УДК 004.056.53

Кривцун Александр Витальевич,
Захаров Алексей Викторович
Группа компаний STT GROUP (ИКМЦ-1 ЮТТА), г.Москва
E-mail: stt@detektor.ru

ИСПОЛЬЗОВАНИЕ НОВЫХ ВОЗМОЖНОСТЕЙ КОМПЛЕКСА РАДИОМОНИТОРИНГА И ЦИФРОВОГО АНАЛИЗА СИГНАЛОВ «КАССАНДРА-М» ДЛЯ ОБНАРУЖЕНИЯ СОВРЕМЕННЫХ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ С ПЕРЕДАЧЕЙ ИНФОРМАЦИИ ПО РАДИОКАНАЛУ

Рассмотрены актуальные проблемы обнаружения утечки информации по стандартным цифровым каналам связи и методы их решения с помощью новых возможностей программного обеспечения комплекса радиомониторинга «Кассандра-М».

КЛЮЧЕВЫЕ СЛОВА:
защита информации, радиомониторинг, цифровые каналы передачи, специальное техническое средство, комплекс «Кассандра»

В статье рассматривается применение комплекса «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу с точки зрения практика. Описание технических характеристик комплекса можно найти в [1], [2], а также на сайте производителя www.detektor.ru.

Современные специальные технические средства (СТС), использующие для нелегального съёма информации радиоканал (для простоты именуемые радиозакладками), за последние несколько лет шагнули в своём развитии настолько далеко вперёд, что многие комплексы радиомониторинга просто не в состоянии их обнаружить с вероятностью, обеспечивающей защиту информации.

Выделим основные направления создания радиозакладок. Во-первых, использование сложных типов сигналов для передачи перехваченной информации (широкополосных, шумоподобных, ППРЧ и т.д. [3]), затрудняющих обнаружение их средствами радиомониторинга. Последнее относится и к активно используемым радиозакладкам с накоплением перехваченной информации, её сжатием и последующим крайне малым временем передачи. Во-вторых, как представляется, наиболее опасное направление – использование легальных каналов связи (DECT, Bluetooth, Wi-Fi, GSM и др.) для передачи перехваченной информации. Высокая опасность в данном случае в том, что специалист, даже используя современные технические средства, разрешённые к применению, не в состоянии отличить работающее по своему прямому назначению легальное радиоизлучающее устройство от СТС. Сделать это без применения специальных средств анализа цифровых пакетов в реальном масштабе времени невозможно. Если специфические формы сигналов «обыкновенных» радиозакладок сразу привлекают к себе внимание специалиста, имеющего соответствующую технику, «нестандартным» видом (рис. 1), то спектры

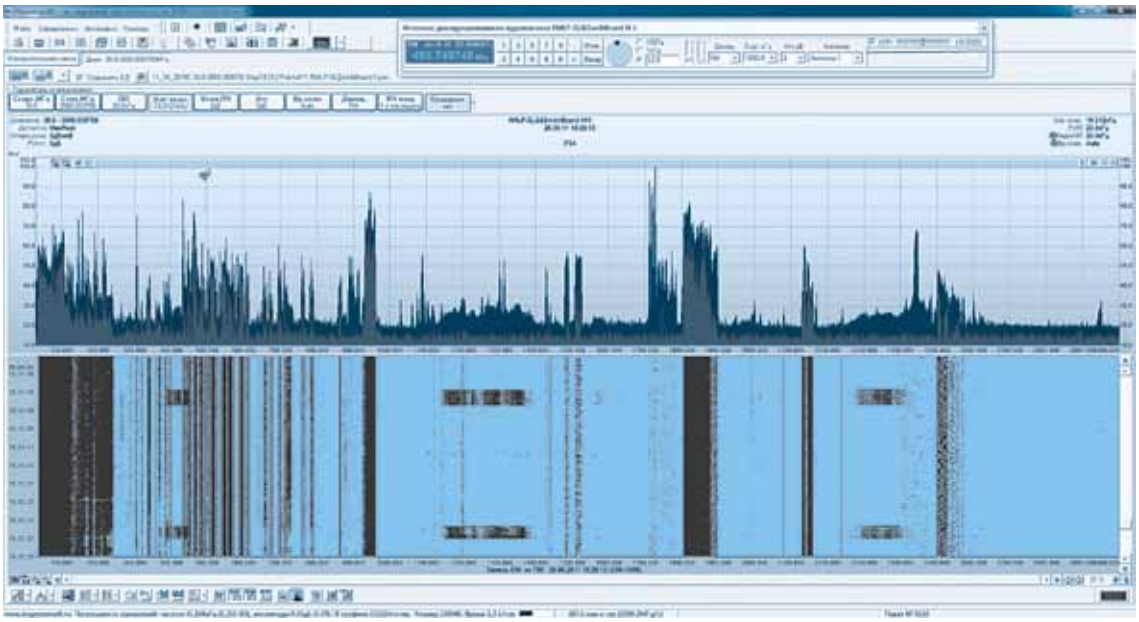

Рис. 1. Отображение работы широкополосной радиозакладки с кратковременным накоплением. Период - 3 минуты.

сигналов устройств, работающих в легальных каналах передачи данных, выглядят одинаково независимо от того, излучает их радиозакладка или вполне «мирное» устройство.

