Особенности работы с индикаторами поля в современных условиях

В данной статье рассмотрена общая методика поиска радиомикрофонов с применением как светодиодных ИП, так и цифровых ИП. Хотя поиск с применением индикаторов поля и не дает полной гарантии успеха, но в некоторых случаях, например при защите коммерческой информации, применение ИП бывает достаточно.

Г. А. Бузов, *кандидат военных наук, доцент, зав. лабораторией защиты информации от утечки по техническим каналам*

Учебный центр «Информзащита»

В предыдущей статье[1] были рассмотрены вопросы, касающиеся структуры и особенностей функционирования одних из наиболее простых и распространенных поисковых приборов – индикаторов поля. Однако применение этих приборов для выявления радиомикрофонов в современных условиях имеет свои особенности, которые необходимо рассмотреть.

Российское законодательство разрешает без лицензии выявлять средства, предназначенные для несанкционированного получение информации, если решается задача по обеспечению собственной безопасности, следовательно, нужно определить, как решить эту задачу с наибольшей эффективностью.

Тактика использования индикаторов поля, прежде всего, связана с условиями и особенностями, в которых функционируют современные закладочные устройства. Поэтому, рассматривая вопросы применения индикаторов поля в процессе проведения поисковых мероприятий с целью выявления закладочных устройств (ЗУ), прежде всего необходимо оценить обстановку, в которой придется решать эту задачу.

Анализ обстановки целесообразно начинать с определения побудительных мотивов проведения мероприятий по выявлению ЗУ, что позволяет оценить масштаб и объем поисковых мероприятий. При этом определение мотивации их проведения является одним из основных факторов, позволяющих грамотно спланировать и осуществить сам поиск.

Если в качестве побудительных мотивов выступает обнаруженная утечка вполне конкретных сведений, уже повлекшая за собой потери (финансовые, материальные и т. д.), объем и номенклатура поисковых мероприятий будет одна, если же руководство организации планирует проведение профилактической проверки, то масштаб и структура поисковых мероприятий окажутся несоизмеримо больше и разнообразней.

В любом случае одних умений и навыков поисковикам будет недостаточно: для эффективного решения поставленных задач необходимо использовать специализированную аппаратуру. К такого рода аппаратуре относятся приборы и оборудование, позволяющие по демаскирующим признакам определить и локализовать источники электромагнитных излучений.

Однако в любом случае подготовка к проверке начинается с выявления и анализа возможных угроз вашей информации. Для этого необходимо:

- проанализировать информацию, циркулирующую на вашем предприятии с целью выявления той,

[1] *Бузов А. Г. Еще раз об индикаторах электромагнитного поля // Защита информации. Инсайд. 2012, № 1, с. 34–38.*

которая может быть востребована и реализована на рынке;
- сделать предположения о том, кто заинтересован в получении этих сведений;
- попытаться определить, кого противник может использовать для получения этих сведений.

Затем необходимо оценить возможности вероятного противника с целью выявления потребительских свойств и технических характеристик ЗУ, которые могут быть им применены. Полученная информация позволит спланировать мероприятия по выявлению ЗУ и подобрать требуемое для этого оборудование. Оптимальный комплект такого оборудования состоит из аппаратно-программного комплекса радиомониторинга, сканирующего приемника, индикаторов поля, оптических обнаружителей видеокамер. В качестве дополнительного оборудования можно рекомендовать нелинейный локатор и комплект инструментов.

Наличие аппаратно-программного комплекса снимает необходимость приобретения оборудования для проверки линий различного назначения.

Однако не всегда финансовые возможности организации позволяют приобрести весь рекомендованный комплект поискового оборудования, и в этом случае приходится довольствоваться минимальным набором. В общем случае такой набор не гарантирует выявления всех видов современных ЗУ, но при некоторых условиях (при использовании злоумышленниками ЗУ, незаконно приобретенных на радиорынках, через Интернет, сделанных самостоятельно) его применение может привести к положительным результатам.

В любом случае, даже при использовании минимального комплекта оборудования для достижения цели проверки необходимо придерживаться определенной последовательности при проведении поисковых мероприятий. В рамках одной статьи сложно дать рекомендации по выявлению всех видов закладочных устройств, поэтому ограничимся рассмотрением вопросов проведения мероприятий по выявлению радиомикрофонов с использованием индикаторов поля, причем как светодиодных, так и цифровых.

Так как любой поиск вызван какими-то причинами, то начинается он после определения этих причин. Как правило, в условиях рыночных отношений основным побудительным мотивом проведения поисковых мероприятий является выявление утечки. При выявлении факта утечки речевой информации необходимо, прежде всего, определить, по каким каналам была возможна утечка, когда и кем мог быть внедрен радиомикрофон. При этом необходимо выявить:
- временной период, когда появились подозрения в утечке информации;
- посторонних лиц и работников фирмы, имевших доступ в защищаемое помещение в данный период;
- временной период, которым мог располагать злоумышленник для установки ЗУ.

Проведенный анализ позволит сделать выводы о возможных местах установки ЗУ и их потребительских характеристиках.

