Кривцун Александр Витальевич,
ведущий специалист STT GROUP
(«ИКМЦ-1» «Группа Защиты-ЮТТА»)

РАДИОМОНИТОРИНГ: ЧАСТОТНЫЙ ДИАПАЗОН

Для эффективного решения задач защиты информации необходим качественный анализ угроз и возможных каналов утечки. Этот процесс связан со сбором всей возможной информации вокруг носителей и объектов защиты. Объём полученной информации об угрозах ограничивается, с одной стороны, возможностями контрольной аппаратуры, с другой – возможностью эффективно эту информацию обработать. Применительно к аппаратуре контроля радиоэфира эффективность получаемой информации определяется, прежде всего, её качеством: полнотой отображения и отсутствием искажений. Полнота отображения определяется, в частности, диапазоном исследуемых частот.

Если провести анализ средств контроля эфира, представленных на рынке (выборка в табл. 1), можно сделать вывод: основные диапазоны работы этих средств – ОВЧ (30 - 300 МГц) плюс УВЧ (300 – 3000 МГц). И это обосновано - большинство доступных средств съёма информации используют именно эти диапазоны. Прежде всего, из-за дешевизны и простоты создания передатчиков, как полностью разработанных авторами, так и реализованных на базе доступных модулей стандартных радиоканалов (табл. 2). Да и распространение радиоволн на этих частотах позволяет без специальных мер организовать уверенный канал передачи добытой информации.

Однако иногда категория информации и её ценность заставляют охотников за чужими секретами не оглядываться на затраты для обе-

Таблица 2. Типовые частотные диапазоны резонаторов для гетеродинов передатчиков

292-294 МГц	857-868 МГц
302-326 МГц	914-916 МГц
378-391 МГц	979-981 МГц
402-434 МГц	

Таблица 1. Частотный диапазон средств контроля радиоэфира.

Поисковые средства	Основной диапазон поиска	Наличие прибора, расширяющего диапазон
Детекторы поля		
NR-D	50 - 3500 МГц	
ST 110	50 - 2500МГц,	антенна – преобразователь до 7 ГГц
RAKSA 120	50 - 3200 МГц	
Блик-М	50 - 3000 МГц	
Блик-Д	100 - 3000 МГц	
СТБ-111 «Фианит»	60 - 2800 МГц	
SEL SP-75 Black Hunter	100 - 3000 МГц	
SEL SP-77/2M «Ловец»	50 - 3000 МГц	
РИЧ-8	200 кГц - 8 ГГц	
Универсальные поисковые устройства		
ST-033 «Пиранья»	30 - 2500 МГц	ST 03.SHF до 10 ГГц
ST-131 «Пиранья 2»	30 – 4100 МГц	ST 131.SHF до 18 ГГц
СРМ-700	200 Гц – 3 ГГц	ВМР-1200 до 12 ГГц
Поисковые приёмники		
Скорпион	30 – 2000 МГц	
Скорпион-XL	30 – 2500 МГц	
Контур	30 – 2500 МГц	
Комплексы радиоконтроля		
Кассандра М	24 - 3000 МГц	СВЧ - конвертер до 18 ГГц
ОМЕГА	25 - 3000 МГц	ОМЕГА-К18 до 18 ГГц
OSC-5000	10кГц - 3 ГГц	MDC-2100 до 21 ГГц
КРОНА	30 - 3000 МГц	СВЧ - конвертер до 18 ГГц
RS digital Mobile	50 – 2000 МГц	СВЧ – конвертер RS/DC до 12 ГГц

Комплекс «Кассандра К21»

спечения гарантированности и скрытности (а значит, долговременности работы) каналов съёма. Особенно всё вышесказанное касается государственных секретов и работы соответствующих служб. В ход идут всевозможные методы маскировки: использование перескоков частоты передачи, расширение спектра сигнала до шумоподобности, сверхкороткие выходы в эфир в наиболее безопасное время и, в частности, выход в частотные диапазоны, не подвергающиеся контролю со стороны служб защиты. Есть сведения, что уже в середине 80-х годов был отмечен случай применения иностранными спецслужбами закладки с поражающей в то время воображение частотой излучения - 40 ГГц.