Необходимо констатировать, что средств анализа цифровых пакетов применительно к задачам поискового радиоконтроля в настоящий момент не существует. Те немногочисленные средства анализа цифровых сетей передачи данных (Rohde&Schwarz TSMW и ПО «ROMES», различные специализированные тестеры цифровых средств связи, ряд других программных средств цифрового анализа сигналов) относятся к классу «гражданских» и предназначены для демодуляции широковещательных пакетов базовых станций и анализа структуры сети. В задачах поискового радиоконтроля актуальным вопросом необходимо считать не только анализ широковещательных пакетов базовых станций (BS), но и пакетов мобильных устройств (MS), получение из них в разрешённых рамках максимума полезной информации, позволяющей идентифицировать каждое такое устройство среди многих работающих одновременно, и в конечном итоге, локализовать местоположение любого из них.

Попыткой создать программные средства демодуляции и анализа цифровых средств радиосвязи можно считать пакет цифровой обработки сигналов «DTest» в программном обеспечении (ПО) «РадиоИнспектор». На сегодняшний день ПО с этой опцией позволяет демодулировать служебные пакеты, анализировать, идентифицировать и локализовывать базовые станции и мобильные устройства, работающие в стандартах DECT и TETRA. В ближайшее время перечень обрабатываемых стандартов пополнят GSM, Bluetooth, что вместе с ПО «RInspectorWi-Fi» замкнёт список основных легальных каналов, которые могут использоваться для организации утечки информации. Кроме того, в пакет цифровой обработки сигналов «DTest» включены ещё несколько полезных функций. Во-первых, возможность демодуляции и отображения картинки аналогового телевизионного сигнала, в том числе с использованием метода инверсии синхроимпульсов. Во-вторых, для любителей, возможность отображения векторной картинки принимаемого сигнала.

Данный пакет цифровой обработки сигналов работает с аппаратурой, позволяющей получать квадратурные отсчёты (IQ) сигналов ПЧ в широкой полосе частот в режиме

реального времени или блоками большой длины. Примером такой аппаратуры является ряд анализаторов спектра и измерительных приёмников производства Rohde&Schwarz и стремительно развивающийся комплекс радиомониторинга и цифрового анализа сигналов «Кассандра-М», который уже стал широко известен многим специалистам благодаря своим техническим параметрам и уникальному ПО «RInspectorRT», не имеющему мировых аналогов (видеоработы комплекса можно посмотреть в интернете по адресу http://www.youtube.com/watch?v=bcX7Lo_GMtI). ПО «RInspectorRT» работает со многими анализаторами спектра, измерительными и связными приёмниками ведущих мировых производителей (R&S, Agilent, Advantest, Anritsu, Aeroflex/IFR, AOR, ICOM), но только считанные единицы современной аппаратуры имеют возможность получать непрерывный поток квадратур в полосе сигнала 2 МГц. Именно поэтому «Кассандра-М» является превосходным инструментом для цифровой обработки и анализа сигналов современных стандартов связи.

В качестве отступления от основной темы статьи рассмотрим некоторые проблемные вопросы радиомониторинга (поискового радиоконтроля) [5]. Вспомним, какие именно сложности могут возникнуть при работе?

Во-первых, загруженность диапазона. Достаточно привести пример типового учреждения. Десятки компьютеров, беспроводных телефонов DECT, мобильных телефонов различных стандартов (только в Москве их 5: CDMA-2000, GSM-900/1800, 3G (UMTS), 4G (WiMax)). Добавим к перечисленному усилители той же мобильной связи (не редкость ситуация, когда в одном здании размещены усилители всех стандартов), легальные радиомикрофоны, беспроводные гарнитуры, устройства Wi-Fi, различные электронные считыватели систем контроля и управления доступом, проводные охранные видеокамеры (которые зачастую имеют уровни ПЭМИ, соизмеримые с излучением радиозакладок) и т.д. и т.п. Не надо забывать и о «качестве» современного электронного оборудования. Чего только стоят некоторые импульсные блоки питания, которые «видны» в эфире иногда в полосе до 500 МГц (!). Плюс учтем всё то, что проникает в помещение извне: теле- и радиовещание (в том числе и цифровое телевидение DVB), авиационные переговоры, «радионяни», радиолюбительская связь, ведомственные каналы связи, всё активнее уходящей в цифровые стандарты (пример: APCO P25, TETRA, DMR), телеметрия и передача данных всевозможных охранных и контрольных устройств, пейджинг (как ни удивительно, до сих пор работает), даже спутники, передающие метеоснимки. Их тоже можно принять, находясь на объектах.

