Васильев Олег Александрович,
кандидат технических наук
ООО НПФ «РАДИОСЕРВИС»
E-mail: rs@radioservice.ru

НАБЛЮДЕНИЕ И БЛОКИРОВАНИЕ
РАЗМЫШЛЕНИЯ ПОСЛЕ ВЫСТАВКИ MILIPOL 13

В чём отличие выставки Milipol-13 от проводимых аналогичных мероприятий у нас в России? Где мы находимся в ряду производителей специальной техники в мировой иерархии? Стоит задуматься. На чём надо делать акцент? Одно могу сказать точно, мы далеко не последние.

Находясь под впечатлением прошедшей в конце прошлого года выставки Milipol-13, должен констатировать, что задачи радиоконтроля и подавления линий связи и управления не только постоянно расширяются, но зачастую смыкаются, являясь одной из важнейших составляющих общей задачи обеспечения безопасности, включающей в себя контроль окружающего пространства, среды обитания, морских границ, мест массового скопления людей, зданий, дорог и т.д. Наблюдение за происходящим, подразумевающее и предсказание событий, требует не только контроля, но и управления радиоэлектронным спектром, или радиообстановкой. Соответственно, границы контроля не могут быть однозначно определены некой зоной, что подразумевает стремление к дополнительным знаниям, то есть к ведению разведки, и радиоразведки в частности.

Как подтверждение сказанному: на парижской выставке Milipol-13 всего один бронированный «Мерседес», море беспилотников, ещё больше систем перехвата и подавления, а также большие рекламные стенды организаций, осуществляющих глобальный контроль всего и вся. А все те, кто занимается безопасностью, в том числе и информационной, являются кирпичиками в оборонительной системе, противостоящей этому глобальному наблюдению – counter surveillance. Все средства безопасности так или иначе связаны с электроникой, системами передачи информации и беспроводным управлением. Интернет породил систему дистанционного управления, охватывающую весь Земной шар. Даже не хочется перечислять, для каких целей она может быть использована. И всё это должно находиться под постоянным контролем спецслужб, обеспечивающих безопасность государства и его населения. Задача обеспечения безопасности на любом уровне является приоритетной как для государственных, так и для частных структур. Её решение всегда должно быть экономически оправданным, затраты разумными, но... жизнь дороже!

Радиоконтроль как задача выявления несанкционированных передающих средств давно изжил себя, превратившись в средство

оперативного поиска и обнаружения подслушивающей, подсматривающей техники, линий связи и управления, которые могут быть использованы в преступных целях. Именно поэтому скорость работы системы радиоконтроля, радиоперехвата, радиоразведки должна быть максимально высокой, только в этом случае такая система может быть составной частью системы обеспечения безопасности, например, системы РЭБ, или системы подавления каналов управления, используемых в террористических целях. Так, например, на выставке были представлены системы, работающие со скоростью обзора до 150 ГГц в секунду и выше, но портативной аппаратуры подобного уровня практически не было. Зато с лихвой были показаны системы подавления.

Не отошла в прошлое и угроза подслушивания с помощью электронных закладных устройств, даже растущая с развитием технологий, в частности, информационных. Интернет даёт круглосуточный доступ к тысячам сайтов с описанием и инструкциями по производству и пользованию такими устройствами, а про использование сотовых телефонов и гаджетов с WiFi для целей прослушки и говорить нечего.

Актуальность противодействия злонамеренным попыткам получения доступа к информационным ресурсам через радиоканал только возрастает со временем, следуя за развитием технологий. Аппаратура поиска и нейтрализации таких попыток минимизируется, а её функциональность стремительно возрастает. Практически изжили себя и программно-аппаратные комплексы, выполненные в виде кейсов с ноутбуком. Представленная на выставке неплохая по параметрам аппаратура RAPTOR RXi британской компании WINKELMANN выглядела довольно громоздкой и неуклюжей в отличие от быстрых портативных анализаторов OSCOR Green (REI, США) и Spectrum Jet (РАДИОСЕРВИС, Россия).

