ИНСТРУМЕНТЫ БЕЗОПАСНОСТИ

Современные средства обнаружения подслушивающих устройств

Что бы там ни говорили, но подслушивать чужие разговоры, несмотря на всю предосудительность этого занятия, всегда было очень привлекательно. А **получение доступа к секретной информации во все времена являлось основной задачей любой разведки.**

Главная причина промышленного (экономического) шпионажа – стремление к реализации конкурентного преимущества, как важнейшего фактора достижения успеха в условиях рыночной экономики. Добытая информация позволяет быть в курсе дел конкурентов, использовать их научно-технические достижения и в конечном счете принимать наиболее рациональные управленческие решения. Экономический шпионаж может осуществляться в целях завладения рынками сбыта, подделки товаров, дискредитации или экономического подавления конкурентов, срыва переговоров по заключению контрактов, шантажа отдельных лиц и т. п.

Часто разведывательные мероприятия проводятся конкурентами с помощью специальных технических средств негласного получения информации (средства негласного визуального наблюдения, негласного акустического контроля, негласного съема информации с каналов связи и пр.). От незаконного негласного прослушивания (подглядывания) в общем случае не застрахован никто. И закономерной является заинтересованность хозяйствующих субъектов в сохранении собственной коммерческой тайны.

Право граждан и юридических лиц на конфиденциальную информацию, определение режима доступа к ней и способов ее защиты закреплено законодательно. Реализуя это право, граждане и юридические лица могут выявлять каналы утечки конфиденциальной информации, осуществлять поиск так называемых закладочных устройств в служебном кабинете, офисе, квартире, автомобиле и пр., использовать для этих целей средства обнаружения подслушивающих устройств.

К подслушивающим устройствам в частности и к закладочным устройствам («жучкам») вообще относятся любые технические средства, предварительно негласно размещаемые на объекте или в его коммуникациях в целях негласного получения информации (акустической, визуальной, текстовой, компьютерной).

В КАЧЕСТВЕ ЗАКЛАДОЧНЫХ УСТРОЙСТВ МОГУТ ИСПОЛЬЗОВАТЬСЯ:

- микрофоны с дистанционной передачей информации;
- стетоскопы с дистанционной передачей или накоплением информации;
- гидроакустические датчики;
- микровидеокамеры с дистанционной передачей или накоплением информации;
- эндоскопы;
- устройства съема информации с линий связи.

Этот перечень «жучков» не является исчерпывающим, поскольку появляются новые виды таких устройств.

Защита от применения закладочных устройств осуществляется по двум основным направлениям:

- поиска и обнаружения «жучков»;
- нейтрализации «жучков».

Мы рассмотрим именно средства поиска и обнаружения «жучков».

Поскольку известно огромное множество различных видов «жучков», а также вариантов их применения, их поиск и обнаружение представляют собой предмет отдельной отрасли знания. В общем случае все методы обнаружения «жучков» можно разделить на универсальные и специальные. Универсальные методы применимы для обнаружения любых «жучков», а специальные – для выявления «жучков» конкретных типов или уста-

ВЛАДИМИР НОРИК,
коммерческий директор ООО «Сюртель»

новленных в определенных условиях.

К универсальным методам обнаружения закладочных устройств относятся:

- визуальный осмотр;
- нелинейная локация;
- рентгеновское просвечивание.

Визуальный осмотр заключается в тщательном обследовании помещения, строительных конструкций, коммуникаций, элементов интерьера, аппаратуры, канцелярских принадлежностей и т. п. по специальной методике. При этом особое внимание обращают на наличие специфических признаков закладочных устройств (антенны, микрофонные отверстия и пр.). В процессе осмотра, как правило, производится необходимый демонтаж или разборка аппаратуры, средств связи, мебели, иных предметов. Специалист, осуществляющий поиск «жучков», должен быть знаком с внешним видом и конструктивными особенностями серийно выпускаемых «жучков», а также иметь представление о радиолюбительских конструкциях, кроме того, обязательно наличие опыта работы в области защиты информации.

В процессе визуального осмотра при необходимости используются досмотровые зеркала типа «Ниоген» и CSS-002 , эндоскопы типа ЭТГ и ТСГ и пр.

Метод нелинейной локации реализуется путем использования специальных приборов – нелинейных локаторов, таких как NR, «Лорнет», «Люкс», ORION (См. Рис.1) и др., и основан на специфическом свойстве полупроводниковых материалов, которое заключается в том, что при их облучении высокочастотным радиосигналом происходит преобразование его частоты в кратные гармоники с последующим переизлучением в окружающее пространство.