Во-вторых, время контроля. В настоящее время, как показала практика и в чём убеждается всё больше специалистов, радиомониторинг обязательно должен быть непрерывным и круглосуточным. Почему? Простой пример: как можно обойти контроль эфира, который осуществляется только во время проведения важных мероприятий? Да очень просто – не работать в это время на передачу. Даже не надо никакого сжатия информации, использования «хитрых» модуляций. Сколько длятся обычные совещания/переговоры/мероприятия? Не дольше, чем рабочий день. Каково время записи современных цифровых диктофонов? Правильно – месяцы. Кто мешает дистанционно (или по расписанию) включить/выключить диктофон командой по радиоканалу, записать всё что требуется, а во внерабочее время (например, ночью) спокойно таким же способом активировать передатчик. И это самый простой пример, не требующий сколь-либо значимых финансовых затрат от злоумышленников, который могут произвести на свет мастера технологий «на коленке». Более профессиональный вариант: SIM-BURST и INCA ULL. Это радиозакладки с промежуточным накоплением информации [3, с.304]. При ширине полосы сигнала в 12 МГц сжатие записанной информации может достигать 100 к 1. То есть при накоплении информации длительностью 100 с время её передачи составит 1 секунду. Несложно подсчитать, что если даже круглосуточно записывать переговоры в течение месяца, то передача накопленной информации займёт чуть больше семи часов. А ведь это относительно узкополосная радиозакладка. Представим, что есть возможность взять и увеличить спектр раз в 300 – до 3 ГГц (конечно, это чересчур смело, но кто знает…). Получается, что теперь она способна

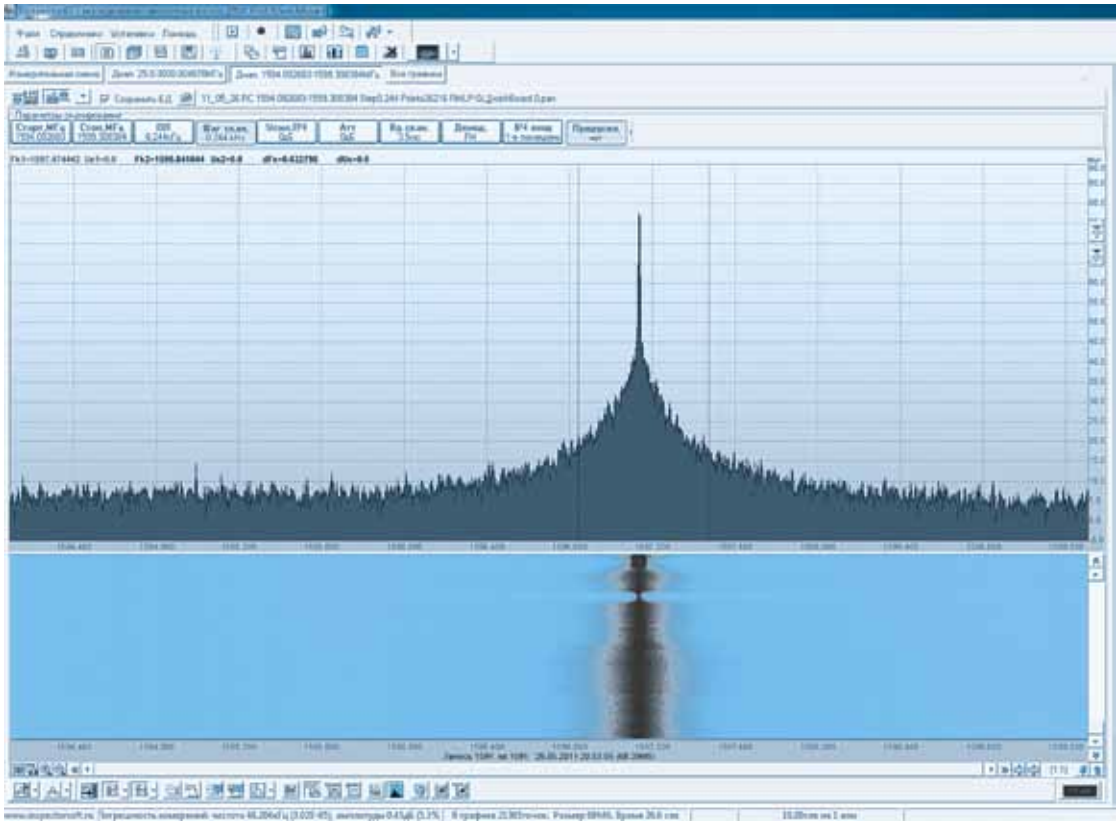

Рис. 2. Работа аналоговой радиозакладки на частоте 1597,2 МГц. Спектр сигнала соответствует изменениям речевого сигнала в контролируемом помещении. Уровень сигнала значительно превосходит стандартные эфирные и находится в диапазоне частот, где практически нет легально работающих аналоговых средств.

«выплюнуть» не более чем за три минуты всю информацию, накопленную за месяц. Как её искать в эфире и как отличить случайный сигнал (например, от блокиратора радиовзрывателей, установленного на проехавшей машине) от сигнала нашей искомой радиозакладки, если не проводить непрерывный круглосуточный радиоконтроль?

Вывод: Только круглосуточный радиоконтроль позволяет наблюдать за тем, как «живёт» сигнал, как он соотносится с различными важными событиями на охраняемом объекте, обнаруживать закономерности во времени появления в эфире, сравнивать текущие спектры сигналов с ранее полученными. Наличие перечисленных возможностей является необходимым и обязательным требованием к современному поисковому комплексу радиомониторинга.

Остановимся ещё на одном моменте. В простых случаях, когда закладка работает непрерывно, находясь на одной частоте, проблем с обнаружением её сигнала не должно возникнуть (рис. 2).