«Nothing goes unnoticed» – ничто не пройдёт незамеченным. Такой слоган был начертан на стенде компании ROHDE&SCHWARZ. А последствия? Заметили - надо нейтрализовать, подавить. Подавление было представлено такими монстрами, как L-3, TRL Technology, CASSIDIAN, SAFRAN и т.д. Хотя и наша владимирская «КОБРА» выглядела неплохо, «Пеликаны» тоже были большие. Однако куда же двигаться дальше? Подавить все сигналы глобально, наверное, легче, чем найти опасный сигнал и блокировать только его. Хотя всё зависит от ситуации.

Вернёмся на землю и посмотрим на ситуацию на отечественном рынке безопасности, пока он ещё существует хоть в каком-то виде. Задача обеспечения безопасности в любом её понимании прежде всего связана с пресечением возможности передачи какой-либо информации, в особенности конфиденциальной или секретной, по радиоканалу. Если ранее имелись в виду главным образом несанкционированные передатчики и побочные излучения, то теперь необходимо предотвратить несанкционированную передачу информации и по легальным радиосредствам, таким как сотовая связь и широкополосный доступ. Необходимо заметить, что занятость диапазона средствами радиодоступа растёт год от года. Широкополосный доступ стандарта LTE уже занимает не только диапазон 2,5 – 2,7 ГГц, но и диапазон 790 -880 МГц. Кроме того, добавился ещё один крупный оператор Tele-2. В связи со стремительным ростом информационных технологий, активно использующих широкополосные радиоинтерфейсы, всё более актуальной становится задача предотвращения доступа абонента, находящегося внутри контролируемой зоны, во внешнюю сеть. Такой зоной могут быть государственное учреждение, деловой офис, секретная лаборатория, следственный изолятор и т.д. Понятно, что экранировать некое пространство большого объёма невозможно, а забить мощным шумовым сигналом отдельные участки диапазона, а теперь практически весь диапазон вплоть до 3 ГГц небезвредно для человека, да и малоэффективно.

Именно поэтому компания «Радиосервис» при разработке систем радиомониторинга и подавления нежелательных сигналов основывается главным образом на принципах **интеллектуального** блокирования. При этом интеллектуальность системы понимается в следующих смыслах:

- обеспечивается полный контроль за выходом в эфир любых радиосредств, включая сотовые телефоны, WiFi трансиверы, коммуника-

торы и т.д., причём некоторые диапазоны могут контролироваться панорамными приёмниками;

- сигнал блокирования является направленным, то есть блокирует только обнаруженный передатчик на его рабочей частоте, а в случае дуплексной работы подавляет сигнал базы или точки доступа, адресованный именно тому абоненту, который предпринимает попытки установить связь.

Многолетний опыт создания систем радиоконтроля, в том числе многоканальных, и разработки интеллектуальных блокираторов для различных стандартов связи и широкополосного доступа позволил инженерам компании объединить радиомониторинг и подавление несанкционированных передач в единую задачу, решаемую представленной ниже распределённой радиосистемой с единым управлением и связанными алгоритмами работы. «**Ковчег-RS/300**» - это новая универсальная система мониторинга и интеллектуального блокирования сотовой связи и беспроводного доступа любых действующих стандартов внутри заданной зоны, предназначенная для защиты утечки информации по каналам сотовой телефонии, Интернету и беспроводным сетям, а также предотвращающая использование сотовой связи в качестве канала управления, например, взрывными устройствами. Базовыми элементами комплекса являются сверхбыстрый приёмник **RS Jet SE**, обеспечивающий обнаружение сигналов несанкционированных абонентов, и универсальный формирователь блокирующих сигналов с усилителем мощности **RS/300.** Приёмник **RS Jet SE** разработан компанией «РАДИОСЕРВИС» специально для применения в системах интеллектуального блокирования и имеет встроенный специализированный вычислитель.

Архитектура системы «**Ковчег-RS/300**» позволяет строить её из отдельных независимых блоков, что чрезвычайно важно при современных темпах развития связи, телефонии, беспроводного доступа и т.д. Кроме того, решение задачи блокирования изначально подразумевает использование системы, распределённой в пространстве, так как в блокируемой зоне действует множество базовых станций, точек доступа и прочих радиотерминалов. Расширение зоны действия системы достигается просто установкой дополнительных блоков, что позволяет спроектировать систему под конкретные условия эксплуатации. Изложенная концепция позволяет настроить аппаратуру под любые действующие стандарты, например: EGSM 900/1800, CDMA2000 (диапазон 450 МГц), WCDMA (диапазон 1,9 - 2,1 ГГц), WiFi/Bluetooth, LTE.