В отличие от большинства других методов нелинейный локатор позволяет обнаруживать:

- неработающие «жучки» (с отключенным электропитанием);
- «жучки» с дистанционным управлением, находящиеся в режиме ожидания;
- «жучки» со специальными технологиями передачи информации, служащими повышению скрытности их работы (узкополосная модуляция, передача сигналов короткими сериями после их предварительного накопления в запоминающем устройстве, использование нескольких несущих частот, различные сложные виды модуляции и пр.).

Эта особенность нелинейных локаторов имеет важное практическое значение, поскольку позволяет при проведении поисковых работ не учитывать возможность дистанционного отключения «жучков» подслушивающей стороной, а также повышает вероятность обнаружения «жучков».

Метод рентгеновского просвечивания используется в целях обнаружения «жучков» всех типов в помещениях, а также в радиоэлектронной аппаратуре. При просвечивании строительных конструкций, мебели и иных предметов в помещении используются портативные досмотровые комплексы серии «Норка», которые оснащены визуализирующим устройством.

Существует большое число специальных методов обнаружения закладочных устройств. К ним можно отнести следующие:

- индикацию электромагнитного поля;
- радиосканирование;
- радиоперехват;
- анализ параметров линий связи и проводных коммуникаций;

СРЕДСТВА ОБНАРУЖЕНИЯ ПОДСЛУШИВАЮЩИХ УСТРОЙСТВ

Рис. 1 Нелинейный локатор ORION NJE-4000
Рис. 2 Индикаторы-частотомер ST-107
Рис. 3 Спектральный коррелятор OSCOR Green

- рефлектометрию линий связи;
- инфракрасное зондирование и др.

Простейший индикатор электромагнитного поля состоит из антенны, широкополосного усилителя, амплитудного детектора и порогового устройства, которое срабатывает, если сигнал на выходе детектора превысит регулируемый пороговый уровень. Порог устанавливается так, чтобы индикатор не реагировал на внешние излучения (фон). В результате подслушивающее устройство обнаруживается только в тех точках помещения, где уровень его поля превосходит фоновый.

Некоторые устройства оснащаются простейшими средствами идентификации: звуковой выход позволяет прослушивать демодулированный сигнал и выявлять радиомикрофоны методом так называемой «акустической обратной связи», вызывающей самовозбуждение в тракте радиомикрофон – индикатор.

Для локализации источников излучения в пространстве полезны измерители уровня сигнала. Индикаторы поля отличаются небольшими размерами и массой, простотой, быстродействием и низкой стоимостью – от 7000 рублей. К ним относятся такие индикаторы поля, как SEL SP-77/2M «Ловец», SEL SP-75 Black Hunter и Bug Hunter. Однако из-за недостаточной чувствительности и избирательности они не обеспечивают требуемой достоверности обнаружения.

Индикаторы-частотомеры (SEL SP-71R Raksa, ST-107, РИЧ-8) отличаются от индикаторов электромагнитных излучений встроенным счетчиком – частотомером, который измеряет частоту радиосигнала, превысившего установленный порог, и помогает оператору идентифицировать сигнал подслушивающего устройства.

Кроме того, некоторые индикаторы, например ST-107 (Рис.2), можно подключать к компьютеру и сканирующему радиоприемнику. В этой конфигурации индикатору поручается предварительный анализ электромагнитной обстановки с последующей проверкой результатов сканером.

Существуют также камуфлированные индикаторы – «Челленджер», SEL SP 71R Raksa, которые позволяют применять их в оперативных целях.

РЕКОМЕНДАЦИИ ДЛЯ ПОИСКА «ЖУЧКОВ» С ПОМОЩЬЮ ДЕТЕКТОРОВ:

- нужно внимательно осматривать все розетки, провода и прочие места, где есть возможность подключиться к электросети, потому что «жучок», установленный в ваше отсутствие таким образом, имеет постоянное питание и может работать сколь угодно долго; это важно, потому что жизнь «жучка», работающего от батареек, ограничена;
- очень тщательно проверяйте подарки, которые вам делают деловые партнеры и просто коллеги;
- внимательно относитесь к «случайно» забытым вещам;
- во время переговоров или важных совещаний включайте фоновую музыку, это, конечно, не спасет от утечки информации, но может «забить» ваш разговор посторонним шумом;
- при осмотре помещения с помощью детекторов «жучков» не надейтесь, что из прибора выскочит стрелка и укажет вам место, где спрятан «жучок». При этом важно учитывать, что по мощности излучения «жучки» бывают разные: один имеет передатчик мощностью 5 мВт и передает сигнал на 10 м, а другой имеет передатчик мощностью 250 мВт и передает сигнал на 100 м, поэтому и дальность реагирования на них тоже будет разной – от 10 см до 5 м.

