Ковровая бомбардировка или точечное попадание?

О. А. Васильев
Компания «Радиосервис»
rs@radioservice.ru

В последнее время в связи с утечками информации по каналам беспроводного доступа (3G, LTE – 4G, Wi-Fi), явившимися следствием внедрения облачных технологий, в ряде государственных и коммерческих структур ограничено или полностью запрещено пользование смартфонами, планшетами, разного рода портативными устройствами с встроенным радиодоступом. Однако эти запреты подчас игнорируются. Проникновение Wi-Fi в системы управления и в бытовую технику нарастает, о чем свидетельствуют проводимые в Лондоне ежегодные конференции и международные выставки или, например, прошедший в 2014 году форум в Барселоне, посвященные этой тематике. Даже, если в здании нет точек беспроводного доступа, утечку можно организовать, задействовав несколько смартфонов в качестве собственноручно созданной сети с последующей передачей данных через внешнюю удаленную точку доступа.

Специалистам по безопасности следует обратить внимание на материалы с сайта РБК, где приводится опубликованный журналом «Шпигель» каталог различных вариантов закладок, в том числе программных, разработанных специалистами АНБ США, с использованием стандартных каналов радиодоступа.

Вкратце коснемся перспектив развития коммуникаций и, соответственно, направлений защиты соответсвующих каналов утечки информации [1]. Госкомиссия по радиочастотам распродает сотовым операторам все новые диапазоны частотного ресурса. На сайте нашей компании приведена таблица распределения радиочастотного спектра всех действующих в Москве операторов на конец 2014 года. После ее изучения становится очевидным: чтобы противодействовать информационным утечкам, подавляя сигналы базовых станций и точек доступа, действующих в прилежащем пространстве, потребуется постоянно излучать сигналы подавления практически во всем диапазоне от 400 до 2700 МГц, интегральная мощность которых недопустимо велика в местах, где живут и работают люди.

Возникает вопрос: где же выход? Единственный возможный вариант – использование интеллектуального блокирования, направленного на конкретного абонента, конкретный стандарт, конкретный канал только в момент запроса или установления связи.

Именно такой принцип заложен в идеологии аппаратуры интеллектуального блокирования сотовой связи и беспроводного доступа, впервые разработанной более десяти лет назад компанией «Радиосервис» и постоянно модернизируемой по мере развития систем коммуникации и введения новых стандартов.

В последних разработках компании использованы новейшие технические решения, построенные на базе достижений современной микроэлектроники, что позволило существенно улучшить массо-габаритные параметры аппаратуры, сделать ее более мобильной и легко контролируемой. В первую очередь отметим мультистандартный интеллектуальный блокиратор ***RS300i***, рассчитанный на блокирование одного-двух помещений общей площадью до 100 м^2. Последовательно включаемые блокираторы способны обеспечить зону блокирования любой конфигурации, вплоть до всего здания, находящуюся под контролем управляющего компьютера. В системе может быть задействован анализатор ***Spectrum Jet*** с выносными антеннами точками и ретрансляцией сигналов. Описания предлагаемой аппаратуры приводятся ниже и имеются в более подробном виде на нашем сайте.

В связи с вышеизложенным все более актуальной становится задача предотвращения доступа абонента, находящегося внутри контролируемой зоны, во внешнюю сеть. Как уже говорилось выше, экранировать пространство большого объема невозможно, а забить мощным шумовым сигналом отдельные участки диапазона, а теперь практически весь диапазон вплоть до 3 ГГц, небезвредно для человека, да и малоэффективно. Отсюда и сравнение, вынесенное в заголовок статьи. Сигнал блокирования должен быть прицельным, кратковременным, безопасным для здоровья человека и не создающим помех иной радиоаппаратуре. Только при интеллектуальном блокировании возможно сохранить

внутри контролируемой зоны вполне определенный набор услуг сотовой связи для определенной категории абонентов.

Напомним вкратце основные стандарты и характеристики сигналов, используемых в соответствующих системах сотовой связи и беспроводного доступа. Известно [3], что основной задачей сотовой связи является обслуживание максимального числа клиентов с предоставлением им множественного доступа в сеть на ограниченном участке диапазона частот. Если системы 1-го и 2-го поколений (например, самый распространенный из них – стандарт GSM) использовали множественный доступ, главным образом, с частотным и временным разделением каналов, то системы 3-го и 4-го поколений (3G и 4G) преимущественно берут на вооружение кодовое разделение каналов – CDMA и технологию OFDM.

Сигналы в стандарте GSM являются узкополосными (ΔF = 200 кГц) и имеют назначенный частотный канал и заданный временной слот длительностью 577 мкс.

