Еще раз об индикаторах электромагнитного поля

Стремительное развитие средств коммуникации и общения, наличие Интернета почти в каждой семье привело не только к позитивным, но и к негативным результатам. Зачастую в Интернете появляются материалы, отнесенные к информации, в отношении которой владельцем установлено требование об обеспечении ее конфиденциальности, то есть те сведения, которые он хотел сохранить в тайне от других лиц. Получение таких сведений, как правило, связано с нарушением закона и применением специальных технических средств (СТС) для негласного получения информации. Утечка информации конфиденциального характера, в свою очередь, может привести к финансовым, моральным потерям, потере деловой репутации ее законного владельца, кроме того, он может стать объектом банального шантажа.

Г. А. Бузов, *к. в. н., доцент, заведующий лабораторией защиты информации от утечки по техническим каналам*
Учебный центр «Информзащита»

Наиболее широкое распространение и применение для незаконного получения информации нашли радиомикрофоны, или «жучки», как их именуют в просторечии. Несмотря на незаконность применения таких средств, их доступность (предложения в Интернете, возможность приобретения на радиорынках, относительная простота изготовления) и легкость применения вывело этот вид СТС на одно из первых мест по частоте использования.

Наше законодательство разрешает владельцам информации самостоятельно, с использованием поисковой аппаратуры, без получения лицензии заниматься выявлением таких СТС для обеспечения собственной информационной безопасности. Так, в Федеральном законе «О лицензировании отдельных видов деятельности» № 99-ФЗ от 04.05.20011 в ст. 12, определяющей перечень видов деятельности, на которые требуются лицензии, в п. 3 написано, что в соответствии с настоящим Федеральным законом лицензированию подлежит «деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

В свете вышесказанного высокую степень актуальности приобретает задача правильного подбора необходимой аппаратуры для выявления такого рода СТС. Так как большинство покупателей слабо разбирается в технических аспектах поисковых мероприятий, им приходится руководствоваться наиболее доступными справочными материалами по этим вопросам, то есть информацией, полученной из Интернета. При этом вполне обоснованным выглядит их желание при наименьших затратах обеспечить максимальный уровень информационной безопасности. Однако большинство покупателей при этом забывают известные пословицы о том, что скупой платит дважды, а бесплатный сыр бывает только в мышеловке. Этим зачастую и пользуются недобросовестные производители и продавцы поискового оборудования. Нельзя сказать, что они напрямую обманывают покупателей, скорее, просто-напросто кое-что не договаривают. Как правило, при рассмотрении возможностей того или иного прибора на первый план выдвигаются наиболее выгодные его характеристики, остальные же, менее привлекательные, замалчиваются.

В последнее время в средствах массовой информации появился ряд статей, в которых индикаторы поля позиционируются практически как «панацея» для защиты от радиомикрофонов, поэтому возникла необходимость разобраться, соответствуют ли подобные утверждения действительности или это очередной рекламный ход.

Прежде всего попытаемся разобраться в том, что же представляет собой индикатор или детектор электромагнитного поля и на каких физических принципах он работает. Элементарный индикатор поля (ИП) представляет собой измеритель электромагнитного поля в ближней зоне, то есть в районе контролируемого или, в соответствии с терминологией специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), защищаемого помещения.

Простейший ИП состоит из антенны, широкополосного усилителя, порогового устройства и устройства индикации обнаруженного сигнала. Рабочий диапазон частот такого индикатора определен полосой пропускания широкополосного усилителя, а полоса пропускания ИП обычно составляет несколько гигагерц. Поскольку в большинстве ИП отсутствуют входные цепи селекции сигналов, они не способны сканировать частотный диапазон и реагируют на появление электромагнитных сигналов, превышающих пороговое значение, практически мгновенно, независимо от частоты передачи. За последнее время на рынке появились селективные ИП, работающие по принципу сканирующего приемника, но с более широкой полосой обзора. За счет широкой полосы пропускания чувствительность ИП не превышает 10 мВ, в связи с чем дальность обнаружения электромагнитных излучений, превышающих пороговое значение, невысока и на практике составляет единицы метров («ближняя зона»), а также сильно зависит от рабочей частоты и мощности источника излучения.

