УДК 681.3.004

Клименко В.А., Яковлев А.И.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ СПЕЦПРОВЕРОК

Практическая реализация обследований, направленных на устранение угроз утечки информации по акустическому каналу, сопряжена с рядом организационных и технических мероприятий. Успешное решение задачи совершенствования этих мероприятий позволяет повысить эффективность проводимого контроля уровня защищенности информации, начиная от его подготовки и до завершения.

1. Методические рекомендации по организации спецпроверок.

1.1. Разновидности проверок

Степень тщательности обследования устанавливается в каждом конкретном случае. Как правило, рекомендуется от двух до четырех глубоких проверок в год. Такая проверка обязательно включает разборку всех телефонов для их обследования, разборку всех сетевых розеток для их обследования и проверки сетевых проводов на наличие несущей,проверку всех телефонных линий, обследование всех полых пространств и подвесных потолков на наличие подозрительных проводов, проверку систем проводного вещания, громкоговорящей связи и других проводных систем. Кроме того, рекомендуется самостоятельно проводить мини-проверки не реже раза в неделю, а также перед и после каждого важного совещания. Такие мини-обследования должны включать физическое обследование всех помещений и включение прибора типа ОСКОРа (1) в автоматическом режиме для радиочастотного обследования. Мини-обследования могут выполняться сотрудниками безопасности данной организации, что будет служить как для повышения эффективности проверок, так и для отпугивания потенциальных шпионов. Кроме того, при планировании глубокой проверки, об этом должны знать только те сотрудники, без которых не обойтись. Только в этом случае можно расчитывать на обнаружение работающих закладок. Для отпугивающего эффекта следует всячески афишировать, что обследования будут проводится нерегулярно, т.е. могут состоятся в любое время. Вероятность установки подслушивающихустройств резко уменьшается, если персонал осведомлен о возможных роверках. В том случае, если необходимо осуществлять постоянный мониторинг разведобстановки, прибор типа ОСКОР можно разместить в укромном месте и установить на нем автоматический режим работы. Раз в неделю следует просматривать память ОСКОРа для выявления новых опасных сигналов и изучения их в ручном режиме с помощью функций вызоваданных.

1.2 Планирование обследования

Важно помнить, что если за Вами наблюдают, то наблюдатель может ожидать соответствующих контрмер. В большинстве случаев закладки обнаруживаются редко, но зато зачастую находятся следы того, что какая-то аппаратура подслушивания была установлена. Если наблюдателю становится известно о предстоящей проверке, то можно быть уверенным, что закладки будут изъяты, обследование ничего не даст, а подслушивание в дальнейшем может быть продолжено. Обследование часто оказывается неэффективным по следующим причинам:

- предстоящее обследование обсуждается по сомнительному телефону;
- обследование указано в плане мероприятий учереждения;

- наблюдатель увидел приход группы обследования;
- обследование выполняется после работы, хотя соответствующая аппаратура задействуется только в рабочее время;
- аппаратура обследования неисправна или используется неправильно (на рынке есть немало детекторов закладок, которые только имитируют настоящую работу, а также много дорогого оборудования от которого мало пользы;
- группа обследования работает кое-как или плохо подготовлена (самым важным компонентом в комплексе оборудования является человеческий мозг);
- обследование проводят перед совещанием, участники которого приносят с собой закладки, носимые на теле или диктофоны.

1.3 Время проведения проверки

Обследование желательно проводить во время активности закладок, т.е. в рабочее время. Это легко осуществить в конференц-залах или других помещениях с ограниченным доступом персонала. Помещения со свободным доступом персонала рекомендуется обследовать после работы или в выходные дни. Важно, чтобы проверка была проведена как можно быстрее после принятия решения, так как это сводит к минимуму риск утечки информации о готовящейся проверке.

1.4 Подготовка обстановки проверки

Благодаря тому, что некоторые приборы могут управляться дистанционно, имитация совещания может заставить наблюдателя задействовать свои устройства. Если совещание анонсируется как "очень важное", наблюдатель может даже повысить уровень аппаратуры подслушивания. Должно быть включено все офисное оборудование (кофеварки, компьютеры, лампы, ксероксы, факсы и т.д.) для того, чтобы активировать закладные устройства. Если обследование проводится в рабочее время, проверяющие должны быть одеты типично для персонала учереждения или посетителей. Оборудование для проведения проверок должно находится в стандартных кейсах.

1.5 Ограничение доступа к месту проверки.