Зная это, многие производители средств радиоконтроля (табл. 1) дополняют свой продукт средствами расширения диапазона. Как правило, это конверторы – автономные гетеродины, переносящие спектр СВЧ в основной диапазон контрольных средств. В силу ряда причин, схемы с вынесенным первым преобразованием имеют ряд недостатков, проигрывая в качестве отображения полноценным тюнерам соответствующего диапазона. Однако такие автономные СВЧ – блоки делают более полной линейку средств контроля, позволяя охватить категорию потребителей, чьи интересы выходят за пределы среднестатистических угроз. В то же время такое решение не нагружает финансово тех, кому такие «изыски» не нужны.

Жизнь же не стоит на месте. Возникает вопрос - на том ли месте остался диапазон среднестатистических угроз? Технические разработки становятся всё более совершенными, *алгоритмы передачи информации* (преимущественно – цифровые) позволяют создавать устойчивые, не подверженные помехам каналы связи на гораздо более высоких частотах, чем ранее. Уже и условия распространения радиоволн не выглядят столь большим препятствием. Радиорелейные станции, например, используют диапазон, близкий к сотне гигагерц, а в диапазоне 5 ГГц организован широкополосный доступ с гигагерцевым трафиком.

Что же там есть, за этими 3000 МГц? Прежде всего, излучения гражданских и военных радиорелейных станций (диапазоны 3,6; 4, 7 ГГц и выше), излучения самолетных РЛС, РЭС управления воздушным движением, метеорологии, морские радары, средства спутниковой связи, ну и, конечно же, системы широкополосного доступа Wi-Fi и WiMAX. Последние наиболее интересны, поскольку позволяют организовать каналы утечки информации, используя как легальные сети, так и передатчики на базе стандартных модулей широкополосных систем. Несанкционированное использование легальных сетей остаётся за рамками данной статьи, а вот выход в эфир незарегистрированных устройств – прямая угроза информационной безопасности и должна быть отслежена средствами радиоконтроля.

Значит, всё-таки имеются угрозы, по частотному диапазону выходящие за традиционно анализируемые УВЧ и ОВЧ, это: во-первых, нелегальные устройства сетей широкополосного доступа, во-вторых, устройства, созданные на основе готовых радиомодулей, применяемых в этих системах и, в-третьих, специально разработанные устройства на базе новейших СВЧ радиоэлементов.

Попытаемся определить, как эти угрозы нейтрализовать.

Для выявления устройств первой группы сейчас используются обычные карты широкополосного доступа со специальным программным обеспечением, позволяющим проанализировать топологию сети и отфильтровать «чужие» устройства. Примером такой программы может служить ПО «RInspector WIFI».

Для выявления второй группы можно использовать тот факт, что для них международными соглашениями определены фиксированные диапазоны частот. В СВЧ диапазоне это 3,4-3,7 ГГц и 5,15-5,85 ГГц.

Чем-то ограничить рабочие частоты третьей группы средств съёма информации достаточно сложно. Можно только оговорить, что вероятность появления таких каналов уменьшается с ростом частоты, поскольку, чем выше частота, тем сложнее реализация.

Исходя из этих рассуждений, определяем, что стандартную верхнюю границу диапазона контроля радиоэфира нужно поднять как минимум до 6 ГГц.

Этот вывод подвиг специалистов ЗАО «Группа Защиты – ЮТТА» пересмотреть концепцию построения комплексов радиомониторинга и анализа сигналов серии «Кассандра». Стало очевидно, что выпускающийся в настоящее время комплекс «Кассандра М», даже оснащённый СВЧ конвертерами, перестал удовлетворять современным требованиям. Расширение частотного диапазона комплекса было реально осуществимо, поскольку уже имелся опыт построения аппаратуры на базе тюнеров с СВЧ диапазоном на специализированных двухканальных «Кассандра СО», имеющих диапазон до 21 ГГц.