Всякое поисковое мероприятие по выявлению ЗУ начинается с визуального осмотра проверяемого помещения, методика его проведения достаточно полно изложена во многих профильных печатных изданиях.

Поиск с применением любого индикатора поля начинается с подготовки прибора к работе. Для этого необходимо в соответствии с руководством по применению выставить необходимый уровень порога обнаружения. Данный уровень рекомендуется устанавливать с превышением уровня фонового электромагнитного поля в проверяемом помещении на 5–10 дБ.

В процессе визуального осмотра помещения поисковики, как правило, определяют несколько потенциальных мест возможного размещения ЗУ, вызывающих у них подозрение по тем или иным признакам. Поскольку камуфлированные ЗУ зачастую невозможно обнаружить путем визуального осмотра, поиск целесообразно начинать именно с обследования мест, вызвавших подозрение, плавно перемещая включенный индикатор поля (ИП) на высоте 5–10 см от контролируемой поверхности.

Светодиодный индикатор при перемещении его в районе возможного отклика излучающего сигнала выдает информацию в виде светящихся светодиодов. Затем путем поворота индикатора поля в разные стороны необходимо добиться максимального уровня сигнала. В зависимости от расположения источника излучения на устройстве индикации будет загораться большее или меньшее число светодиодов. При загорании максимального числа светодиодов необходимо путем загрубления чувствительности прибора уменьшить число светящихся светодиодов до двух или трех и опять повторить операцию до максимального числа загоревшихся светодиодов. При приближении к источнику излучения возможно проявление акустозавязки в виде характерного свиста в динамике ИП. Режим акустозавязки характеризуется возникновением положительной обратной связи между источником излучения и динамиком ИП. По максимуму уровня излучения и возникновению акустозавязки оператор делает вывод о наличии в районе поиска источника излучения и визуально, методом осмотра подозрительных мест, выявляет его.

Однако при кажущейся простоте использования светодиодных индикаторов поля для поиска и локализации ЗУ их применение имеет ряд существенных недостатков:
- по индикации невозможно определить характеристики источника излучения, а это особенно важно при сложной электромагнитной обстановке в районе поиска;
- при наличии рядом с проверяемым помещением мощного внешнего источника излучения (например, базовой станции сотовой связи) индикатор поля отображает только излучение, исходящее от этого источника, а на другие не реагирует.

Для успешного проведения поиска наиболее целесообразно использование цифровых, селективных ИП. На цифровой дисплей ИП выводится информация об обнаруженных

сигналах, превышающих пороговое значение: частота источника излучения, мощность излучаемого сигнала в децибелах. По этим параметрам, зная характеристики легальных источников излучения, оператор может сосредоточиться на анализе подозрительных излучений.

Более подробно рассмотрим методику поиска ЗУ на примере использования селективного индикатора поля RAKSA-120.

Селективный индикатор поля RAKSA-120 предназначен для обнаружения в ближней зоне и определения местоположения радиопередающих устройств, использующихся для негласного съема информации, включая сотовые телефоны стандартов GSM900/1800, UMTS(3G), CDMA450, беспроводные телефоны стандарта DECT, устройства Bluetooth и Wi-Fi. По принципу действия селективный индикатор поля RAKSA-120 представляет собой супергетеродинный приемник с низкой ПЧ и синтезатором частоты. При работе происходит непрерывное сканирование частотного диапазона и анализ пиков спектрограммы. Идентификация стандартных цифровых сигналов осуществляется по их амплитудно-временной характеристике.

Время цикла сканирования и анализа всех цифровых и аналоговых сигналов составляет 1,0–1,5 с. Для фильтрации кратковременных помех необходимо наличие сигнала как минимум в двух циклах сканирования. Этим и определяется время обнаружения сигнала, равное 2–3 с.

Любой непрерывный радиосигнал с коэффициентом амплитудной модуляции менее 0,5 и без скачков частоты классифицируется как аналоговый. Сюда относятся собственно аналоговые сигналы с различными видами модуляции (АМ, ЧМ, ФМ) и цифровые сигналы с модуляцией FSK, PSK и др.

Индикатор поля RAKSA-120 может работать в режимах охраны, обзора, поиска, поиска с вычитанием спектра и мониторинга цифровых сигналов.

Поисковое мероприятие начинается с подготовки поискового оборудования. Прибор включается нажатием кнопки [**C/PWR**] с удержанием более одной секунды (до короткого звукового сигнала). После включения индикатора на дисплее отображается главное меню (рис. 1):

Рис. 1

1. Охрана.
2. Обзор.
3. Поиск.
4. Поиск с вычитанием.
5. Цифровой сигнал.
6. Журнал.
7. Настройки.
8. О приборе.

Нажатием [▼] необходимо выбрать режим «Настройки» и нажать кнопку [**OK**]. На дисплее высветится:

Analog – аналоговый сигнал.
GSM – сигнал GSM900/1800.
UMTS – сигнал UMTS (3G).
CDMA – сигнал CDMA450.
DECT – сигнал DECT.
Bluetooth – сигнал Bluetooth.
Wi-Fi – сигнал Wi-Fi.
2.4 GHz – прочие импульсные сигналы диапазона 2,4 ГГц.