При проведении обследования не следует допускать персонал на место ее проведения. Это не проблема, если обследование проводится после работы. При проверке в рабочее время следует выставить охрану и препятствовать проходу персонала. Охрану не обязательно информировать о проведении проверки, она должна говорить, что проходит важное совещание и нельзя беспокоить ни в коем случае. Должны быть задернуты все шторы и закрыты все двери, ведущие на место проверки.

2. Методические рекомендации по технологии спецпроверок

2.1 Активация известного источника звука.

Источник звука должен быть типичным для обследуемого рабочего места типа негромкой музыки. Музыку следует включать немного громче обычного. Большинство зданий имеет системы связи и встроенные громкоговорящие системы, которые могут быть использованы для заполнения звуком помещения. Причем рекомендуется использовать не радио и телестанции, а заранее записанную на магнитофон музыку, иначе при работе в автоматическом режиме прибор типа ОСКОР будет выдавать ложный сигнал опасности.

Кроме того, для проверяющих важно заранее ознакомиться с используемым источником звука. Опорный источник звука дает следующие преимущества:

- маскирует шумы, производимые в процессе проверки;
- обеспечивает качественный опорный звук для проведения корреляционных измерений;
- может активировать закладки, оборудованные акустоматом;
- при использовании встроенной громкоговорящей системы для создания акустического наполнения обследуемой территории (несколько камнат, этаж или все здание), прибор обнаружения будет регистрировать все закладки, находящиеся везде на озвучиваемой территории (при достаточной их мощности). Другими словами, если звук наполняет все здание, то можно обследовать много комнат одновременно.

2.2 Специальные процедуры для инфракрасных и лазерных угроз.

Из-за того, что инфракрасное излучение не проходит через стены, инфракрасные подслушивающие устройства обычно располагаются вблизи окон или могут быть расположены вне здания и соединены с микрофоном внутри проводом. Поэтому рекомендуется, чтобы при проведении инфракрасных проверок детектор располагался вблиз окна. Шторы или жалюзи следует закрыть, чтобы никто не увидел проверочных действий. Если окна большие, то необходимо менять расположение детектора в процессе проверки. При наличии в помещении инфракрасного передатчика, часть его излучения неизбежно отражается от окна, что дополнительно говорит в пользу задействования 360-градусного инфракрасного датчика. Внешнюю проверку рекомендуется проводить в ночное время (для того, чтобы исключить влияние солнца на ИК-детектор) с расстояния 6-10 м от окон. В этом случае все шторы, занавески и т.д. должны быть открыты.

Примечание: Внешнее инфракрасное обследование многоэтажных домов практически лишено смысла.

2.3 Физический осмотр

Самым лучшим антиподслушивающим устройством был и остается человеческий глаз. Физический осмотр целесообразно проводить в то время, когда прибор обнаружения работает в автоматическом режиме. Следует помнить, что физический осмотр - залог успешного противоподслушивающего обследования.

Для проведения физического осмотра обычно необходимо:

* набор отверток;
* цифровой мультиметр с диапазоном 40 МОм и выше;
* перочинный нож;
* плоскогубцы;
* устройство для зачистки проводов;
* кусачки;
* ультрафиолетовые ручка и фонарик (Примечание 1);
* электрический фонарик;
* обследовательские (стоматологические) зеркала;
* 20-сантиметровый проволочный пробник (Примечание 2);
* небольшой ручной металлоискатель (Примечание 3);
* обнаружитель проводов (Примечание 4);
* удлинители проводов и кабелей;
* легкая лестница;
* комбинезон для работы в грязных местах.

Примечания:

1. Ультрафиолетовую ручку можно использовать для отметок положения винтов и шурупов в сетевых розетках, компьютерах, телефонах и т.п.. В дальнейшем эти метки можно использовать для выяснения вопроса о том, вскрывались помеченные устройства или нет.

2. 20-сантиметровый проволочный пробник это не более чем тонкий металлический штырь, который может быть использован для обследования труднодоступных полостей в мебели на предмет наличия там подслушивающих устройств.

3. Небольшой (помещающийся в кейсе) ручной металлоискатель используется для обследования штор, подвешенных картин, мягкой мебели, книжных полок, ламп и т.п.. Этот дешевый прибор может выполнять многие функции нелинейного локатора.

4. Обнаружитель проводов состоит из передатчика, который подключается к концам проводов, и приемника, с помощью которого отслеживается путь проводов. Наиболее употребительная модель этого прибора - "Fox and Hound", ее легко приобрести и удобно использовать для выяснения функционального назначения проводов.