Таким образом, ИП регистрирует в месте контроля электромагнитные излучения, превышающие пороговые значения и, в соответствии с критериями, заложенными в управляющую схему прибора, выводит данные об обнаруженных сигналах на устройство индикации.

Для лучшего понимания принципов, реализуемых в ИП при выявлении сигналов активных закладочных устройств (ЗУ), целесообразно проанализировать структуру электромагнитных излучений в защищаемых помещениях.

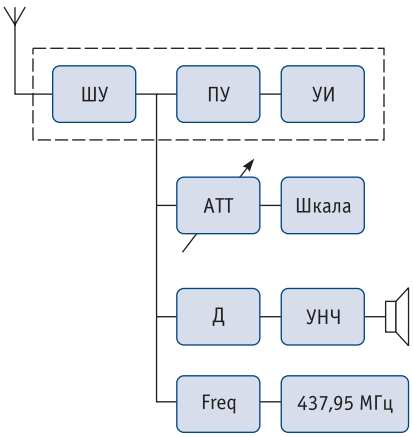
Электромагнитная обстановка практически любого помещения характеризуется многими составляющими. В нее входят, прежде всего, излучения легальных источников, к которым можно отнести УКВ-радиостанции, системы сотовой и транкинговой связи, телевидение, радиотелефоны, работающую бытовую электронную технику и т. д. Совокупность этих излучений и составляет электромагнитный фон помещения, по которому определяется уровень порогового значения для большинства индикаторов поля. Фоновые значения электромагнитных излучений будут приблизительно одинаковы для прилегающих к проверяемому помещений.

При внедрении в помещение активного ЗУ его излучение в большинстве случаев будет резко отличаться от фонового по мощности, амплитуде и существенно превышать пороговое значение. При правильно выставленном уровне порогового значения ИП станут улавливать излучение ЗУ и выводить параметры сигнала на устройство индикации, по информации которого оператор сможет принять решение о принадлежности выявленного источника излучения к ЗУ. Следовательно, информация, выводимая на устройство индикации, играет немаловажное значение при определении принадлежности обнаруженных излучений к работе ЗУ. Поэтому возникает необходимость более подробно разобраться с техническими характеристиками и особенностями функционирования различных типов индикаторов поля.

В зависимости от решаемых с помощью индикаторов электромагнитного поля задач можно провести их классификацию, условно разделив на бытовые и профессиональные.

Бытовые индикаторы электромагнитного поля. Как правило, единственной функцией таковых является включение индикации при превышении уровня электромагнитного поля некоторого ранее установленного значения (порога). Индикация таких приборов в основном имеет смысл – Да/Нет. Данные индикаторы предназначены для информирования владельца о наличии (появлении) в ходе переговоров или в месте нахождения владельца ИП несанкционированных излучений, превышающих фоновое значение излучений в данном месте. Как правило, данные приборы имеют небольшие габаритные размеры, скрытую индикацию. В большинстве своем они закамуфлированы под часто используемые бытовые приборы и различного рода сувениры: брелоки для ключей, пульты включения автомобильной сигнализации, авторучки («Спутник», «Комар», Antibug+, «Блокнот», «Hunter ручка-детектор» и т. д.).

Профессиональные индикаторы электромагнитного поля. Основным предназначением профессиональных ИП является выявление и локализация несанкционированных источников излучения. Они имеют более сложную структурную схему (рис. 1), включающую ряд дополнительных устройств.