Система блокирования полностью совместима с системами радиомониторинга, построенными на базе приёмников RS Jet. Эта система практически не создаёт помех для приёмника системы мониторинга, так как мониторинг сотовых диапазонов и диапазонов доступа осуществляют приёмники RS Jet SE. Можно сказать, что используется частотное разнесение двух параллельно работающих систем радиомониторинга.

Вернёмся опять к вопросу обнаружения сигнала управления, или момента выхода в эфир с запросом сотового телефона, или абонента беспроводного доступа. Задача обнаружения должна решаться максимально быстро, что особенно важно для интеллектуальных подавителей RCIED (сигналов управления взрывными устройствами). Скорость сканирования в системе радиоконтроля ограничивает компьютер. Система блокирования должна работать в реальном времени, а решение о блокировании в таких системах должно приниматься специальным вычислителем, без участия компьютера.

Общее время анализа заданного диапазона, равного полосе ПЧ, или удвоенной полосе ФНЧ квадратурного преобразователя в ноль, складывается из времени набора выборки, времени вычисления FFT, времени передачи команд управления синтезаторами и времени перестройки приёмника. Как бы быстро ни перестраивался и ни управлялся приёмник, сколь бы мощным ни был вычислитель, невозможно физически провести анализ быстрее времени получения данных, а их объём зависит от требуемого разрешения. Из теории следует, что время набора выборки равно t = 1/Fразр, так для получения разрешения в 10 КГц требуется 100 мкс, а для разрешения в 100 КГц - 10 мкс. Общее время анализа полосы в 32МГц при разрешении 10 Кгц в приёмнике RS Jet SE составляет величину в 200 мкс, что соответствует скорости мониторинга 160 ГГц/с.

После обнаружения сигнала принимается решение о начале блокирования, если все заданные условия соблюдены. Сигнал блокирования излучается минимально возможной для осуществления блокирования мощности и длительности. Система построена таким образом, что в ней каждый приёмник, имеющий собственный вычислитель, управляет приданным ему подавителем или системой подавителей, которые могут быть встроены в один корпус, а могут и быть выносными. Все вычислители приёмников и контроллеры формирователей блокирующего сигнала связаны между собой через собственную управляющую сеть. Их совместная работа организована так, что блокираторы одного стандарта не влияют на работу остальных. Система позволяет оборудовать несколько больших помещений, залов, этажей аппаратурой интеллектуального блокирования с единым центром управления, располагаемым на расстояниях до нескольких сотен метров.

Рассмотрим более подробно основной элемент системы: универсальный формирователь сигнала блокирования (УФСБ). Блок-схема формирователя приведена на рис.1

Формирователь содержит:

- синтезатор ВЧ сигнала, работающий в широком диапазоне частот от 30 МГц до 3 ГГц;
- цифровой синтезатор (DDS) с квадратурными выходами (тактовая частота 500 МГц);
- квадратурный модулятор;
- управляющий контроллер;
- широкополосный усилитель мощности;
- систему переключаемых формирующих фильтров;
- антенну.

Высокочастотный широкополосный синтезатор вырабатывает сигнал, поступающий на квадратурный модулятор. Прямой цифровой синтезатор формирует квадратурные составляющие модулирующего сигнала, позволяющие получить на выходе модулятора сигналы с различными видами амплитудной, частотной и фазовой модуляции. Полоса сигнала может варьироваться в пределах от 0 до 200 МГц. Для уменьшения уровня побочных составляющих применена система переключаемых диапазонных фильтров НЧ. Сигнал с модулятора поступает на широкополосный усилитель мощности и на антенну. Работой формирователя управляет контроллер. Формирователь содержит соответствующие интерфейсные модули CAN, LAN и по необходимости WiFi.

Формирователь сигнала блокирования способен синтезировать узкополосные и широкополосные сигналы с различными видами модуляции и полосой до 200 МГц.