Но если противник идёт в ногу со временем? Сидеть и смотреть на экран, ожидая, когда появится сигнал? Появиться он может через сутки или, вообще, через неделю или месяц. Не зная алгоритма выхода радиозакладки в эфир, крайне сложно обнаружить её сигнал. Поэтому очень важную роль в комплексах радиоконтроля стала играть функция отображения спектра сигналов в виде так называемого «водопада», позволяющего наблюдать за изменениями радиочастотного спектра с привязкой ко времени. Появляется возможность вести базу данных непрерывно и круглосуточно, не теряя ни один принятый комплексом сигнал.

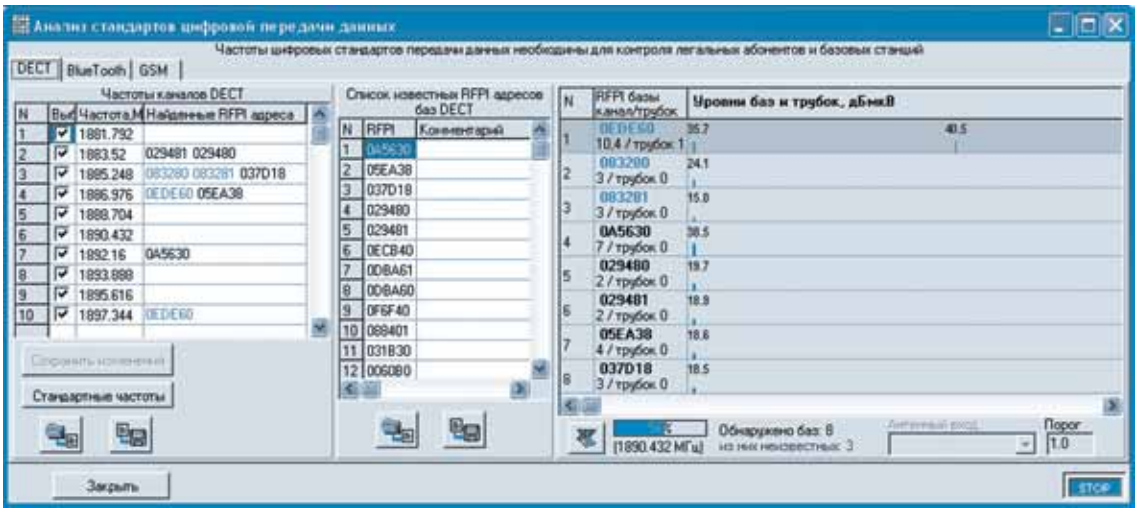

Рис. 3. Основное окно анализа стандарта DECT

Иногда достаточно взглянуть на «водопад», чтобы визуально обнаружить работу закладки. Пример на рис. 1.

Ну и наконец, в-третьих, диапазон контроля. Ни в коем случае нельзя дробить диапазон работы комплекса на куски – весь спектр надо смотреть целиком. В диапазонах, нарезанных, допустим, по 100 МГц, можно не увидеть закономерностей в спектре, которые бросаются в глаза при одновременном просмотре полосы шириной, например, 3 ГГц. Наличие в ПО комплекса «Кассандра-М» функции «водопада» с возможностью регулировки цветового соответствия различным уровням сигналов позволяет увидеть в эфире малейший всплеск и проанализировать его поведение в конкретный момент времени. При этом скорость комплекса, вплотную подошедшая к 3 ГГц в секунду при полосе пропускания 40 кГц, позволяет зафиксировать даже очень короткие выходы в эфир.

Вернёмся теперь к вопросу использования легальных каналов связи для работы радиозакладок.

Для начала рассмотрим радиотелефонию стандарта DECT и проблемы, связанные с выявлением радиозакладок, созданных с применением приёмопередатчиков, работающих в этом стандарте. Практика показала, что плотность установки устройств DECT такова, что на десяти каналах, используемых в стандарте, фиксируется в зоне приёма до двухсот (!) устройств данного стандарта. Это позволяет идеально маскировать работу радиозакладок. При существующей в настоящее время плотности использования беспроводной связи стандарта DECT и активном производстве СТС на его базе уже недостаточно просто фиксировать факт работы данного стандарта связи. Необходимо идентифицировать и контролировать все находящиеся на охраняемом объекте устройства DECT.

В настоящее время эта проблема стоит как нельзя остро. Есть ли готовые решения, позволяющие её решить? Многие специалисты по поисковым мероприятиям и радиомониторингу обходят эту проблему стороной, только фиксируют факт работы DECT в диапазоне частот 1880-1900 МГц. Во многих поисковых приборах на дисплее просто индицируется: DECT. Самые «продвинутые» пишут: DECT BASA. А этого абсолютно недостаточно, ведь зачастую на охраняемом объекте могут работать десятки легальных устройств, использующих данный стандарт. И в контролируемом помещении тоже может постоянно находиться легальная трубка**.** Как отмечалось выше, даже методом анализа спектра невозможно отличить пакеты, излучаемые «законными» и «незаконными» передатчиками**.**

В новой опции комплекса «Кассандра-М» - программном обеспечении DTest (Digital Test) [4] - предложено решение проблемы идентификации легальных и нелегальных устройств стандарта DECT. Теперь пользователи получили уникальный и не имеющий аналогов на рынке поисковой техники инструмент. Как это выглядит? Всё реализовано таким образом, чтобы максимально автоматизировать работу комплекса и разгрузить и без того сложную работу оператора: нажал кнопку – получил результат. Комплекс получает в реальном времени спектры сигналов с полосой 2 МГц, что позволяет демодулировать и анализировать открытые заголовки пакетов устройств одного частотного канала стандарта DECT. На весь анализ уходит порядка семи секунд на все 10 каналов, используемых в данном стандарте.

