналов утечки информации является сеть электропитания 220 В, которая может использоваться и как канал для передачи перехваченной информации, и для размещения в ней закладных устройств. При этом «жучки», встроенные в сеть, обычно и питаются от нее. Часто такие закладные устройства бывают закамуфлированы под тройники, розетки, удлинители, настенные лампы т.д. А время их работы практически не ограничено — до тех пор, пока существует сеть. Некоторые устройства снабжены дистанционным управлением, причем есть возможность их перестройки по частоте и регулировки мощности. Также имеется возможность снятия информации, протекающей в заземляющих проводниках, в экранирующей оплетке кабелей локальных вычислительных систем.

Устройства защиты сети переменного тока разделяются на 2 группы: сетевые фильтры и генераторы шума.

Генераторы шума в сети электропитания создают маскирующий сигнал в цепи и таким образом защищают информацию, обрабатываемую средствами оргтехники, от утечки по сети электропитания. Кроме того, эти приборы подавляют устройства несанкционированного съема информации, использующие в качестве канала передачи цепи электропитания 220 В. Примерами техники такого типа можно назвать генераторы SEL SP-41/C, «Соната-РС-1», ЛГШ-220, работа которых не вносит помех в работу средств оргтехники.

Второй группой защитных устройств являются сетевые фильтры, которые обеспечивают защиту сети от несанкционированной передачи по ней перехваченной информации и предотвращают утечку информативных сигналов от оргтехники. Сетевые фильтры работают по принципу ослабления любых сигналов в диапазоне 0,01-1000 МГц с эффективностью 60 дБ. Эти функции успешно выполняют фильтры серий ФП, ФСПК, ФАЗА, ЛФС и др.

Около 1-2% информации, обрабатываемой на персональных компьютерных системах и различных средствах оргтехники, утекает через канал побочных электромагнитных излучений и наводок (ПЭМИН).

С одной стороны, может показаться, что объем возможной утечки невелик, однако не стоит забывать о том, что обычно информация, обрабатываемая на компьютере, имеет довольно-таки высокую степень важности, а следовательно, представляет большой интерес для злоумышленника.

Рассмотрим на примере, что является побочным электромагнитным излучением. Любая компьютерная система имеет в своем составе монитор, при этом видеосигнал на кинескоп передается по проводникам, вокруг которого существуют электромагнитные поля, которые можно фиксировать, — это и есть побочное электромагнитное излучение. Помимо монитора, побочные электромагнитные излучения создают также головки накопителей на гибких и жестких магнитных дисках, кабели, элементы электрических схем и т.д.

Защита информации за счет утечки из-за ПЭМИН обычно осуществляется за счет создания широкополосной электромагнитной шумовой помехи. Этот принцип реализован в устройствах SEL SP-21 «Баррикада» и «Бриз» с регулируемым уровнем излучения, в генераторе шума с рамочной антенной ГШ-1000М, ГШ-К-1000М, ГШ-2500, ЛГШ-501, Гном-3 и других приборах.

От шпионских ушей лучше избавиться заранее...

Очевидно, что гораздо легче выявить закладное устройство, чем защититься от него. Существует целый ряд систем, предназначенных именно для этой цели: от простых индикаторов электромагнитного поля до комплексных систем радиомониторинга, универсальных поисковых приборов и анализаторов проводных линий.

Простейшими приборами, предназначенными для выявления несанкционированно установленных радиопередатчиков, являются индикаторы поля. Эти приборы работают на принципе выявления мест с повышенной концентрацией электромагнитного поля, которая возникает при передаче информации, регистрируемой закладкой, за пределы помещения. При приближении к закладке возрастает и уровень электромагнитного излучения.

Еще одним демаскирующим признаком радиозакладки является появление нового источника излучения в свободном частотном диапазоне. Для регистрации этого события должен производиться периодический (а лучше постоянный) мониторинг радиоэлектронной обстановки. В ряде закладных устройств используются направленные антенны, что приводит к существенной неравномерности уровня излучения, и это может использоваться для выявления закладки.

В некоторых индикаторах поля реализован принцип акустической завязки: оператор, осуществляющий поиск закладного устройства, слышит шум помещения или свой собственный сигнал, отраженный от «жучка». Также одним из признаков закладок является их периодическое включение — «жучки», имеющие систему дистанционного включения, будут включаться на передачу только во время ведения важных переговоров или же отключаться ночью.

Индикаторы поля различаются также наличием или отсутствием частотомера, диапазоном частот, чувствительностью, наличием или отсутствием режима акустозавязки, видами индикации, конструктивным исполнением (в том числе камуфляжем), а также возможностью измерения частоты излучения. Примеры камуфлированных индикаторов — «ДИ-К», «Спутник», «Ekostate», SEL SP-71/M «Оберег», «Комар». Некамуфлированные индикаторы поля — ИЭП, SEL SP-75 Black Hunter с тремя режимами работы (сторожевой, поисковый и режим акустозавязки), ST 007, принцип действия которого основан на широкополосном детектировании электрического поля, и ряд других подобных приборов.