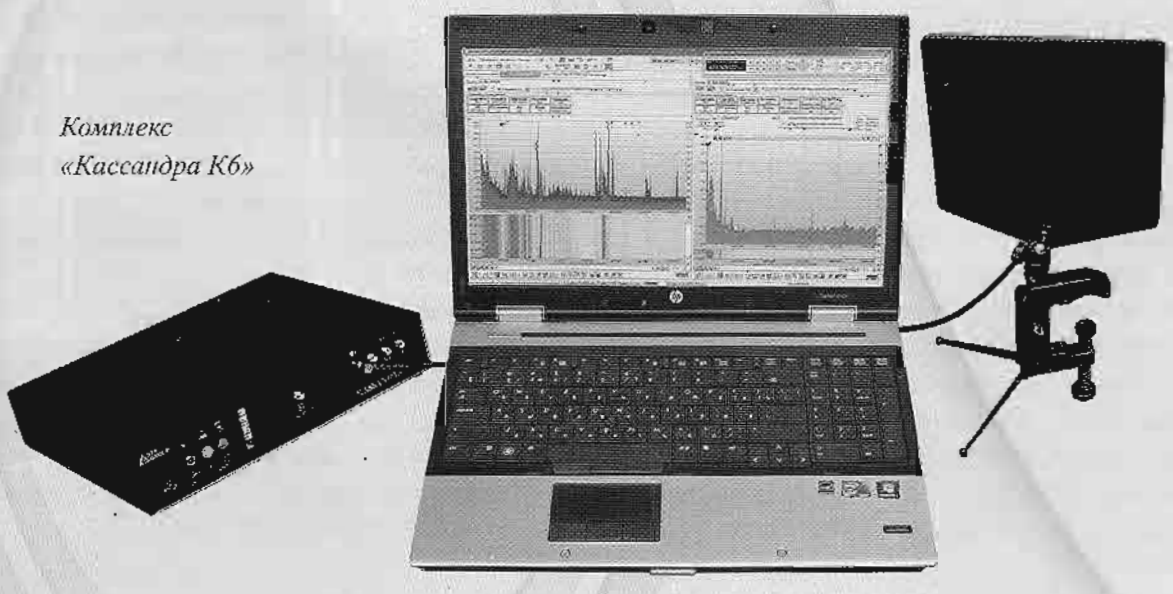
Так была разработана новая линейка комплексов – «Кассандра Кх». Концепция построения этой линейки предполагает унификацию элементов и создание радиоконтрольных комплексов под требуемый диапазон подбором соответствующего тюнера. С июля 2012 года в серийное производство запущены два из них – «Кассандра К6» и «Кассандра К21».

«Кассандра К6» на данный момент представляет собой модернизацию «Кассандра М». В ходе модернизации помимо замены тюнера были доработаны широкополосные антенны и подобраны соответствующие фидеры. Новый тюнер, несмотря на то, что его рабочие частоты увеличены до 6 ГГц, по своим основным характеристикам – чувствительности и динамическому диапазону – не хуже, чем трёхгигагерцевый. Все основные характеристики, кроме диапазона, новый «Кассандра К6» взял у своего предшественника.

«Кассандра К21» представляет собой «усечённый» до одного канала вариант комплекса «Кассандра СО». Поэтому радиочастотные характеристики идентичны. Скорость сканирования оказалась выше, чем у полноразмерной версии, поскольку самое «узкое» место, ограничивающее скорость комплекса – канал передачи данных от основного блока в ПЭВМ обработки в одноканальной версии, – разгрузился. В настоящее время «Кассандра К21» выполнен в ударопрочном кейсе размером 500×350×120 мм, вес комплекса около 6 кг.

Модернизация, естественно, повысила отпускную цену изделий. Однако цена модернизированных комплексов ниже цены аппаратуры старого поколения, оснащённой соответствующим конвертером.

Судьба же «Кассандра М» такова: серийный выпуск прекращается уже с сентября этого года, однако это не исключает возможность заказа его в индивидуальном порядке. Техническая поддержка выпущенных комплексов, также как и устаревших комплексов «Кассандра» будет осуществляться в прежнем режиме.



Комплекс «Кассандра К6»