Что нового на невидимом фронте?

Белоус И. П.
"Каталог электронной техники российского производства "Живая электроника России", том 2, 2001 г.

Промышленный шпионаж является одним из инструментов постоянно обостряющейся конкурентной борьбы в сфере экономики. О фактах подкупа и шантажа информированных сотрудников фирм и государственных чиновников с целью получения от них конфиденциальной информации мы неоднократно узнаем со страниц массовых изданий и с экранов телевизоров. А вот факты использования технических средств получения информации, как правило, не афишируются.

Дело в том, что обнародование сведений о подобных акциях может иметь самые тяжкие последствия для фирмы, против которой применялись технические методы шпионажа. Но есть специалисты, которые хорошо знакомы с фактами использования технических средств. Так, например, в одну из московских фирм, работающую в сфере безопасности, обратился коммерсант из небольшого районного центра и рассказал, что содержание его телефонных переговоров о готовящемся контракте было передано конкурентам, в результате чего он потерпел большие убытки.

В недалеком прошлом защита информации осуществлялась в рамках сохранения государственной тайны, причем работами в этой области занимались целые НИИ. Теперь же, в связи с отсутствием финансирования в промышленности, большое количество специалистов перешло в различные частные фирмы, где продолжают разрабатывать современные технические средства защиты информации, а иногда и специальные технические средства, предназначенные для ее негласного получения.

В соответствии с действующим законодательством, правом на использование специальных технических средств обладают только государственные специальные службы, однако в действительности встречаются как самодельные, так и профессиональные устройства съема информации, которые используются явно незаконно.

Радиомикрофоны, которые в обиходе часто называют 'жучками', являются самыми простыми устройствами несанкционированного получения информации, но при этом и наиболее часто используемыми. На самом деле способов получения информации существует достаточно большое количество. Попробуем определить вначале виды информации, которую можно получить с применением различных технических средств.

Визуальная информация: наблюдение за объектом, копирование (фотографирование) документов на бумажных носителях, фото- и видеосъемка объекта.

Информация, обрабатываемая и передаваемая средствами офисной техники: компьютерная информация, факсимильные сообщения, информация на бумажных, магнитных и других носителях.

Акустическая речевая информация: телефонные переговоры, разговоры,

ведущиеся в помещениях.

Выявление попыток получения визуальной информации может быть осуществлено в основном оперативным путем. Сейчас появились технические средства, позволяющие обнаруживать оптические приборы на расстоянии от нескольких метров до 1 км. Существует также очень простой в эксплуатации прибор, обнаруживающий включенные проводные видеокамеры и работающий по принципу регистрации очень слабых побочных излучений, возникающих при подаче питания на видеокамеру. Сразу оговоримся, что не стоит обольщаться и требовать от прибора чрезмерного.

Перехват информации, обрабатываемой средствами офисной техники, возможен за счет наличия побочных излучений, имеющихся практически у любого электронного устройства. Любое электромагнитное излучение может быть перехвачено с помощью специальной радиоприемной аппаратуры, однако следует учитывать, что излучения наводятся и на проводные коммуникации, распространяются по ним и могут быть перехвачены средствами разведки. Кроме электромагнитных излучений, работа некоторых средств офисной техники, например, пишущих машинок, сопровождается характерными акустическими сигналами, которые также можно перехватить и расшифровать. Перехват информативных сигналов возможен также за счет регистрации неравномерности тока потребления средствами офисной техники.

Акустическая речевая информация наиболее уязвима и перехватывается чаще всего. Виды нападения на нее можно условно разделить на прослушивание помещений и перехват информации, передаваемой по открытым каналам связи.

Информация, передаваемая по каналам связи, перехватывается или с междугородних линий, или с помощью специальных технических средств, подключаемых к абонентским линиям.

Методов прослушивания помещений значительно больше. Прослушивание возможно через строительные конструкции (стены, перекрытия, стекла) и инженерные коммуникации (различные трубопроводы и металлоконструкции). Паразитные излучения средств офисной или бытовой техники (усилителей низкой частоты, телевизоров, магнитофонов, телефонных аппаратов и т.п.) могут модулироваться речевыми сигналами и перехватываться радиоприемной аппаратурой. Характерным примером являются телефонные аппараты VEF ТА-12. Ведущиеся с их помощью переговоры можно прослушать на небольшом расстоянии даже с помощью простейших радиоприемных устройств. Прослушивание помещений, например, через телефонный аппарат при положенной трубке возможно за счет микрофонного эффекта или ВЧ-навязывания. Некоторые виды датчиков охранной сигнализации способны преобразовывать акустическую информацию в электрические сигналы, которые могут быть перехвачены. Воздуховоды, открытые окна и неплотно закрывающиеся двери могут стать каналами утечки акустической информации. Например, одна коммерческая фирма прослушивалась из подвала через трещину в полу. Наиболее опасным является прямое прослушивание помещений с использованием проводных или акустических закладок и миниатюрных звукозаписывающих устройств.