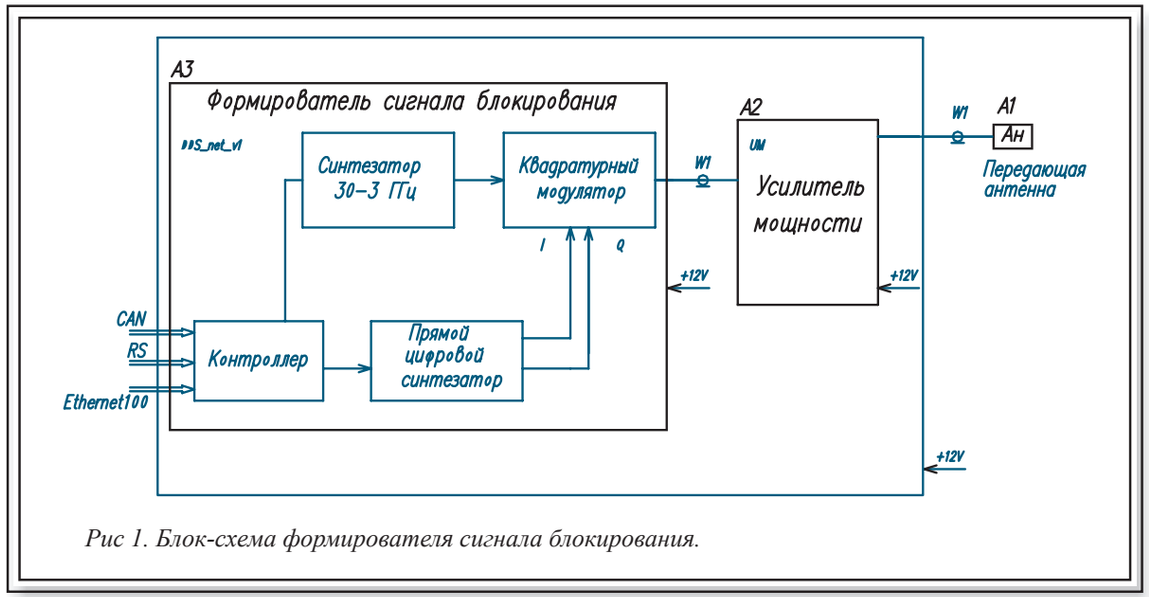

Рис 1. Блок-схема формирователя сигнала блокирования.

Ниже перечислены виды сигналов блокирования, доступные для реализации формирователем:

1. Сигнал с линейной частотной модуляцией (ЛЧМ сигнал).

2. Сигнал с двухпозиционной (бинарной) амплитудной, частотной или фазовой модуляцией (манипуляцией).

3. Сигнал с четырёхпозиционной амплитудной, частотной и фазовой модуляцией (QPSK).

4. Узкополосный сигнал.

Параметры каждого из вышеприведённых сигналов можно задать программно с управляющего компьютера. Для каждого стандарта сотовой связи и беспроводного доступа используется определённый вид оптимального сигнала блокирования, параметры которого уже занесены в память контроллера формирователя.

На базе подобного формирователя компанией «Радиосервис» разработан универсальный восьмиканальный блокиратор сотовой связи и беспроводного доступа **RS/300.** Блокиратор способен подавить каналы сотовой телефонии и беспроводного доступа всех действующих на данный момент стандартов. Он может работать как в заградительном, так и в интеллектуальном режимах. В производстве стационарные и портативные варианты блокиратора. Портативный блокиратор в автономном режиме при его включении может осуществлять подавление до 8-ми различных заранее запрограммированных диапазонов. Стандартной литий-ионной батареи хватает на 1-1,5 часа. Управлять автономным блокиратором можно через WiFi, LAN, CAN.

В системе **«Ковчег-RS/300»** управление блокиратором осуществляется непосредственно контроллером вычислителя приёмника **RS Jet SE** через UART, либо по сети CAN.

Блок схема автономного блокиратора с управлением по WiFi (5,1 – 5,3 ГГц) или LAN представлена на рис. 2.

Блокиратор содержит:

- универсальный 4-х канальный формирователь сигнала блокирования 2 шт.
- встроенную широкополосную антенну 2 шт.
- приёмопередатчик WiFi (5,1 – 5,3 ГГц) 1 шт.
- разветвитель (HUB) 1 шт.
- плату питания 1 шт.
- Li Ion–ый аккумулятор 1 шт.