ШУ – широкополосный усилитель;
ПУ – пороговое устройство;
УИ – устройство индикации;
АТТ – аттенюатор;
Шкала – устройство индикации уровня;
Д – демодулятор;
УНЧ – НЧ-усилитель;
Freq – частотомер

Рис. 1. ***Блок-схема профессионального индикатора поля***

Так как эффективность индикаторов поля сильно зависит от помеховой обстановки в конкретном месте поиска, то для уменьшения этой зависимости в некоторых моделях ИП используются режекторные или полосовые фильтры (АПП-7). Первые в значительной степени уменьшают уровень помех от известных источников (как правило, передатчиков телевещания) и настроены на наиболее мощные из них. Вторые сужают частотный диапазон поиска, чем уменьшают мощность помех на входе прибора. Обычно применяется несколько полосовых фильтров, каждый из которых настроен на свой диапазон частот. Вместе они перекрывают диапазон частот индикатора поля. При поиске, в зависимости от загрузки проверяемого диапазона, фильтры могут использоваться выборочно.

Рис. 2. ***Устройства индикации светодиодных индикаторов поля***

Рис. 3. ***Образцы цифровых индикаторов поля***

Наличие режима частотомера позволяет измерять значение несущей частоты радиосигнала, уровень которого значительно превышает уровень фона. Это дает возможность ориентировочно идентифицировать передатчик по значению несущей частоты и определить, к какому виду можно отнести обнаруженный сигнал. Режим частотомера очень полезен, когда известно значение несущей частоты ЗУ и стоит задача конечной локализации передатчика опасного сигнала. Например, при использовании автоматизированных комплексов радиоконтроля, когда поиск и идентификация могут проводиться автоматически. При этом несущая частота ЗУ будет определена комплексом, а локализацию удобней осуществлять при помощи индикаторов поля, имеющих режим частотомера («Ракса120», «Брелок», CORDON, «Блик-Д», ST-107, «Флик»).

Мы уже говорили о том, что информация, выводимая на устройство индикации, имеет немаловажное значение при определении принадлежности обнаруженных излучений к работе ЗУ. Устройства индикации современных индикаторов поля можно разделить на два основных вида: светодиодные и цифровые, выводящие информацию об обнаруженных сигналах на дисплей прибора.

Принципиально светодиодная индикация представляет собой дорожку светодиодов, загорающихся при обнаружении сигнала, превышающего уровень порогового значения электромагнитного поля (рис. 2). По количеству загоревшихся светодиодов оператор делает вывод о возможном местонахождении источника излучения (чем ближе источник излучения, тем больше амплитуда принимаемого сигнала и большее число светодиодов загорится).

Рассмотрим цифровые устройства индикации, выводящие информацию об обнаруженных сигналах на дисплей (рис 3).

Устройства индикации современных цифровых индикаторов поля позволяют выводить на дисплей следующую информацию: частоту обнаруженного сигнала, мощность излучения в децибелах или по количеству закрашенных секторов, а также принадлежность к известным видам излучения (GSM, DECT, Bluetooth и Wi-Fi). Такой объем выводимой информации позволяет оператору определить, в зависимости от частотной области излучения, принадлежность сигнала к тому или иному виду и локализовать его источник. Кроме того, у некоторых цифровых индикаторов имеется возможность производить селекцию обнаруженных сигналов и в данный момент работать только с тем сигналом, который вас интересует. Некоторые из цифровых индикаторов имеют возможность подключения к персональному компьютеру, что также расширяет их возможности.

Таким образом, проведенный краткий анализ тактических возможностей поисковых индикаторов с различной индикацией информации об обнаруженных излучениях позволяет сделать определенные выводы:

- светодиодная индикация не обеспечивает оператора необходимой информацией для идентификации обнаруженного сигнала, даже для ЗУ с открытым каналом передачи данных;
- при наличии мощного внешнего излучения (например, от находящейся рядом с контролируемым помещением базовой станции сотовой связи) светодиодный индикатор будет реагировать только на этот сигнал, что не позволит выявлять излучение ЗУ из защищаемого помещения;
- информация, выводимая на дисплеи цифровых индикаторов поля, а именно частота, мощность излучаемого сигнала и принадлеж-

ность импульсных сигналов к определенному виду, позволяет оператору с более высокой вероятностью выявить принадлежность излучаемых сигналов к определенному источнику излучения;
- наличие системы селекции обнаруженных сигналов позволяет отстроиться от источника помехового сигнала и анализировать сигналы, подходящие по параметрам к излучениям закладочных устройств.