Акустические закладки можно разделить на несколько групп: по виду

модуляции, по способу передачи информации, по способу кодирования, по типу датчика, по способу включения передатчика, по типу источника питания, а также по виду исполнения.

Проводные закладки подразделяются по виду подключения, по типу питания и по способу передачи информации.

Многообразие устройств съема информации и вариантов их использования порождает множество методов обнаружения и противодействия. Не может существовать какого-либо одного прибора, способного обнаружить любые закладки, также как не существует одного устройства, защищающего информацию от всех видов перехвата.

Таким образом, для выявления различных каналов утечки информации необходимо использование некоторого набора поисковой аппаратуры, позволяющей обнаруживать не только работающие радиомикрофоны, но и оценивать возможность использования потенциальным противником другого, например, виброакустического канала.

Наиболее простыми поисковыми средствами являются индикаторы поля, предназначенные для обнаружения и локализации включенных радиопередающих устройств. Индикатор поля представляет собой широкополосный высокочастотный усилитель, к которому подключена схема индикации. Чувствительность индикаторов невелика, поэтому они не реагируют на мощные теле- и радиопередатчики. Работа с индикаторами поля вблизи телецентров затруднена, а зачастую просто невозможна. Однако по сочетанию цена/возможности эти приборы являются достаточно привлекательными для проведения оперативных проверок, а некоторые специально разработанные модели эффективно используются в сторожевом режиме для обнаружения вносимых в помещение нательных радиомикрофонов.

К следующей группе можно отнести различные радиоприемные устройства: сканирующие и скоростные приемники. Использование сканирующих приемников в ручном режиме для обнаружения радиомикрофонов малоэффективно, так как проход частотного диапазона обычно занимает очень много времени. Для этой цели разработаны так называемые скоростные приемники ближней зоны: Скорпион, RF-850, MRA-3, позволяющие быстро просканировать рабочий диапазон частот и обнаружить сигнал работающего радиомикрофона.

Аппаратуру для проверки проводных коммуникаций можно условно разделить на три группы.

Для выявления передаваемых по проводам сигналов подслушивающих устройств существуют специальные НЧ-приемники, среди которых наиболее известными являются Scanner-3 и SP-31/C.

Для проверки телефонных линий с целью выявления ранее установленных устройств съема информации разработаны такие приборы, как SP-18/T, КТЛ-400, ТПУ-6.

Наиболее эффективным для выявления гальванических подключений к проводным коммуникациям является метод нелинейной локации. Наиболее известным прибором, использующим этот метод, является АТ-2.

В начале 90-х годов американской фирмой REI был разработан универсальный поисковый прибор CPM-700 'Акула', представляющий собой

широкополосный усилитель с большим набором зондов для выявления различных каналов утечки информации. Сегодня более эффективным является разработанный в 1998 г. российской фирмой 'Смерш Техникс' универсальный поисковый прибор ST-031 'Пиранья'. Он позволяет выявлять работающие радиомикрофоны, проверять проводные коммуникации на наличие передаваемых по ним сигналов, оценивать акустику и виброакустику помещений, обнаруживать источники магнитных полей и с помощью дополнительного зонда ДАПЛ проверять средства офисной техники на наличие микрофонного эффекта. Существуют и другие более простые универсальные поисковые приборы, обеспечивающие выявление более одного канала утечки, например, ПСЧ-5, D008.

Выявить различные радиопередающие устройства можно при помощи автоматизированных комплексов радиоконтроля, таких, как АРК-Д, RS-1000, OSCOR-5000 и т.п. Эти комплексы позволяют в ручном и автоматическом режимах проводить круглосуточный мониторинг радиоэфира, регистрировать вновь появляющиеся сигналы и по нескольким параметрам оценивать их опасность. В ручном режиме можно локализовать местонахождение источника сигнала.

Для выявления активизированных устройств съема информации существует большое количество разнообразной аппаратуры, но остается группа подслушивающих устройств, которые излучают не постоянно. Это могут быть устройства с дистанционным управлением, с накоплением информации или просто с разряженными элементами питания.

Обнаружение таких устройств возможно только приборами, называемыми нелинейными локаторами, представляющими собой малогабаритную радиолокационную станцию. При попадании зондирующего луча на полупроводниковый переход происходит его преобразование и переотражение на кратных гармониках, которые регистрируются приемным устройством прибора. Наиболее известными являются приборы «Родник», NR, «Онега», «Обь». На рынке средств безопасности имеются еще несколько менее известных моделей российского производства, а также импортные модели, принципиальное отличие которых заключается в дизайне и существенно более высокой цене.

При проведении поисковых работ часто используются досмотровые средства: рентгеновские комплексы, эндоскопы, металлодетекторы и прочее вспомогательное оборудование.

Проведение поисковых работ является неотъемлемой частью работ по защите информации, но при этом не следует забывать о собственно средствах и системах защиты.

Как уже было сказано, не существует одного прибора, обеспечивающего всеобъемлющую защиту. Для обеспечения защиты какого-либо объекта (здания, помещения или их группы) требуется использование набора технических средств, обеспечивающих защиту информации от утечки по каждому из возможных каналов.