Какие возможности появляются у оператора комплекса радиомониторинга при использовании программы DTest для анализа DECT? Список довольно внушительный:

1. Фиксация количества баз, идентификатора базы RFPI и уровня сигнала базовых станций DECT (BS DECT). В таблицу заносятся все без исключения базовые станции, которые в данный момент включены (рис. 3).

2. Фиксация количества и принадлежность к базовой станции работающих мобильных терминалов (трубок, MS DECT). Так как трубка не передаёт в эфир никаких идентификаторов после однократной регистрации, то фиксируется факт работы трубки с привязкой её к «родной» базе. Особо отметим фиксацию всех работающих трубок, подключённых и работающих с базой. То есть если через базу одновременно работают две трубки или более, то оператор видит их все и уровни сигналов каждой трубки.

3. Оценка расстояния до BS и MS по уровню сигнала.

По уровню сигнала базы и трубки можно оценить их расстояние до антенны комплекса радиомониторинга.

4. Локализация работающих BS и MS методом амплитудной пеленгации.

В некоторых случаях при необходимости есть вероятность локализовать радиозакладку, подключив к комплексу направленную антенну.

5. Измерение уровня сигнала каждой обнаруженной BS и MS.

По уровню сигнала и графику работы можно эффективно выявлять радиозакладки. В некоторых случаях BS будет иметь довольно слабый уровень, не характерный для устройств, работающих в учреждении, а MS (трубка), наоборот, будет иметь неожиданно большой уровень. И главное - длительное время работы в эфире. Останется локализовать MS и убедиться, что это нелегальная трубка, которую «забыли выключить».

6. Ведение протокола сеанса связи между MS и BS.

Все сеансы связи, обнаруженные базы и подключения к ним трубок заносятся в протокол (документ стандарта Micrsoft Word®). Он имеет довольно внушительный размер, так как при постоянной работе происходит регулярное обновление списков выявленных устройств с занесением в протокол. Ни одно событие в эфире не теряется.

7. Ведение списка легальных (идентифицированных) BS и выделение вновь появившихся BS.

Такой список позволяет быстро выявлять появление новых баз, которых не было ранее на объекте. Пополнять его довольно просто: чтобы выявить легальную базу, достаточно взять прописанную на ней трубку и позвонить рядом с комплексом. У Вас сразу выявится база, к которой подключена трубка с большим уровнем сигнала. Выключите трубку – сигнал от неё пропадёт, всё – это Ваша база, заносите её в список легальных. Можно к каждой базе добавлять свои комментарии, чтобы не запоминать шестиразрядный RFPI-идентификатор базы.

8. Фиксация частотного распределения BS и MS. Определение загрузки каналов.

Определение загрузки каналов позволяет выявить проблемы с перебоями связи, ведь зачастую у специалистов по радиоконтролю и эти работы входят в круг задач.

9. Проверка всех стандартных частот работы стандарта DECT с возможностью анализа любых добавленных частот на принадлежность к данному классу передачи.

Данная функция введена для того, чтобы оператор, в случае обнаружения в любом

Таблица 1. Частоты работы GSM

Характеристики	E-GSM	GSM-900	GSM-1800 (DCS-1800)
Частоты передачи MS и приёма BS, МГц	880-890	890-915	1710-1785
Частоты приёма MS и передачи BS, МГц	925-935	935-960	1805-1880
Дуплексный разнос частот приёма и передачи, МГц	45	45	95
Количество частотных каналов связи (один канал занимает 200 кГц)	50	124	374

Таблица 2. Частоты работы 3G и 4G

Характеристики	3G (UMTS)	4G (WiMax)
Частоты передачи MS и приёма BS, МГц	1935-1950, 1950-1965, 1965-1980, 2010-2015, 2015-2020, 2020-2025	2500-2700
Частоты приёма MS и передачи BS, МГц	2125-2140, 2140-2155, 2155-2170	2500-2700

участке спектра сигнала, напоминающего DECT по своим параметрам, имел возможность проанализировать его на принадлежность к данному стандарту связи.

Перейдём теперь к одной из самых сложных проблем – радиозакладкам на основе мобильных стандартов связи. В короткой статье сложно описать все особенности практической работы. Мы отметим главное. Сложность задачи идентификации (телефон или радиозакладка?) состоит в большой концентрации легальных устройств, работающих в зоне ответственности оператора. Как отличить сигнал легального телефона от закладки? Никак, если не применять специальных методов. Закладка также регистрируется в сети оператора мобильной связи, как и легальные трубки, и также выглядит её спектр. Что же может сделать в данном случае оператор с помощью комплекса «Кассандра-М»? Очень многое. Пройдёмся детально по всем стандартам.