Следует отметить, что не во всех случаях индикаторы поля могут обеспечить гарантированную детекцию подслушивающих устройств. Часто уровень помех в обследуемом помещении оказывается настолько высок, что приходится снижать порог чувствительности индикатора, а это, в свою очередь, приводит к пропуску закладных устройств. Поэтому в некоторых случаях предпочтительнее пользоваться более сложными системами поиска «жучков», такими как анализаторы проводных линий, системы радиомониторинга, различными поисковыми приборами.

Анализаторы проводных линий предназначены, как видно из названия, для обследования различных проводных коммуникаций с целью выявления установленных в них закладных устройств. Работа приборов этой группы основана на нескольких принципах. Например, приборы «Отклик-2» и «Рейс-105» проводят поиск неоднородностей в телефонных линиях, периодически измеряя техниче-

ЛГШ-701

Мультистандартный блокиратор сотовой связи.
Три независимо регулируемых диапазона.
Эффективный радиус подавления – от 3 до 50 м
Возможно подключение выносных направленных антенн.
Сертификат ФСТЭК России.
Заключение Роспотребнадзора.

ЛГШ-702

Блокиратор активности устройств, работающих в стандартах Bluetooth и WiFi.
Регулировка мощности.
Эффективный радиус подавления – 10–15 м.
Сертификат ФСТЭК России.
Заключение Роспотребнадзора.

ЛПА-101 «РИМП»

Импульсный рефлектометр для проверки проводных линий.
Высокая точность измерений.
Протяженность контролируемых линий – до 50 км.
Автономная работа.
Память на 100 рефлектограмм.
Режимы сравнения и вычитания.
Сертификат ФСТЭК России.

ские параметры линии. Эти приборы могут детектировать и наличие датчика в линии, непосредственно не контактирующего с ней. Также существуют приборы, проводящие поиск нелинейностей в линии и способные не только выявлять закладные устройства, но и определять их характер и расстояние до места установки. Импульсный рефлектометр «РИМП» может проверять линии длиной до 50 км и проводить в них измерения с высокой точностью.

В настоящее время активно применяются универсальные поисковые приборы, производящие комплексную проверку всех коммуникаций. Примерами являются устройство ST 031 «Пиранья» производства компании «Смерш Техникс», ST 032, совмещающее в себе функции детектора-частотомера, сканирующего анализатора проводных линий, детектора инфракрасных и низкочастотных излучений и ряд других.

Поскольку возможности индикаторов поля не всегда являются достаточными в условиях сложной радиомагнитной обстановки, в некоторых случаях рекомендуется применять скоростные приемники типа SEL SP-81 «Оракул», «Скорпион» или системы радиомониторинга типа RS-Turbo, «Сапсан», «Акор» и др. Возможности скоростных приемников расширены по сравнению с детекторами поля, однако работать с ними проще, чем с универсальными поисковыми приборами.

Приемник проводит сканирование диапазона излучений и в случае обнаружения сигнала индуцирует его частоту и уровень. Кроме того, в «Оракуле» имеется встроенный корреляtор для сравнения демодулированного радиосигнала с опорным акустическим, присутствующим в помещении, что облегчает поиск закладных устройств. Системы радиомониторинга проводят комплексный анализ радиоэфира для поиска возможных каналов утечки информации.

Одними из наиболее интересных приборов по выявлению каналов утечки информации являются локаторы нелинейностей. Их отличительная особенность — способность обнаруживать неработающие радиопередающие устройства. Нелинейные локаторы предназначены для выявления полупроводниковых элементов, входящих в состав радиопередающих устройств, то есть для детекции закладок, находящихся как в работающем, так и в выключенном состоянии. Следует отметить, что p-n переходы могут происходить и при так называемых контактах со слабым прижимом (например, при соприкосновении скрепок, монет и других металлических предметов, в подвергнутых коррозии металлах). В этом случае образуется промежуточный окисный слой, в котором также возможны p-n переходы, однако их вольтамперная характеристика обычно симметрична, что позволяет эффективно проводить в локаторах селекцию помех.

Физический смысл действия нелинейных радиолокаторов состоит в излучении волны с определенной рабочей частотой и отражением ее от закладки обратно на приемник локатора, причем с усилением вдвое или втрое. В качестве примеров локаторов нелинейностей можно привести локатор SEL SP-61/M «Катран» с автоматической настройкой частоты, что обеспечивает минимальный уровень помех, локаторы серии NR, «Орион», «Люкс», «Лорнет», «Мастер» и ряд других.

Как видно, существует немало способов, которыми пользуются нарушители для того, чтобы сначала «снять», а потом использовать чужую информацию в своих целях. Вот почему средства защиты должны обеспечивать закрытие всех возможных каналов утечки информации — а для этого существует достаточно большое количество разнообразных устройств, различающихся по функциональным и техническим особенностям. И чтобы быть полностью уверенным в своей защищенности, лучше всего обращаться за помощью к профессионалам.