Сигналы систем с кодовым разделением являются широкополосными: так, полоса пропускания канала в стандарте CDMA2000 – 1,25 МГц, а в стандарте W-CDMA – 5 МГц. Системы 3G и 4G широко используют пакетную передачу данных. К таковым, например, относится вариант стандарта W-CDMA, получивший название высокоскоростного доступа к пакетным данным – HSDPA (High Speed Data Packet Access).

Для достижения нашей цели – исключения доступа из контролируемой зоны по радиоканалу – нас интересует физический уровень, на котором общаются базовая станция и абонент мобильной сети, поэтому в дальнейшем разговор будет идти лишь о радиоинтерфейсе стандарта WCDMA (широкополосный доступ с кодовым разделением каналов).

Надо отметить, что в зависимости от занятости канала или для защиты от действующих помех, в том числе преднамеренных, система может менять длительность пакетов и скорость передачи данных абоненту. Следовательно, блокирование таких сигналов должно осуществляться непрерывно. Наличие временных интервалов без блокирования приводит к «просачиванию» передаваемой информации короткими пакетами.

Следует иметь в виду, что в России реальная эксплуатация сетей 3G началась не так давно, в то время как опережающими темпами развиваются конкурирующие мобильные технологии, основанные на фиксированном и мобильном беспроводном доступе. Это, прежде всего, VoIP через точки доступа Wi-Fi и технология LTE, вытеснившая с рынка WiMAX. Организация по стандартизации IEEE утвердила стандарт LTE для мобильных устройств еще несколько лет назад. LTE является перспективной технологией беспроводной связи следующего поколения, так как обладает высокой пропускной способностью и большой областью покрытия. Пиковая скорость, обеспечиваемая этой технологией, достигает 50 Мбит/с (uplink) и 100 Мбит/с (downlink). Считается, что технология сможет в будущем вытеснить городские сети Wi-Fi. Пропускная способность сотовой сети по-прежнему сильно ограничена. Сегодняшние сети 3G, в том числе технологии CDMA2000 (в России – «Скай Линк») и W-CDMA, позволяют достичь реальной скорости передачи данных лишь порядка 3,4–4,8 Мбит/с.

Очевидна тенденция сращивания двух направлений беспроводной передачи данных, включающих с одной стороны сотовую связь и беспроводные сети с другой.

В целом, задача обнаружения широкополосных сигналов (ШПС) является достаточно сложной. Так, если базовая станция находится недалеко от зоны блокирования (10–50 м), то сигнал абонентского передатчика может лежать ниже уровня шумов приемника-обнаружителя. В этом случае говорить об интеллектуальности не приходится, если не используются специализированные приемные устройства, например, с виртуальной базой. В стандартной ситуации, однако, обнаружение абонентского сигнала вполне возможно. Это замечание относится, главным образом, к стандарту W-CDMA (UMTS).

При анализе задачи блокирования, являющейся разделом радиоэлектронной борьбы (РЭБ), имеет смысл опираться на хорошо известные результаты, полученные в работах по проблеме помехоустойчивости цифровых линий передачи информации, в том числе помехоустойчивости различных видов модуляции и кодирования [4, 5]. Существует противоречие между пропускной способностью системы и ее помехоустойчивостью [3]. С одной стороны, улучшение пропускной способности требует увеличения энергии сигнала либо расширения полосы частот. С другой стороны, для повышения помехоустойчивости необходимо делать то же самое, но, не увеличивая при этом пропускную способность, то есть вводить в систему избыточность [3, 5].

Все современные методы многопозиционной модуляции с высокой информационной емкостью на одну позицию, такие как QPSK, QAM-16, -32, -64, -128, имеют слабую помехозащищенность. Однако в системах с кодовым разделением каналов используются широкополосные сигналы, обладающие высокой помехоустойчивостью.

Приведенные в [2] расчеты показывают, что для подавления сигналов, используемых в системах 3G и 4G, при любом виде непрерывного сигнала блокирования его мощность должна превышать мощность информационного сигнала не менее чем на 20 дБ в точке приема абонентом сигнала базы. При этом эффективность блокирования не зависит от формы сигнала или его спектральных характеристик, но полоса блокирующего сигнала должна лежать внутри полосы блокируемого, только тогда блокирование будет эффективным и связь не установится.

Из всего многообразия средств подавления сигналов сотовой связи, присутствующих на российском рынке, можно выделить следующие основных группы. К первой группе относятся блокираторы сотовой связи, обеспечивающие постановку заградительной шумовой помехи в диапазоне частот работы базовых станций соответствующего стандарта, то есть на частотах приема мобильных

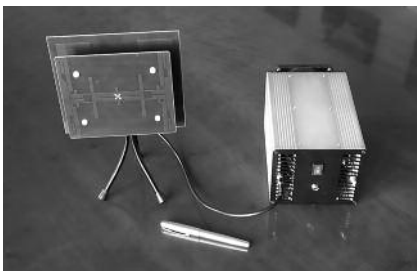

Рис. 1. ***Внешний вид блокиратора RS300i***

телефонов сотовой связи, и представляющие собой генераторы радиопомех с ручным управлением. В целом, это достаточно примитивные устройства со сходными характеристиками.