Единственным «недостатком» цифровых индикаторов поля, по сравнению со светодиодными, является их более высокая стоимость. Впрочем, он вполне компенсируется изложенными выше преимуществами.

Анализируя рынок поисковых технических средств? можно выделить ряд цифровых индикаторов, которые по своим параметрам и характеристикам удовлетворяют требованиям, предъявляемым к поисковым приборам. К ним можно отнести универсальный прибор РИЧ-8, анализатор электромагнитного поля «КОРДОН», детектор электромагнитного поля ST 107, селективный индикатор поля RAKSA-120. Дадим краткую характеристику каждому из перечисленных приборов.

Портативный измеритель мощности РИЧ-8 (MFP-8000) (рис. 4) – универсальный прибор, который органично сочетает в себе свойства, присущие сразу нескольким типам измерительных приборов: измерителю мощности, частотомеру, индикатору поля и анализатору сигнатуры.

С его помощью можно:
- определять частоту входного сигнала в диапазоне частот от 100 кГц до 8 ГГц;
- измерять мощность входного сигнала в диапазоне уровней от –60 до +30 дБм;
- идентифицировать во входном сигнале наличие признаков протокола обмена данными для сотовой и телефонной систем связи (GSM 900/1800/1900, DECT);
- автоматически (посредством встроенного интерфейса) настраивать панорамные радиоприемники или другие устройства на измеренную MFP-8000 частоту сигнала;
- использовать (встроенные) память прибора, часы и календарь для протоколирования и хранения результатов измерений;
- задействовать встроенный интерфейс для организации использования MFP-8000 в качестве измерительного элемента в составе автоматизированных компьютерных систем.

Анализатор электромагнитного поля «КОРДОН» (рис. 5) предназначен для выявления и локализации маломощных источников электромагнитного излучения в диапазоне от 50 до 8000 МГц. Анализатор поля позволяет выявлять закладные устройства, внедренные в выделенные помещения и на объекты информатизации и использующие для передачи информации радиоканал. Работа анализатора основана на интегральном методе измерения уровня электромагнитного поля в точке его расположения. Прибор позволяет идентифицировать сигналы устройств сотовой и телефонных систем связи стандартов GSM-900, GSM-1800 (DCS), DECT, а также беспроводных систем связи Bluetooth и Wi-Fi (диапазон – 2,4 ГГц) и при этом не только обнаружить излучение радиопередатчика, негласно установленного в выделенном помещении, но и измерить частоту его сигнала, а также оценить мощность электромагнитного излучения в точке приема. Анализатор имеет два режима: режим поиска и режим акустической завязки. В первом случае осуществляется измерение частоты и уровня электромагнитного излучения, во втором – возможен поиск радиопередатчиков методом акустической обратной связи. Прибор снабжен жидкокристаллическим дисплеем, на котором отображаются:
- диапазон частот;
- уровень и частота принимаемого сигнала;
- наличие сигналов GSM-900, GSM-1800, DECT, Bluetooth, Wi-Fi;
- уровень порога обнаружения и заряда элементов питания.

Детектор электромагнитного поля ST 107 (рис. 6) предназначен для выявления и локализации маломощных источников электромагнитного излучения в диапазоне от 50 МГц

Рис. 4. ***Портативный измеритель мощности РИЧ-8***

Рис. 5. ***Анализатор электромагнитного поля «КОРДОН»***

до 7000 МГц. Большой набор встроенных эффективных инструментов (частотомера, графического и цифрового индикаторов уровня принимаемого сигнала, осциллографа, самописца) позволяет успешно выявлять и локализовывать:
- радиомикрофоны;
- телефонные радиоретрансляторы;
- радиостетоскопы;
- видеокамеры с радиоканалом;
- радиомаяки;
- технические средства пространственного ВЧ-навязывания;

Рис. 6. ***Детектор электромагнитного поля ST 107***

Рис. 7. ***Селективный индикатор поля RAKSA-120***

- сотовые телефоны и радиомодемы стандарта GSM и беспроводные телефоны стандарта DECT;
- устройства передачи информации с использованием стандартов Bluetooth, WLAN.