Физический осмотр должен включать, но не ограничиваться следующим:

* разборка всех сетевых розеток на закладки;
* проверка (металлоискателем) всех полых предметов, особенно с питанием от сети, таких как лампы, часы, калькуляторы;
* разборка, по возможности, телефонных и факсовых аппаратов для выявления подозрительных проводов и модификаций;
* открытие кожухов компьютеров, принтеров и факсов для выявления подозрительных проводов и электрических цепей;
* проверка (металлоискателем) швов оконных штор;
* обследование всех чертежных устройств;
* проверка всех панелей на наличие подозрительных проводов и следов вмешательства. Следует также проверить края кавровых покрытий;
* проверка (металлоискателем) за развешанными картинами;
* проверка (металлоискателем) за книжными полками, книгами, книжными переплетами;
* выяснение принадлежности всех проводов в помещении (провода компьютеров, ламп, часов, радиоприемников, громкоговорителей, телефонов и т.п.);
* устранение неиспользуемых проводов, которые могут использованы для подслушивания;
* обследование потолочного пространства и идентификация всех проводов в области потолка;
* выяснение принадлежности всех проводов в технических отсеках;
* проверка прохождения звука через любые отверстия в помещении. Для этого прямо напротив вентиляционного отверстия располагают источник звука (радио, магнитофон и т.п.) и прослушивают вентиляционные отверстия на большой территории для определения возможной акустической утечки. Для этих целей можно использовать ALP-700 или EAR-200 (продукция REI);
* проверка правильного функционирования громкоговорящей связи. Громкоговорители являются хорошими микрофонами, поэтому несложно, после соответствующего переключения, использовать их для подслушивания. Таким образом, если громкоговорители не используются постоянно, то рекомендуется их совсем отключать или убирать из помещения.

2.4 Гармоники передатчиков

Большинство закладок предназначены для работы на одной частоте, называемой также основной, но в них, из-за жестких требований к размерам и стоимости, отсутствует качественная фильтрация. Значит эти устройства должны излучать на кратных частотах. Так, если основная частота равна 110 МГц, то излучаться будут и частоты 220 МГЦ, 330 МГц, 440 МГц и т.д.. Уровень высших гармоник уменьшается с ростом частоты до полного исчезновения. Отметим, что в автоматическом режиме прибор типа ОСКОР регистрирует каждую гармонику как новый опасный сигнал.

Обычно, если передатчик содержит внутренний низкочастотный осциллятор, то он излучает на частотах, являющихся комбинацией основной и внутренней частот. Например, в продаже есть коммерческий беспроволочный микрофон, который хорошо работает на своей основной частоте 155 МГц, но при этом сильно излучает на частотах 165 МГц, 175 МГц и 185 МГц.

Наличие гармоник повышают вероятность обнаружения подслушивающего устройства, т.к. прибор обнаружения регистрирует не один, а несколько "опасных" сигналов. Если в процессе автоматического обследования зарегистрировано несколько сигналов угрозы, то очень важно проверить соотношение частот этих сигналов для вывода о возможном едином их источнике.

2.5 Уширенный спектр.

Технология уширения спектра сигнала находится в стадии развития и находит все большее применение в закладных устройствах. Эта технология заключается в генерации мощного сигнала и размывании его спектра в широкой полосе частот. Такое преобразование спектра значительно затрудняет обнаружение подслушивающего устройства. Кроме того, сигналы с уширенным спектром подвергнуты цифровому кодированию и при отсутствии соответствующего приемника с декодером невозможно перехватить транслируемую информацию.

Для распознания передатчика с уширенным спектром необходимо использовать сканирование для различных частотных диапазонов. При этом следует помнить, что спектр такого передатчика представляет собой плато, а не острый пик. Но даже если обнаружен спектр такого типа, то это еще не значит, что это сигнал закладки - много спутниковых систем и специальных систем связи имеют такие же спектры. Более того, из-за использования в спектральноуширенных приборах цифрового кодирования, их спектры могут оказаться во много раз меньше, чем спектры приборов со скачущей частотой. Для дальнейшего анализа таких сигналов следует воспользоваться методикой, описанной в следующем разделе.

2.6 Скачущая частота.

Другим высокотехнологическим методом в развитии подслушивающих устройств является использование скачущей частоты. В соответствии с названием, закладки со скачущей частотой работают на какой-то одной частоте очень короткий промежуток времени (5...100 мс) и затем перестраиваются на другую частоту по случайному закону. Эти частотные скачки дают набор множества частотных каналов внутри определенной частотной полосы. При работе в автоматическом режиме детектору трудно распознать такую закладку, т.к. частота излучения изменяется.

Если сигнал со скачущей частотой обнаружн во время проверки, то определить расположение источника очень сложно, потому что приемник прибора со сканированием частоты не способен захватить быстро движущийся по спектру сигнал.