В таких подавителях могут использоваться генераторы помех с пилообразной перестройкой несущей частоты, генераторы импульсов с амплитудой, изменяющейся по псевдослучайному закону, или же подавление осуществляется с помощью самих же принятых сигналов базовых станций в несколько искореженном виде. Количество усилителей мощности и антенн, как правило, соответствует количеству подавляемых стандартов связи. Несмотря на относительную простоту реализации, для достижения эффективного подавления требуется весьма приличная интегральная мощность и, как следствие, громоздкая конструкция.

Более сложными и более безопасными устройствами являются подавители сотовой связи с блоком управления. В такой системе при обнаружении сигнала абонента передатчик помех включается на короткое время, как правило, на несколько секунд. При постановке широкополосной заградительной помехи происходит срыв сеанса связи.

К особой группе подавителей относятся интеллектуальные блокираторы сотовой связи, отличающиеся от второй группы наличием в составе их приемного устройства специализированного анализатора сигналов и обладающие следующими особенностями:

- постоянным контролем диапазонов сотовой связи;
- направленным блокированием сигнала базы, который адресован абоненту, предпринимающему попытки установить связь;
- формированием блокирующего сигнала импульсной структуры и минимально возможной мощности;
- более слабым воздействием на человека, чем в непрерывных подавителях.

Понятно, что сложность реализации интеллектуальных и обычных блокираторов несопоставима. Одним из наиболее удачных решений в области интеллектуального подавления является система «Ковчег М», приведенная в [6]. Однако развитие сотовой связи и беспроводного доступа заставило разработчиков пересмотреть свои взгляды на алгоритмы работы системы, ее конфигурацию и конструкцию, что привело к созданию совершенно нового класса оборудования интеллектуального блокирования RS300i.

Современный сотовый телефон (смартфон) может работать в сетях практически всех действующих стандартов, причем по всему миру. Это сети GSM, UMTS (3G), LTE (4G). Кроме того, что во всех стандартах выполняются все функции сотовой телефонии и доступа, имеется и доступ через Wi-Fi. Отсюда следует, что блокирование должно производиться одновременно по всем каналам доступа, иначе связь установится через другой радиоинтерфейс.

Структура нового оборудования блокирования такова, что в нем наблюдение идет по всем каналам uplink (абонент – база), а блокирующий сигнал формируется не кучкой генераторов с усилителями мощности и собственными антеннами, а синтезируется в системе формирователей с процессорным цифровым управлением. Общий блокирующий сигнал имеет импульсную структуру, что позволяет использовать временное разделение по стандартам или каналам, а также выбирать наиболее эффективные параметры для каждого стандарта, причем делать это можно дистанционно. Специально для данной системы был разработан широкополосный усилитель мощности для диапазона 0,5–3 ГГц, развивающий выходную мощность до 10 Вт.

Итак, в чем заключаются основные различия между системами RS300i и «Ковчег М»? Структура приемника-обнаружителя претерпела существенную модернизацию, однако ее функциональность сохранилась. При этом сигнал блокирования формируется и выглядит совершенно по-новому. Включаемый на короткое время блокирующий сигнал одновременно перекрывает все возможные пути (диапазоны) установления связи абонентом. Импульсная структура сигнала позволяет существенно снизить излучаемую блокиратором интегральную мощность. Блокирующие сигналы для разных стандартов разнесены не только по частоте, но и по времени, что гарантирует существенное снижение нелинейных продуктов в блокирующем сигнале на входах действующих радиосистем, например систем радиоконтроля, то есть эфир остается практически «чистым».

Общий вид блокиратора RS300i приведен на рис. 1. Как видим, в весьма малом объеме с одной антенной уместился практически весь основной блок аппаратуры «Ковчег»!

Рассмотрим более подробно универсальный формирователь сигнала блокирования. Блок-схема формирователя приведена на рис. 2.

Формирователь содержит:

- синтезатор ВЧ-сигнала, работающий в 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. Сигнал с модулятора поступает на широкополосный усилитель мощ-

ности и на антенну. Для уменьшения уровня побочных составляющих применена система переключаемых диапазонных фильтров. Работой формирователя управляет контроллер. Формирователь содержит соответствующие интерфейсные модули CAN, LAN и, при необходимости, Wi-Fi. Формирователь сигнала блокирования способен синтезировать узкополосные и широкополосные сигналы с различными видами модуляции. Для каждого стандарта сотовой связи и беспроводного доступа используется определенный вид оптимального сигнала блокирования, параметры которого уже занесены в память контроллера формирователя.

