Выявление сигналов электронных устройств негласного получения информации в каналах цифровой радиосвязи

В статье рассматриваются новые угрозы безопасности информации, возникающие одновременно с развитием и распространением современных телекоммуникационных технологий, анализируются возможности использования каналов цифровой радиосвязи электронными устройствами негласного получения информации (ЭУНПИ), предлагаются методы выявления ЭУНПИ в каналах цифровой радиосвязи, а также описывается практическая реализация этих методов на примере автоматизированного комплекса выявления и идентификации несанкционированных электронных устройств беспроводной связи «Цифра 2».

А. Л. Панферов, *начальник отдела технических средств защиты информации ЗАО «НПЦ Фирма «НЕЛК»*

Д. И. Белорусов, *генеральный директор ООО «РИКОМ»*

Ю. Е. Крыжановский, *инженер ООО «РИКОМ»*

В условиях постоянного развития телекоммуникационных технологий и средств связи радиоэлектронная обстановка становится все более насыщенной и загруженной сигналами со сложной структурой. В такой ситуации средств радиомониторинга, построенных на принципах спектрального анализа сигналов, уже недостаточно для надежного выявления ЭУНПИ с передачей по радиоканалу.

С наибольшими сложностями в обнаружении ЭУНПИ оператор обычно сталкивается при анализе диапазонов частот, выделенных для цифровых каналов связи, таких как радиотелефонная и радиочастотная беспроводная связь. Это обусловлено, прежде всего, тем, что в диапазонах цифровых каналов связи модель угроз усложнена дополнительными рисками, не свойственными для поддиапазонов, в которых применяются постоянно действующие сигналы с простыми видами модуляций. К таким рискам можно отнести:

- регулярную загруженность диапазонов;
- использование цифровыми системами радиосвязи сигналов, которые сложно регистрировать широкополосной радиоприемной аппаратурой;
- низкое соотношение сигнал\шум на входе приемного устройства;
- использование частотного уплотнения каналов;
- нахождение устройства в «дежурном» режиме.

Регулярная загруженность диапазонов. Диапазоны цифровых систем связи, как правило, постоянно заняты сигналами систем радиотелефонной связи или сигналами собственной или соседних беспроводных сетей, среди которых сигнал ЭУНПИ может «легко» затеряться, если будет иметь форму, схожую с сигналами легальных систем. Например, диапазоны downlink канала базовых станций систем сотой связи (GSM), или диапазоны, которые выделены для безлицензионного использования системам радиочастотной беспроводной связи (ISM 2,4–2,5 ГГц, 5,1–5,8 ГГц и др.), или диапазоны систем микросотовой связи (DECT).

Использование цифровыми системами радиосвязи сигналов, которые сложно регистрировать широкополосной радиоприемной аппаратурой. Для увеличения пропускной способности и повышения помехозащищенности в радиочастотной беспроводной связи используются сигналы со сложной структурой: широкополосные сигналы; сигналы передатчиков, функционирующие в пакетном режиме; сигналы с псевдослучайной перестройкой рабочей частоты (ППРЧ), например в стандартах Wi-Fi, Bluetooth, Zigbee, NanoLoc, LTE, UMTS и т. д.

Низкое соотношение сигнал\шум на входе приемного устройства. Поскольку цифровые системы бес-

Рис. 1. ***Внешний вид комплекса «Цифра 2»***

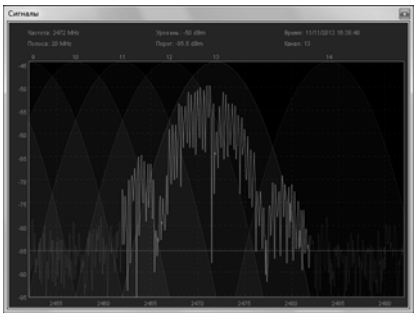

Рис. 2. ***Программное обеспечение «Цифра». Окно анализа сигнатур***

проводной связи зачастую построены по схемам, которые предполагают оптимальный прием сигналов, соотношение «сигнал/шум» на входе собственных приемников таких систем может быть достаточно низким, что затрудняет или делает невозможным обнаружение опасных сигналов широкополосными поисковыми приемниками.

Использование частотного уплотнения каналов. Цифровые каналы с частотным уплотнением (OFDM) имеют спектр сигнала, по которому невозможно определить количество устройств, задействованных в радиообмене, и их уровень сигнала. Например, это применимо для сигналов Wi-Fi некоторых спецификаций.

Нахождение устройства в «дежурном» режиме. «Дежурным» называется такой режим работы устройства, при котором в момент простоя радиообмен устройства сведен к минимуму или вообще отсутствует, что существенно затрудняет их обнаружение. Так ведут себя, например, многие устройства систем радиотелефонной и радиочастотной беспроводной связи (Wi-Fi, Bluetooth, DECT, CDMA, GSM и т. д.).