CDMA-2000 (оператор «Скайлинк» и др.). Частотный диапазон работы базовых станций (BS) 463,4-467,15 МГц. Например, в Москве работают три канала шириной по 1,25 МГц. Самые опасные закладки: уровни сигнала, его тип (шумоподобный) и занимаемая полоса (1,25 МГц) привели к тому, что большинство детекторов поля (даже стоимостью более 100 тыс.руб.) не видят этот стандарт иногда даже, что называется, «впритык».

Комплекс радиоконтроля и связные приёмники, конечно, не страдают такой болезнью, но здесь надо знать некоторые особенности стандарта. У специалистов есть такой приём: включить подавитель сотовой связи, связь, естественно, пропадёт, а после выключения подавителя все трубки мобильной связи, находящиеся в помещении, начинают перерегистрироваться, тут-то их и отслеживают. Так вот, к CDMA-2000 это не относится. Это неоднократно проверялось на практике. Надо контролировать диапазон частот передачи трубки 28 минут, чтобы дождаться её перерегистрации – так настроена сеть. В комплексе при этом должна быть включена функция «Отобразить график максимумов». Ждем. Если через полчаса его работы на частоте 453,4-457,15 МГц (на 10 МГц ниже работы базовых станций стандарта) появится сигнал, то он будет виден на графике максимумов и, конечно, на «водопаде» (рис. 4). По уровню этого сигнала можно оценить, находится ли он в непосредственной близости или «это не ваша головная боль». В любом случае, просто регистрация в сети ещё не криминал, а вот длительная работа в эфире – повод понаблюдать за сигналом. Конечно, это может быть модем секретаря-референта руководителя. А если нет? С направленной антенной, подключённой к «Кассандре-М», можно попытаться локализовать источник излучения.

Далее рассмотрим GSM-900/1800. Частоты работы сетей приведены в табл.1.

Имея эти данные, с помощью комплекса «Кассандра-М» можно выявлять нестандартную работу сети – фактически, обнаруживать работу средств перехвата мобильной связи.

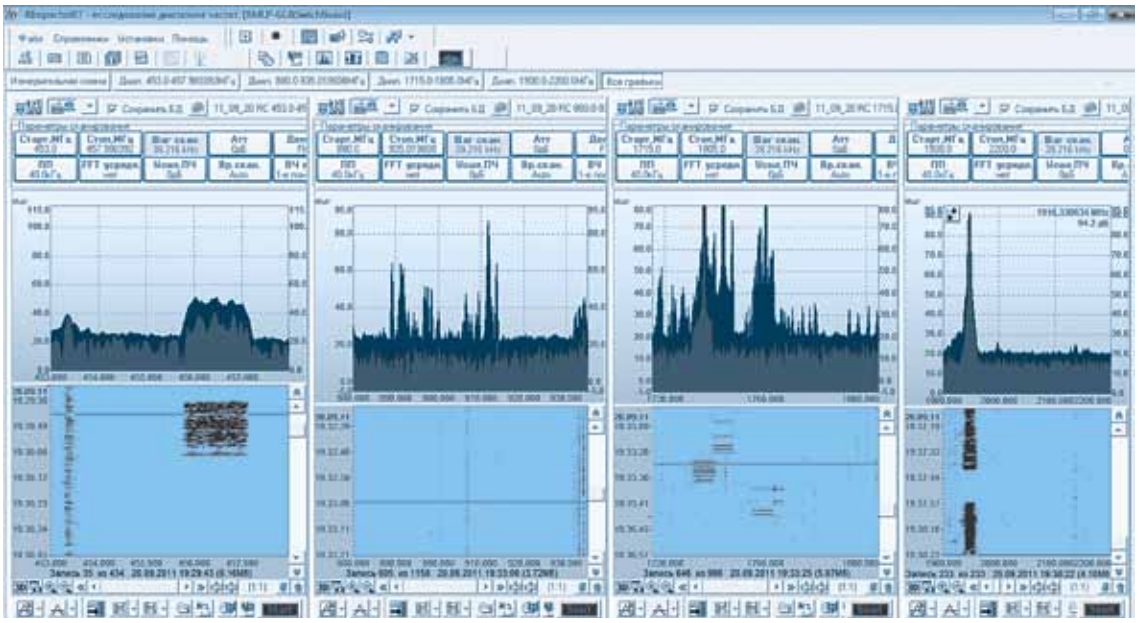

Рис. 4. Многозадачный режим с отображением всех графиков одновременно. Отображается контроль четырёх стандартов мобильной связи. Виден кратковременный момент работы трубки стандарта CDMA-2000, появление в ближней зоне трубки стандарта GSM-1800 и длительная работа в ближней зоне (с коротким перерывом) трубки стандарта 3G.

Видя все каналы, оператор получает следующие параметры топологии сети: принадлежность к стране, к оператору, идентификатор базовой станции, код сектора, Location Area (LA – идентификатор группы сот, объединённых по географическому признаку).

Комплекс видит все служебные каналы, каналы трафика и привязку их друг к другу. При возникновении подмены базовой станции (БС) оператор может увидеть или новый идентификатор БС с мощным уровнем сигнала, или просто значительное увеличение мощности сигнала одной из БС. Также может измениться привязка служебных каналов к трафиковым.