Именно на базе подобного формирователя компанией «Радиосервис» разработан универсальный восьмиканальный блокиратор сотовой связи и беспроводного доступа RS/300i. 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 интеллектуальное подавление до восьми различных заранее запрограммированных диапазонов. Для реализации блокирования 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 телевидении, связи и т. д. Соответствующее программное обеспечение позволяет вводить требуемые параметры для получения ЛЧМ-сигнала с заданными характеристиками.

При этом 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 расчет позволяет подобрать блокирующие сигналы для всех стандартов сотовой связи и беспроводного доступа. Спектрограмма, приведенная на рис. 3, иллюстрирует распределение спектральной плотности мощности сигнала передатчика 5-полосного блокиратора на фоне сигналов действующих базовых станций сотовых операторов.

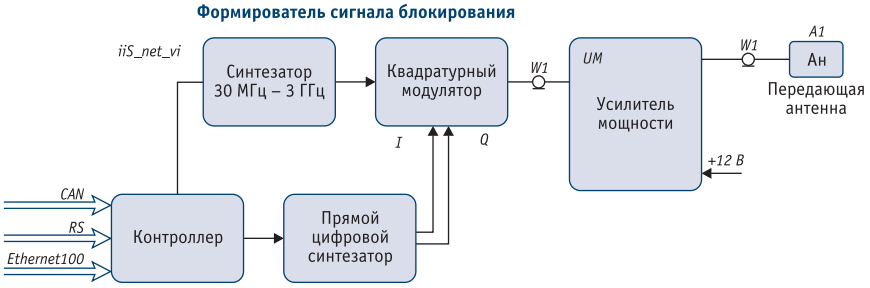

Рис. 2. ***Блок-схема формирователя сигнала блокирования***

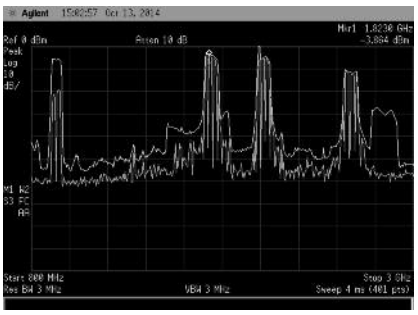

Рис. 3. ***Распределение спектральной плотности мощности сигнала передатчика 5-полосного блокиратора на фоне сигналов действующих базовых станций сотовых операторов***

На базе управляемых блокираторов строятся распределенные системы, предназначенные для подавления сотовой связи в нескольких больших помещениях, залах, этажах, отдельно стоящих зданиях или на закрытых территориях. При этом в каждом защищаемом помещении устанавливаются блокираторы, которые объединяются в локальную сеть. Для прокладки сети можно воспользоваться любым типом шины: витой парой, оптоволокном, радиоканалом и т. д.

Каждый блокиратор решает индивидуальную задачу подавления сотовой связи в данном помещении. Настройка блокиратора осуществляется в соответствии с его индивидуальными особенностями размещения. Информация о выходе в эфир мобильных телефонов в контролируемых помещениях с указанием времени работы и привязкой к конкретному помещению поступает в управляющий компьютер по локальной сети.

С управляющего компьютера можно дистанционно производить включение/выключение режима подавления отдельных блокираторов, регулировать зону подавления и осуществлять диагностику работоспособности системы.

Наибольшая эффективность системы информационной безопасности достигается при объединении радиомониторинга и подавления несанкционированных передач в единую задачу, решаемую распределенной радиосистемой с единым управлением и связанными алгоритмами работы. ■

ЛИТЕРАТУРА

1. *Васильев О. А. Наблюдение и блокирование. Размышление после выставки MILIPOL 13 // Специальная техника. 2013, № 6, с. 31–36.*
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.*
3. *Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В. Широкополосные беспроводные сети передачи информации – М.: Техносфера, 2005. – 592 с.*
4. *Современная радиоэлектронная борьба. Вопросы методологии / под ред. В. Г. Радзиевского. – М.: Радиотехника, 2006. – 421 с.*
5. *Архипкин В. Я., Мешковский К. А. Сравнительная помехозащищенность систем связи с широкополосными и узкополосными сигналами // Информация и космос. 2004, № 3.*
6. *Сайт компании «Радиосервис». Системы интеллектуального блокирования сотовой телефонии и беспроводного доступа [Электронный ресурс]. – Режим доступа: http://www.radioservice.ru.*