Среди средств защиты информации важное место занимают системы виброакустического зашумления: SP-51/A, VNG-006D, Заслон и т.д., обеспечивающие защиту помещений от прослушивания через элементы строительных конструкций. Такие системы состоят из генератора и

виброакустических преобразователей, а также имеют возможность подключения акустических колонок в случае необходимости. При работе таких приборов на строительных конструкциях создаются микроколебания, которые маскируют опасные акустические сигналы. Использование акустических колонок позволяет зашумить воздуховоды, тамбуры, межоконные проемы и т.д. и, соответственно, предотвратить утечку информации по акустическому каналу.

Наибольший выбор эффективных устройств защиты существует для предотвращения утечки за счет побочных излучений и наводок. Эту задачу решают генераторы шума SP-21B1, Гном-3, ГШ-1000 и другие аналогичные изделия. Но они работают только по радиоканалу, а защищать приходиться также системы электропитания и заземления и телефонные линии. Такую комплексную защиту обеспечивает только комбинированный генератор 'Заслон' (не надо путать с системой виброакустического зашумления 'Заслон').

Не стоит использовать такие генераторы для подавления радиомикрофонов, так как для решения этой задачи их мощность недостаточна. Подавление радиомикрофонов возможно имеющими существенно более высокую мощность генераторами 'Спектр', 'Равнина-5И'.

Для защиты сети электропитания, в том числе подавления сетевых закладок, возможно использование специальных генераторов SP-41/D, Цикада-С, или сетевых помехоподавляющих фильтров ФСП-1Ф-7А, ФП и т.д.

На рынке средств безопасности предлагается значительное количество устройств защиты для подавления телефонных подслушивающих устройств: SP-17/D, Прокруст, Гром-ЗИ-6 и т.д. В связи с большим разбросом параметров абонентских телефонных линий эффективность данных изделий оценить сложно. Практически все эти изделия обеспечивают снижение эффективности телефонных подслушивающих устройств и широко применяются для защиты от прослушивания телефонных переговоров.

К средствам защиты телефонных линий относятся и устройства защиты от прослушивания помещений за счет микрофонного эффекта средств офисной техники и, в первую очередь, телефонных аппаратов. Многим известны устройства серии 'Гранит', широко использовавшиеся ранее. В настоящее время выпускаются изделия: 'Корунд', МП-1А и Ц, Грань-300 и некоторые другие.

Если в помещениях установлены динамики систем оповещения или трансляционные приемники, то из-за особенностей данных устройств необходимо обязательно использовать соответствующие устройства защиты: МП-2, МП-5, МП-3.

Неизбежным при обеспечении конфиденциальных переговоров является защита от несанкционированной аудиозаписи. Имеющиеся на рынке системы обнаружения диктофонов имеют ограниченные возможности, поэтому во многих случаях более предпочтительным является использование устройств подавления, таких как «Шумотрон», «Бастион», «Рамзес» и т.д. Дальность подавления экранированных диктофонов без выносного микрофона составляет 1,5-2,5 м в зависимости от модели.

Наличие разнообразных каналов утечки информации и необходимость их защиты влечет за собой обеспечение комплексной защиты объекта. В тех случаях, если в организации имеется собственная служба безопасности,

укомплектованная специалистами, обращения за теми или иными изделиями носят, как правило, конкретный характер. При проведении работ, связанных с защитой гостайны, обязательным требованием является наличие сертификата Гостехкомиссии России на приобретаемое изделие. В некоторых случаях при этом приобретаются изделия недостаточно высокого качества, т.к. проведение сертификационных испытаний является достаточно дорогостоящей процедурой. По этой причине некоторые производители предпочитают предлагать свои изделия в основном коммерческим фирмам.

Небольшие фирмы часто не имеют собственных служб безопасности. В лучшем случае имеется сотрудник, занимающийся обеспечением безопасности параллельно, например, с телефонией. Обычно такие сотрудники не являются специалистами в области безопасности и даже не всегда могут объяснить, что именно им требуется. В таких случаях квалифицированный консультант подробно расспрашивает об основных характеристиках объекта защиты и только после этого предложит необходимый набор аппаратуры и объяснит ее назначение и функциональные возможности. Основная задача - объяснить неспециалисту, что не может существовать «маленькая коробочка за 10 $», защищающая от всего на свете.

Разумеется, в каждом конкретном случае требования по защите информации разные и оценить в среднем стоимость защиты практически невозможно, но можно привести несколько ценовых характеристик основных технических средств:

системы виброакустического зашумления (генератор и 6 вибропреобразователей) стоят 650 - 1 100 $;

генераторы зашумления сети питания - 180 – 250 $;

генераторы пространственного зашумления - 150 – 1800 $;

устройства защиты телефонных линий - 150 - 650 $;

подавители диктофонов – 1000 – 2200 $.

Те бизнесмены, которые в результате утечки коммерческой конфиденциальной информации понесли крупные материальные потери, поняли, что гораздо дешевле принять превентивные меры безопасности и на ней не экономить.