Очень тщательно проверяйте подарки, которые вам делают деловые партнеры и просто коллеги

Во многих случаях обнаружение радиопередающих устройств несанкционированного съема информации с помощью простейших приборов – индикаторов поля – бывает затруднительным из-за повышенного уровня промышленных помех, что в условиях города является вполне нормальным явлением.

Поэтому были разработаны специальные приемники ближней зоны: скоростной приемник-корелятор SEL SP-81 «Оракул» и скоростной приемник «Скорпион». Алгоритм работы этих изделий упрощен, чтобы им могли пользоваться не только профессионалы, но и люди, далекие от техники. Стоимость этих приборов составляет 30–40 тыс. руб.

Системы радиомониторинга представляют собой существенно более сложные изделия, в состав которых входят: персональный компьютер, сканирующий приемник, векторный анализатор или анализатор спектра, коммутатор, одна или несколько антенн, различные адаптеры и специальное программное обеспечение. Как правило, такие системы используются службами безопасности, в которых работают специалисты.

Одними из наиболее известных являются спектральные корреляторы Oscor-5000 и OSCOR

Green (Рис.3) производства фирмы REI (США). Среди отечественных разработок следует обратить внимание на комплексы «Эврика», «Кассандра» и «Омега», в составе которых имеется векторный анализатор, позволяющий визуально распознавать различные виды цифровых сигналов. Системы радиомониторинга предназначены для контроля состояния радиодиапазона в ручном или автоматическом режиме и выявления технических каналов утечки информации в контролируемых помещениях. Данные комплексы могут быть одно- и многоканальными, благодаря чему можно осуществлять мониторинг нескольких помещений без перемещения самого прибора. Стоимость таких комплексов на порядок выше стоимости приемников ближней зоны.

Анализаторы проводных коммуникаций предназначены для обнаружения фактов несанкционированного подключения к различным проводным коммуникациям, таким, как телефонные линии, электрические сети переменного тока, компьютерные сети, линии охранной сигнализации и т. п. Анализатор способен не только выявить и идентифицировать обнаруженные устройства, но и, используя метод импульсной локации, с высокой точностью измерить расстояние до места несанкционированного подключения. Наиболее известны анализаторы «Сириус» отечественного производства и Talan фирмы REI.

Группа приборов, включающих в себя несколько поисковых функций, получила название универсальных.

В состав этих приборов могут входить:

- индикатор поля для обнаружения радиоизлучающих устройств;
- проводной приемник для обнаружения сигналов, передаваемых по проводам;
- усилитель, позволяющий обнаруживать микрофоны, подключенные к проводам, с помощью акселерометра работать в режиме стетоскопа и оценивать проницаемость строительных конструкций и работу систем виброакустического зашумления, а с помощью микрофона – проверять системы воздуховодов;
- детектор ИК-излучений.

В тех случаях, когда у потребителя нет возможности приобретения комплекта поисковых приборов, вполне эффективно можно проводить проверку помещений с помощью таких универсальных приборов. Наиболее известны многофункциональные поисковые приборы СРМ-700 «Акула» и ST 031M «Пиранья», в зависимости от модели и модификации их стоимость варьируется от 90 000 до 140 000 руб.

Что касается обнаружения скрытых видеокамер, то здесь существуют два типа обнаружителей.

К первому типу относятся приборы, основанные на оптической локализации, которые по-

При осмотре помещения с помощью детекторов не надейтесь, что из прибора выскочит стрелка и укажет вам место, где спрятан «жучок»

зволяют обнаружить объектив видеокамеры благодаря эффекту световозвращения, или «обратного блика», характеризующемуся тем, что отраженное излучение распространяется в узком телесном угле и точно в направлении на зондирующий излучатель при однопозиционной локации. При обнаружении объектива скрытой камеры в объективе такого обнаружителя будет наблюдаться точечное световое пятно – результат отражения подсветки от видеокамеры. К таким приборам относятся «Гранат», «Оптик», «Хаббл», «Чистильщик», отличающиеся оптическими параметрами, в том числе дальностью обнаружения, что и влияет на стоимость прибора (12 000–85 000 руб.).

Второй тип – электромагнитные обнаружители SEL SP-101 «Аркан», IRIS, действие которых основано на анализе определенных участков электромагнитного спектра на предмет выявления излучений, свойственных только видеокамерам. Такие приборы предназначены для дистанционного обнаружения в помещениях и предметах скрытых видеокамер, находящихся в активном состоянии, т. е. ведущих съемку.

В заключение можно сделать вывод, что в настоящее время на рынке систем электронной безопасности имеется широкий выбор приборов, с помощью которых специалисты с высокой степенью достоверности могут обнаруживать средства несанкционированной передачи информации из контролируемых помещений. Выбор этих приборов зависит от степени подготовки специалистов и от денежных средств, выделяемых руководством на мероприятия по обеспечению безопасности своей организации. ●