Очевидно, что для эффективного выявления ЭУНПИ в каналах цифровой радиосвязи с учетом особенностей их функционирования, изложенных выше, необходимо комплексное решение целой группы задач, таких как:

- регистрация радиообмена в каналах цифровых систем связи, в том числе сигналов с низким соотношением «сигнал/шум», широкополосных сигналов и сигналов с нестационарным энергетическим спектром (пакетных);
- обнаружение новых беспроводных устройств, в том числе в «дежурном» режиме, по сигналам широковещательных «маяков» и с помощью принудительного перевода устройств в режим радиообмена и посредством широковещательных опросов сетевого окружения;
- различение устройств «свой – чужой» по сетевому адресу в многоканальных интерфейсах и диапазонах с высокой загруженностью сигналами собственной и соседних сетей связи;
- определение изменений интенсивности использования существующих беспроводных каналов связи, в том числе различение трафика данных и управления, анализ связей устройств и топологии сетей.

Фирма «НЕЛК» разработала программно-аппаратный комплекс «Цифра 2», который позволяет выявлять ЭУНПИ следующими специализированными методами:

- анализом радиоинтерфейса;
- прослушиванием канального уровня;
- активным воздействием по радиоканалу.

Аппаратура «Цифра 2» (рис. 1) включает в себя комплекс программных и аппаратных средств, которые позволяют реализовать поиск ЭУНПИ в каналах цифровой радиосвязи, в частности:

- различение профилей каналов;
- анализ сигнатур;
- регистрацию сетевых адресов устройств в диапазоне ISM и каналах сотовой связи;
- анализ топологии Wi-Fi сетей;
- принудительный перевод беспроводных устройств в режим активного радиообмена.

Комплекс имеет собственную информационно-справочную систему по беспроводным интерфейсам, системам радиосвязи и их сигналам, которая представляет собой уникальную базу знаний, наработанную многолетним опытом специалистов фирмы.

Остановимся подробнее на особенностях реализации алгоритмов поиска.

Различение профилей каналов. Автоматизированный контроль профиля каналов радиоинтерфейсов позволяет значительно снизить нагрузку на оператора при исследовании загруженных диапазонов, таких как downlink каналы систем сотовой связи GSM или диапазон ISM. Все обнаруженные сигналы автоматически классифицируются и привязываются к каналам тех систем связи, которым они принадлежат. Нестандартные и неизвестные сигналы классифицируются отдельно. Если диапазон используется несколькими различными беспроводными интерфейсами одновременно, например ISM, то каналы каждого интерфейса отображаются в индивидуальном окне.

Анализ сигнатур. Данный алгоритм позволяет оператору проконтролировать корректность автоматического различения каналов и распознать нестандартные сигналы по банку данных эталонных сигнатур (рис. 2). Банк данных содержит сигнатуры различных нестандартных передатчиков, в том числе беспроводных видеокамер, периферии и т. п.

Регистрация сетевых адресов устройств в диапазоне ISM и каналах сотовой связи. Регистрация устройств по сетевым адресам позволяет в автоматизированном режиме структурировать и классифицировать обнаруженные устройства различных систем связи, оперативно выявлять новые устройства. Анализ сетевых заголовков на канальном уровне взаимодействия беспроводных устройств позволяет комплексу эффективно обнаруживать Wi-Fi-устройства в «дежурном» ре-

жиме по широковещательным «маякам» (рис. 3–4).

Анализ топологии сетей Wi-Fi. Этот алгоритм поиска позволяет классифицировать данные, передаваемые с устройства, по степени потенциальной опасности, в частности различать трафик данных от передачи служебной и широковещательной информации, выявлять изменения в интенсивности использования существующих каналов связи, определять роли устройств и выявлять несанкционированные или потенциально опасные связи устройств Wi-Fi. В режиме анализа связей комплекс позволяет анализировать открытые сетевые порты и определять IP-адреса источника и получателя информации в сети (рис. 5).

Принудительный перевод беспроводных устройств в режим активного радиообмена. Специальные инструменты комплекса осуществляют активное воздействие на беспроводные устройства, находящиеся в режиме радиомолчания, позволяют переводить мобильные терминалы GSM в режим активного радиообмена с базовой станцией и провоцировать устройства Bluetooth и Zigbee к обмену информацией по радиоканалу, который может быть обнаружен и зарегистрирован комплексом.

Каждый из рассмотренных выше алгоритмов поиска устройств негласного получения информации, использующих для своей работы каналы цифровой радиосвязи, может быть реализован отдельным специализированным устройством или комплексом. Единственное на сегодняшний день комплексное устройство, одновременно реализующее данные алгоритмы и охватывающее максимальное количество стандартов цифровой радиосвязи (GSM, DCS, UMTS, ISM, LTE, CDMA, DECT, Wi-Fi, Bluetooth, Zigbee), – автоматизированный комплекс «Цифра 2».