Как определить, что передача, обнаруженная комплексом, вероятнее всего идёт от GSM закладки? Надо искать сигнал в ближней зоне на частоте передачи трубки. Помимо того, что уровень сигнала будет значительно отличаться от «дальних» трубок, спектр сигнала также будет шире – это признак ближней зоны (рис. 5). Далее следует просто посмотреть, как «живёт» этот сигнал, то есть проанализировать его поведение во времени: длительность работы, появление в эфире в периоды времени, когда в помещении никого нет. Можно включить блокиратор связи, определить на каком расстоянии он действует, отрегулировать мощность, чтобы вне помещения подавление отсутствовало, а потом выключить подавитель минут через 10. Почему именно через 10 минут? Потому, что в стремлении сэкономить энергию батарей, производители всё больше увеличивают интервалы пропадания сигнала базовой станции, при которых будет происходить перерегистрация. А вот сильно полагаться на данный метод применительно к 3G (UMTS) нет смысла, поскольку всё идёт к тому, что трубки будут вести себя как в стандарте CDMA-2000. Ведь именно этот стандарт взят за основу стандарта 3G (UMTS) – так называемый WIDE CDMA (WCDMA) – широкий CDMA. Надо комбинировать оба способа: долговременный контроль выделенного участка и периодическое включение блокираторов мобильной связи с последующим контролем регистрации после их выключения. Что касается 3G (UMTS) и 4G (применительно к России в настоящее время это, конечно же, стандарт WiMax, развёртывание LTE плани-

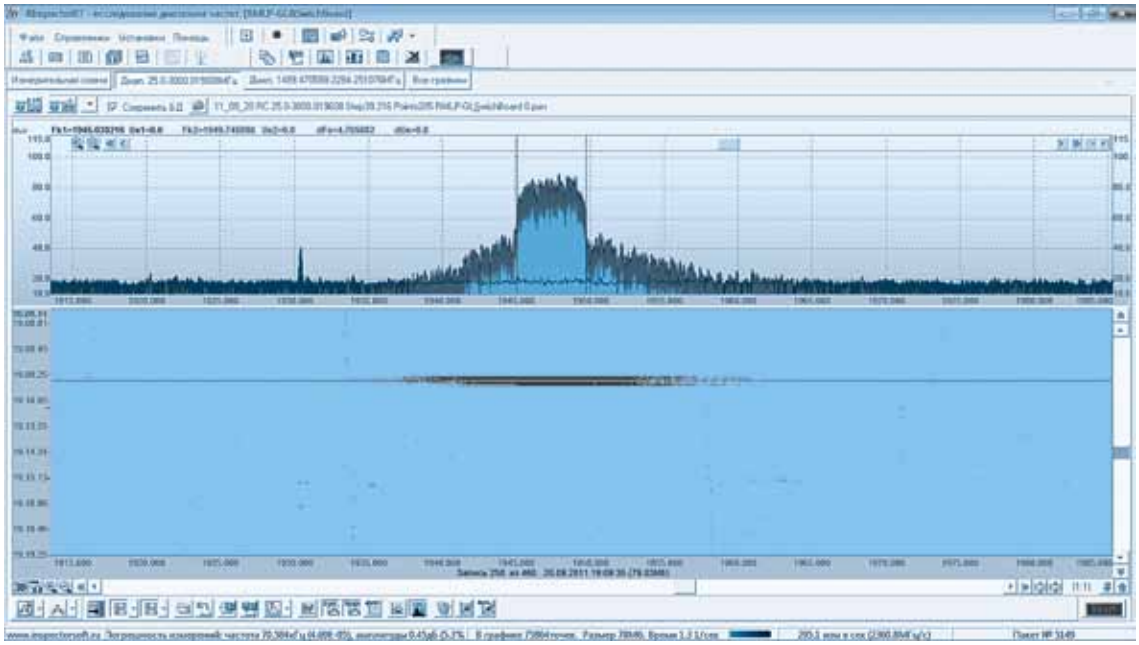

Рис. 5. Работа мобильного телефона (MS) стандарта 3G в ближней зоне.

руется через несколько лет), распределение частот которых приведено в табл. 2, то на данном этапе их тоже надо искать по «энергетике» – резкому увеличению уровня сигнала в ближней зоне. При этом спектр сигнала становится не только мощнее по уровню, но и шире. Пример приведён на рис. 5. Наглядно видны два «крыла» расширения спектра в ближней зоне.

Отдельно хочется отметить удобство многооконного режима и возможность ставить любое количество задач со своими параметрами для контроля мобильной связи. Запустив все задачи по контролю мобильной связи, можно или сразу смотреть все участки (рис. 4), или выбирать нужное окно. При этом активные задачи будут продолжать работать.