Для реализации блокирования был выбран сигнал с линейной частотной модуляцией (ЛЧМ сигнал) как наиболее универсальный для подавления всех видов аналоговых и цифровых сигналов, используемых в системах передачи информации, в

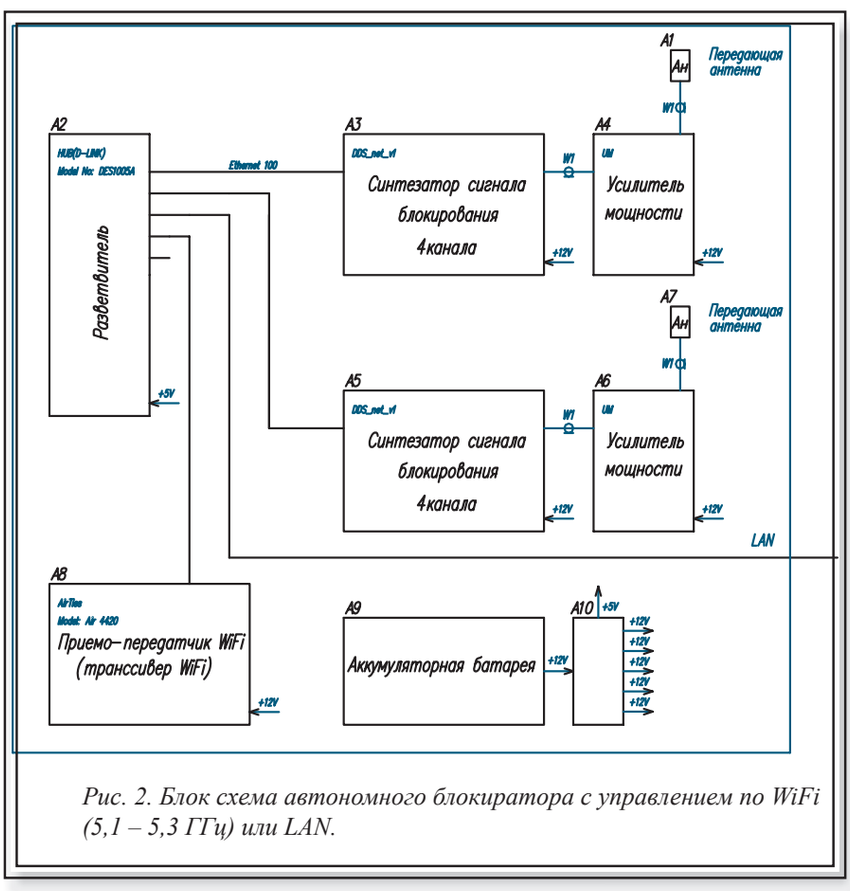

Рис. 2. Блок схема автономного блокиратора с управлением по WiFi (5,1 – 5,3 ГГц) или LAN.

телевидении, связи и т.д. Соответствующее программное обеспечение позволяет вводить требуемые параметры для получения ЛЧМ-сигнала с заданными характеристиками.

Необходимо определить несущую частоту, требуемую девиацию частоты, профиль T, или время нарастания пилы, задать временной интервал, или длительность ступеньки, а также величину шага по частоте. Эти параметры имеют соответствующие ограничения вследствие физической реализации, а их расчёт позволяет подобрать блокирующие сигналы для всех стандартов сотовой связи и беспроводного доступа.

Расчёт линейного тракта радиоприёмного устройства, аналогичного используемому в приёмнике RS Jet SE, интересующийся читатель может найти в (1), а описание характеристик оптимального сигнала подавления для систем 3G и 4G в работе (2).

В заключение заметим, что система интеллектуального блокирования «**Ковчег-RS/300**» может быть использована в залах для проведения закрытых совещаний, на секретных предприятиях и военных базах, в учреждениях пенитенциарной системы (зоны, тюрьмы, изоляторы и т.д.), а также для соблюдения тишины в концертных залах, театрах, аудиториях, церквях и т.д.

Литература

1. *Васильев О.А., Грязнов К.В., Ефремов И.А. Расчёт, проектирование и реализация широкополосного приёмника // Специальная техника. - 2012. - №2. – С. 46-52.*

2. *Васильев О.А., Грязнов К.В., Моисеев С.А. Интеллектуальное блокирование сотовой связи и беспроводных сетей 3G и 4G // Специальная техника. – 2012. - №6. – С. 23-26.*