Выбрать тип сигналов для поиска «**Меню** [**OK**] → **Настройки** [**OK**] → **Сигналы**». Выбранные типы сигналов отмечаются значком «V» путем нажатия [▼]. Нажатием кнопки [**OK**] перейти в меню и выбрать режим «**Обзор**».

Во время поиска в помещении не должно быть работающих источников радиосигнала: сотовых и беспроводных телефонов, устройств Bluetooth, Wi-Fi, бытовых микроволновых печей. Для активации радиопередатчиков, использующих акустопуск, необходимо обеспечить наличие в помещении тестового акустического сигнала, например от работающего радиоприемника.

Выбор порогового значения осуществляется за пределами проверяемого помещения и зависит от оперативной обстановки. В сложной оперативной обстановке выбирается уровень порога равный 5–10 дБ.

Поиск радиомикрофонов при использовании данного режима целесообразно проводить в сложной оперативной обстановке, так как в этом режиме на дисплее отображается список текущих обнаруженных сигналов, отсортированный по частоте или типу сигнала (рис. 2).

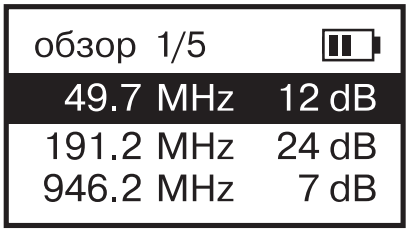

Рис. 2

В верхней строке отображается номер выбранного сигнала и общее число сигналов в списке. Список начинается с аналоговых сигналов, для которых определено значение частоты. Затем из всех аналоговых сигналов, для которых невозможно достоверно определить значение частоты, отображается один, имеющий максимальный уровень. В конце списка находятся цифровые сигналы. В случае пропадания сигнал удаляется из списка не сразу, а с задержкой примерно в 10 секунд – в это время на дисплее отображается последнее ненулевое значение уровня сигнала.

Оператор, анализируя список обнаруженных сигналов, имеет возможность сделать выводы о сигналах, которые могут относиться к разряду подозрительных, и в дальнейшем работать только с этими сигналами. Выбор сигнала для анализа осуществляется перемещением по списку обнаруженных сигналов нажатием кнопок [▲] или [▼]. Выбрав сигнал для анализа, нажмите кнопку [**OK**]. На дисплее высветятся параметры обнаруженного сигнала, частота и мощность излучения.

Перемещением индикатора поля в районе обнаруженного излучения необходимо добиться максимума уровня и визуально обнаружить источник излучения. Для более надежного обнаружения источника излучения аналогового сигнала можно осуществить его аудиоконтроль, нажав на кнопку [**OK**]. В данном режиме при работе ЗУ с открытым каналом передачи данных возможна акустозавязка, проявляющаяся в виде характерного свиста и при наличии

тестового акустического сигнала в контролируемом помещении его прослушивание в динамике индикатора поля.

После обнаружения источника излучения следует вернуться в режим обзора для анализа списка обнаруженных сигналов нажатием кнопок [**OK**] или [**C**]. Затем, действуя аналогично описанному выше, провести анализ и локализацию другого подозрительного сигнала.

В более простых случаях при незагруженной электромагнитной обстановке можно применять режимы «поиска» и «поиска с вычитанием спектра». В данных режимах ИП выявляет только аналоговые сигналы, превышающие фоновые значения в проверяемом помещении. Поиск сигналов в первом из этих режимов несущественно отличается от поиска в режиме обзора. В данном режиме ИП фиксирует максимальное излучение, превышающее фоновое в проверяемом помещении, а в дальнейшем динамика работы аналогична.

Более интересен метод поиска с вычитанием спектра (рис. 3). В этом режиме определяется не абсолютный уровень аналоговых сигналов, а относительный, то есть его разница с базовым спектром, который был измерен в начале работы в этом режиме. Известно, что при приближении или удалении от радиопередатчика, который находится внутри помещения, уровень сигнала изменяется сильнее по сравнению с радиопередатчиком, расположенным вне помещения. Так как в режиме поиска с вычитанием спектра индикатор поля селективно реагирует на изменения уровня, то локальные радиопередатчики будут обнаружены с большей вероятностью.

Поиск с вычитанием спектра начинается с накопления в течение 5 секунд базового спектра аналоговых сигналов. В это время на дисплей выводится соответствующее сообщение. Накопление спектра проводится в помещении, находящемся рядом с проверяемым, в котором гарантированно отсутствуют закладочные устройства. После накопления фона с включенным индикатором поля оператор заходит в проверяемое помещение.

Рис. 3

После завершения накопления на дисплее отображается аналоговый сигнал, имеющий максимальный относительный уровень.

В режиме поиска с вычитанием спектра реализована световая и звуковая индикация относительного уровня сигнала: по частоте повторения вспышек светодиода можно судить о приближении или удалении от радиопередатчика. В данном режиме возможен аудиоконтроль обнаруженного сигнала. ■