В схемотехнические решения и программное обеспечение комплекса «Цифра 2» заложены широкие возможности для его дальнейшего совершенствования. Одна из модификаций данного изделия – «Клен-СР» – принята на снабжение Вооруженных Сил РФ.

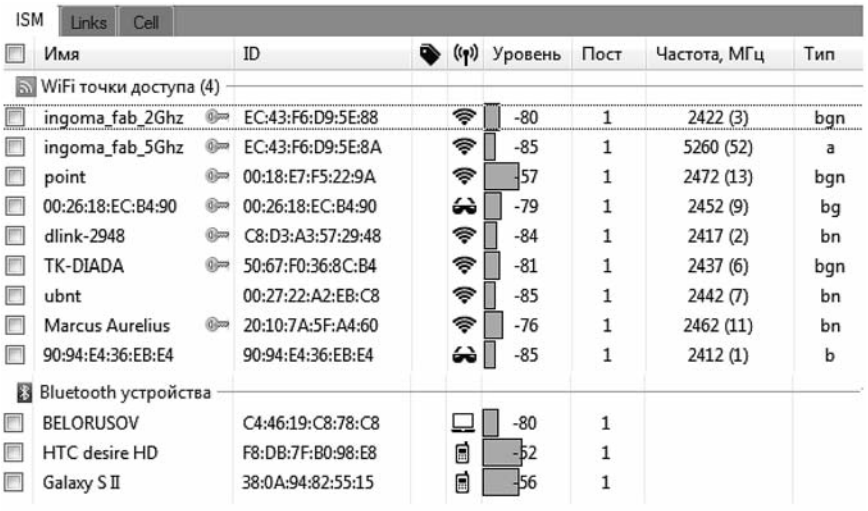

Рис. 3. ***Программное обеспечение «Цифра». Устройства диапазона ISM***

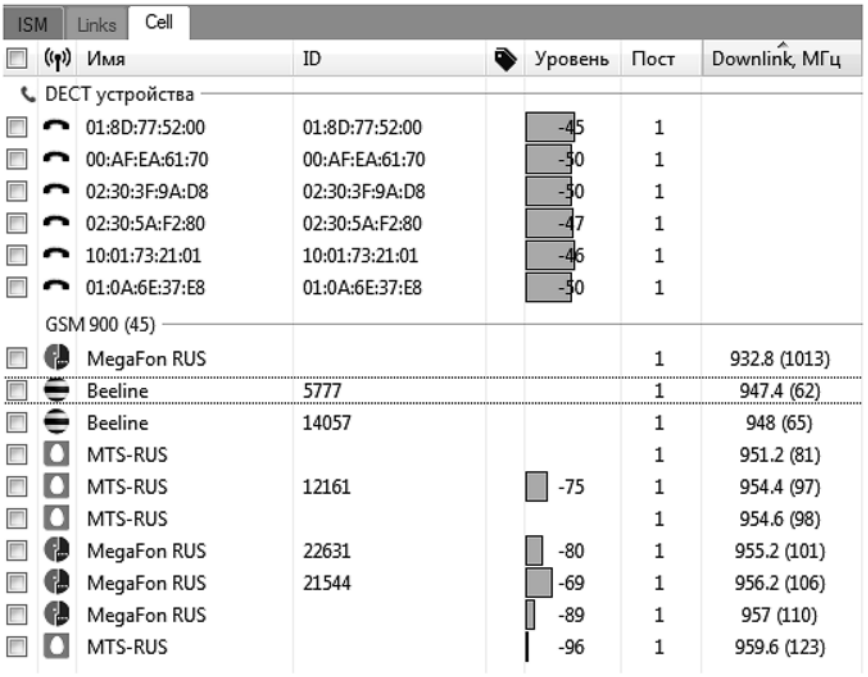

Рис. 4. ***Программное обеспечение «Цифра». Устройства диапазонов GSM и DECT***

Принимая во внимание современные угрозы безопасности информации, возникающие с появлением новых электронных устройств негласного получения информации, использующих для своей работы каналы цифровой радиосвязи, приведенная в статье технология практической реализации методов их выявления делает нетривиальную задачу поиска таких устройств легко решаемой, а комплекс «Цифра 2» – универсальным средством поиска с большим потенциалом наращивания его возможностей. ■

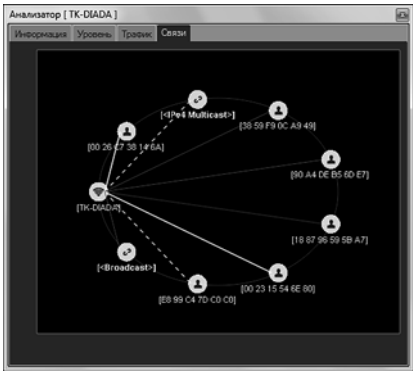

Рис. 5. ***Программное обеспечение «Цифра». Граф связей точки доступа Wi-Fi***