Выявление сигналов электронных устройств негласного получения информации в каналах цифровой радиосвязи

Раин Артем Сергеевич
студент КубГУ, Россия, г. Краснодар

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 постояннодействующие 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 down-link 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 беспроводной 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.