Кроме того, устройство позволяет идентифицировать принимаемые цифровые сигналы (GSM, DECT, Bluetooth, WLAN). Информация выводится на графический цветной OLED-индикатор. Специальное программное обеспечение обеспечивает работу ST 107 под управлением персонального компьютера, что расширяет возможности по визуализации полученной информации, ее архивированию для последующего анализа.

Перечисленные выше поисковые приборы с расширенным частотным диапазоном могут успешно использоваться при выполнении поисковых работ при защите сведений, составляющих государственную тайну. Применение противником современных СТС для получения такой информации вызывает необходимость использования всех потенциальных возможностей этих приборов, что предъявляет повышенные требования к уровню подготовки поисковиков.

Защита от утечки информации, составляющей коммерческую тайну или относящейся к информации, в отношении которой владельцем установлено требование об обеспечении ее конфиденциальности, имеет свои особенности. Эти особенности, прежде всего, связаны с возможностями злоумышленников. Как правило, эти возможности ограничены незаконными предложениями радиорынков и различных «шпионских» сайтов в Интернете.

Другой аспект данной проблемы связан с уровнем подготовки поисковиков. При защите сведений, составляющих коммерческую тайну, в условиях нашей действительности большинство коммерсантов старается своими силами устранить возникшие проблемы, поставив задачу выявления ЗУ сотрудникам собственных служб безопасности, которые, как правило, обладают недостаточной подготовкой в данной области. Это налагает определенные требования к применяемым поисковым приборам. Они при хороших технических характеристиках должны иметь удобную схему управления, хороший интерфейс, выдавать достаточную и понятную информацию об обнаруженных сигналах, выводимую на устройство индикации. Такими параметрами обладает селективный индикатор поля RAKSA-120.

Селективный индикатор поля RAKSA-120 (рис. 7) предназначен для обнаружения в ближней зоне и определения местоположения радиопередающих устройств, использующихся для негласного съема аудио- и видеоинформации в диапазоне от 50 до 3300 МГц, таких как:

- радиомикрофоны с аналоговой, цифровой и широкополосной модуляцией;
- сотовые телефоны стандартов GSM 900/1800, UMTS (3G), CDMA450;
- беспроводные телефоны стандарта DECT;
- устройства Bluetooth и Wi-Fi;
- беспроводные видеокамеры;
- радиомодемы и радиомаяки систем слежения.

По принципу действия селективный индикатор поля RAKSA-120 представляет собой скоростной супергетеродинный приемник с низкой промежуточной частотой и синтезатором частоты, поэтому, в отличие от широкополосных детекторов, позволяет обнаруживать сигналы в условиях значительных помех, что особенно актуально для городских условий. Индикатор поля RAKSA-120 может работать в режимах охраны, обзора, поиска, поиска с вычитанием спектра и мониторинга цифровых сигналов. Высокая скорость сканирования позволяет обнаруживать цифровые и аналоговые сигналы за 2–3 секунды.

В индикаторе поля RAKSA-120 предусмотрен аудиоконтроль сигналов, позволяющий использовать «акустозавязку». В режиме охраны осуществляется непрерывная адаптация к помеховой обстановке, ведется журнал событий тревоги. Отсутствие внешней антенны и бесшумная индикация тревоги с помощью вибросигнала позволяют использовать его скрытно. Для поиска активных ЗУ можно воспользоваться режимом обзора, при котором все обнаруженные сигналы отображаются на дисплее в виде списка с указанием частоты и уровня. В этом режиме оператор имеет возможность выделить интересующее его излучение и в дальнейшем работать только с этим сигналом до обнаружения источника излучения.

В рамках одной статьи невозможно осветить все аспекты затронутой проблемы, которая в настоящее время становится все более актуальной. Организация и осуществление поисковых мероприятий в современных условиях также требуют переосмысления и разработки нового подхода. В данной статье была предпринята попытка проанализировать особенности функционирования современных поисковых индикаторов и на их примере оценить возможности по выявлению активных ЗУ. ■