2.7 Непреднамеренные источники радиочастот.

Существует много объектов, которые по своему назначению не должны излучать, но являются источниками радиоизлучения и дают ложные сигналы. Большинство таких излучателей имеют малый радиус действия и легко распознаются, а их местоположение можно определить с помощью широкополосного локатора по максимуму сигнала. Простым выключением соответствующего оборудования можно проверить предположение о происхождении данного сигнала. Ниже, в таблице, приведены некоторые возможные непреднамеренные излучатели, характер их сигналов и оценка вероятности их присутствия.

Излучатель	Возможный сигнал	Вероятность
Люминисцентные лампа	Низкочастотный шум	Средняя
Монитор компьютера	Мощный полигармонический сигнал	Высокая
Компьютеры	Гармонический сигнал обычно обусловлен работой таймеров и могут иметь звук, типичный для цифрового шума.	Средняя
Тюнеры, радиоприемники	Слабые сигналы в полосе радиоприема (УКВ, СВ,ДВ и более низких частотах). Из-за того, что радиоприемники содержат опорные генераторы для преобразования принимаемого сигнала, они могут переизлучать этот сигнал на частотах, больших принимаемого на частоту гетеродина (455 кГц или 10,7 МГц).	Средняя
Светодиодные дисплеи	Низкочастотный шум от системы питания светодиодов.	Низкая
Флюоресцентные или газовые дисплеи	Низкочастотный шум	Низкая
Проводные цифровые телефоны	Очень слабые сигналы. Цифровые телефоны могут иметь систему управления, которая работает на частотах в несколько килогерц или мегагерц.	Низкая

Примечание:

Существует множество других непреднамеренных излучателей: беспроволочные телефоны, сотовые телефоны, игровые мониторы, любые типы современных беспроводных систем (внутренняя связь, уоки-токи, приборы с дистанционным управлением и т.п.). Для повышения эффективности обследования полезно предварительно ознакомиться с используемыми передатчиками.

2.8 Проверка телефонов

Если телефонная система нецифровая, то при повешенной трубке аудиосигнал на проводах должен отсутствовать. У цифровых телефонных систем в линии может присутствовать мощный цифровой сигнал, похожий на шум. Можно отсоединить телефон от розетки, чтобы убедиться, что при этом шум в линии пропадает. Кроме того, если обнаруживается звуковой отклик при постукивании (например карандашем) по подключенному телефону с положенной трубкой, то это значит, что в телефоне установлено шунтирующее устройство. Некоторые типы телефонов остаются активными и при положенной трубке (особенно это касается телефонов с переговорными устройствами). Такой аппарат представляет прямую угрозу и его необходимо заменить.

При снятой трубке телефона аналоговой или гибридной системы хорошо прослушиваются все сигналы с микрофона (в гибридных системах используется аналоговый сигнал для переговоров и звонков и остальные 2...6 проводов для питания и цифрового управления).

Некоторые радиозакладки активируются только при снятой телефонной трубке, поэтому проверку следует проводить как при снятой, так и при повешенной трубке.

В заключение необходимо отметить, что следование приведенным выше рекомендациям позволит достичь успеха и повысить эффективность выполнения спецобследований помещений при условии, если они будут проводиться профессиональными специалистами.Это должны быть штатные сотрудники фирм, имеющих лицензии на услуги в сфере защиты информации.

ЛИТЕРАТУРА:

1. Каталог фирмы “Westinghause Audio Intelligence Devices ”, USA.

Поступила 29.11.2000 р.

УДК 681.3.004

Зуєв О.В., Хмелько Ю.М., Чирков Д.В.

КРИТЕРИЙ ОЦЕНКИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Современные средства защиты информации (СЗИ) характеризуются множеством качественных показателей. Достижение требуемых значений качества по одним из показателей нередко сопровождается ухудшением качества по другим показателям. В таких условиях требуется объективная оценка качества СЗИ со стороны потребителя.

Качество СЗИ предлагается определять вероятностной мерой , значение которой должно соответствовать уровню доверия к СЗИ со стороны потребителя . Необходимо оценить обобщенные эксплуатационно-технические характеристики СЗИ, отражающие их свойство выполнить поставленную перед ними задачу с вероятностью не ниже заданой. Такая оценка может быть проведена в результате исследования целостности (Ц)СЗИ. Вероятность того, что исследуемое СЗИ окажется работоспособным в произвольный момент времени и проработает безотказно с этого момента в течении заданного интервала времени определяется непрерывностью обслуживания (НО) СЗИ.