Коснёмся вопроса возможности утечки информации с помощью устройств специальных цифровых стандартов радиосвязи, на которые всё активнее переходят ведомственные и частные радиосети. С какими угрозами могут столкнуться в данном случае специалисты по поисковому радиомониторингу? Рассмотрим их на примере стандарта TETRA. Основной режим работы в данном стандарте предусматривает связь через базовый ретранслятор. Но существует и другой режим, при котором абоненты связываются в прямом канале. Так как стандарт довольно современный (при проведении олимпиады в Сочи стандарт TETRA будет основным), то в него внедрили массу полезных возможностей. Например, есть возможность дистанционно включить другую станцию (внимание!) – без каких либо демаскирующих признаков, что станция работает на передачу. В этом режиме она не издаёт никаких предупреждающих сигналов, не работает дисплей, и не подсвечиваются кнопки. При этом микрофон станции имеет максимальную чувствительность, что позволят спокойно подслушивать разговор в нескольких метрах от него. Аналогично можно включать в режим «акустики» и станции других современных стандартов: DMR, APCO P25 - надо только знать как.

Как же определить, что на охраняемом объекте при функционировании служебной связи используется прямой канал, и выявить устройство, работающее в нём на передачу? В настоящее время этот вопрос решён в комплексе «Кассандра-М» применительно к стандарту TETRA. При анализе сигнала на принадлежность к данному стандарту на

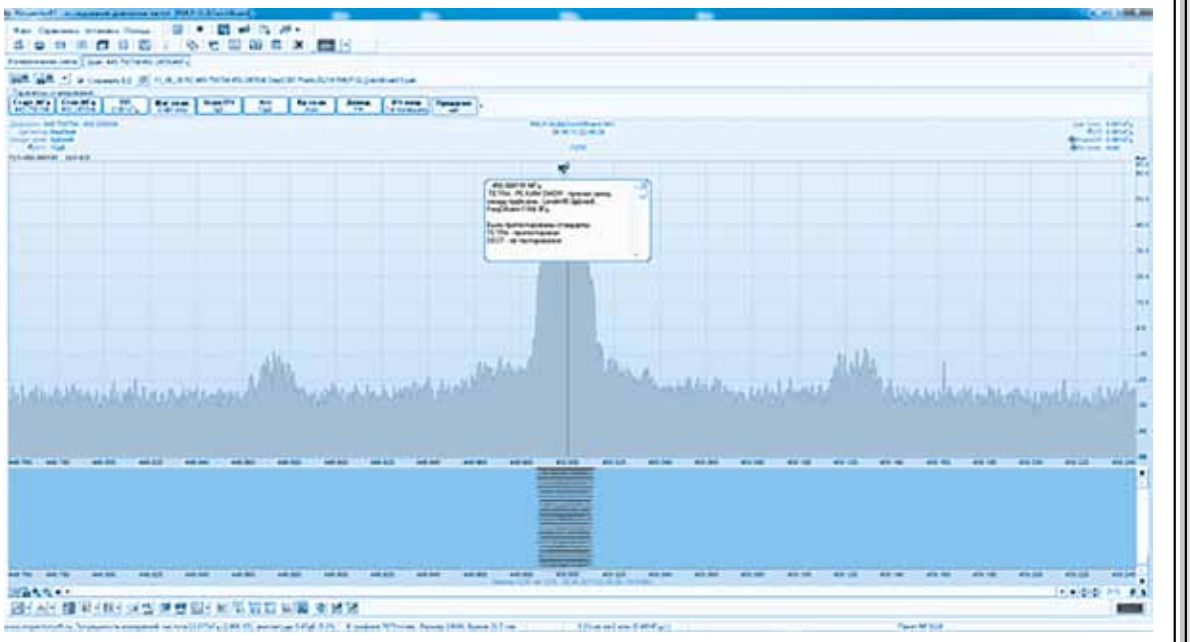

Рис. 6. Отображение обнаружения режима DMO 5-ти ваттной радиостанции Motorola MTH800, работающей в ближней зоне (5 метров)

экран выводится вся информация о базовых станциях и если фиксируется, что станция работает в режиме DMO (в прямом канале), то на экране появляется выделенное красным цветом предупреждение «TETRA РЕЖИМ DMO!!!» с информацией об устройствах, работающих на передачу (рис. 6).

Проблема утечки информации через цифровые легальные каналы связи требует к себе всё более пристального и постоянного внимания, поэтому создатели комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» непрерывно его совершенствуют и пополняют список стандартов связи, по которым оператор может получить исчерпывающую информацию.

Остался за пределами данной статьи вопрос применения ПО «RInspector» для анализа стандартов связи Bluetooth, Wi-Fi и многие другие его возможности. Подробно эти вопросы, а также другие, кратко освещённые, будут рассмотрены в последующих публикациях.

Литература

1. *Кривцун А.В. Комплекс радиомониторинга «Кассандра-М» // Защита информации. Инсайд. – 2010. - №1. – С 46-47.*
2. *Ткач В.Н., Кривцун А.В., Дыбовский В.Г. STT GROUP «Шагаем в 2011 год с принципиально новыми изделиями в области защиты информации и антитеррора» // Защита информации. Инсайд. – 2011. - №1. – С 40-43.*
3. *Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. - М: «НПЦ Аналитика», 2008. - 436 с.*
4. *ПО РадиоИнспектор [Электронный ресурс]. - Режим доступа: http://www.inspectorsoft.ru/soft.php?id=289*
5. *Кривцун А.В. Незаконно действующие передатчики. Алгоритмы поиска, требования к аппаратуре // Специальная техника. – 2010. - №2. – С 49-63.*