



СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОГО БЛОКИРОВАНИЯ СОТОВОЙ ТЕЛЕФОНИИ, КАНАЛОВ СВЯЗИ И УПРАВЛЕНИЯ

О. А. Васильев, Д. О. Егоров, А. Н. Кадыков
Компания «Радиосервис»

В статье кратко рассматривается стратегия построения систем подавления радиоканалов связи и управления, использующих панорамный прием для обнаружения коротких сигналов и блокирование приемника абонента коротким согласованным по спектру импульсом. Представлен вариант реализации подобной системы с использованием прямой конвертации диапазона частот вниз и дальнейшей цифровой обработки квадратурных составляющих на DSP-контроллере «Tornado-E67».

➤ Задача подавления сигналов является чрезвычайно актуальной для антитеррористической аппаратуры нейтрализации радиоканалов дистанционного управления и систем защиты каналов утечки информации. Поскольку во многих случаях априорных данных о сигналах, подлежащих блокированию, ничтожно мало, то обычно подавлению подвергается весь диапазон, в котором возможна работа радиолинии управления или передачи информации. Чем шире охватываемый диапазон частот и больше мощность заградительной помехи, тем меньше вероятность исполнения команды, передаваемой по радиолинии. Неоспоримо, но примитивно. Энергетический, да и человеческий ресурсы не безграничны. РЭБовские принципы подавления в мирное время по меньшей мере не гуманны.

Однако систему подавления можно оптимизировать, сделав ее интеллектуальной: сначала обнаружить сигнал и оценить его параметры, а потом точно заблокировать приемник радиолинии, которому адресована информация, содержащаяся в данном сигнале. Как в системе ПРО, сначала обнаружим цель, вычислим ее траекторию, а затем запустим

свою антиракету для ее поражения. Стрелять всеми ракетами сразу бессмысленно, да и накладно.

Характерным примером такого рода систем являются устройства подавления сотовой связи в заданном районе, здании, помещении. Сигналы в сотовых сетях могут быть командной радиолинией или использоваться для передачи конфиденциальной информации. Аналогичные функции могут выполнять любые современные радиолинии, соответствующие стандартам беспроводных компьютерных сетей (WLAN, Wi-Fi, Zig-Bee), а также различные системы беспроводного доступа и т. д.

Рассмотрим ниже стратегию и основные принципы построения интеллектуальных систем блокирования и покажем на примере, что энергетический выигрыш в таких системах по сравнению с системами, использующими заградительную помеху, достигает десятков децибел при одинаковой эффективности.

ОБНАРУЖЕНИЕ КОРОТКОГО ИМПУЛЬСА В ЗАДАННОМ ДИАПАЗОНЕ

При построении современных систем интеллектуального блокирования, как и систем радиомониторинга и защиты информации, основной задачей является быстрое обнаружение и вычисление параметров коротких сигналов длительностью вплоть до нескольких микросекунд. Эти сигналы могут быть как одиночными (например, представлять собой кодированную команду управления), так и являться мгновенной выборкой из потока радиоимпульсов различной частоты. Такой поток может представлять собой канал передачи информации в какой-либо связанной системе, соответствующей

определенному стандарту связи, где для улучшения помехоустойчивости используется режим передачи со скачками по частоте (Frequency Hopping — FH). Для режима FH характерна смена несущей частоты радиоимпульса по псевдослучайному закону с высокой скоростью. Например, для стандарта Bluetooth она происходит 1600 раз в секунду в полосе 79 МГц. Соответственно, спектр одного импульса занимает полосу частот около 1 МГц.

Режим скачков по частоте используется для расширения спектра (Frequency Hopping Spread Spectrum — FHSS) в беспроводных компьютерных сетях для передачи данных по протоколу IEEE 802.11 и в различных радиосистемах военного применения.

Одним из наиболее характерных примеров является режим скачков FH в стандарте сотовой связи GSM, эффективно используемый для борьбы с замираниями сигнала, главным образом, при движении в автомобиле. Длительность радиоимпульса, или слота, в стандарте GSM равна 577 мкс, а при запросе связи абонентской трубкой — как в случае исходящего, так и в случае входящего звонка составляет всего 300 мкс. Выход мобильного телефона в эфир с импульсом запроса (Random Burst — RB) осуществляется на дуплексной частоте канала управления базовой станции. Весь последующий процесс обмена информацией между абонентским терминалом и базовой станцией может происходить уже в режиме скачков. Число используемых частотных каналов определяется базовой станцией.

Рассмотрим далее задачу обнаружения короткого радиоимпульса, в основном, применительно к системе сотовой телефонии стандарта

GSM. Система, решающая задачу обнаружения короткого импульсного сигнала, может быть построена различными путями. Известно, что вероятность обнаружения сигнала зависит от отношения «сигнал/шум», то есть от энергии сигнала и чувствительности приемника. Важнейшим вопросом является согласование полос сигнала и приемника. В идеале полоса пропускания приемного устройства до детектора должна повторять форму огибающей спектра радиосигнала. Очевидно, что если полоса пропускания приемного устройства или полоса фильтра измерительного устройства, работающего на широкополосном выходе промежуточной частоты приемника, в несколько раз уже полосы радиоимпульса, то такой приемник просто не прореагирует на сигнал, воздействующий на его входе. Для правильного построения обнаружителя необходимы полные априорные данные о сигнале, включая несущую частоту. В рассматриваемой задаче с прыгающей по частоте несущей необходимо знание всех возможных частот, используемых для режима скачков. Для стандарта GSM это частотные каналы: 124 полнодуплексных канала в диапазоне 890-915 МГц (обратные каналы, абонентские терминалы — базовая станция) и 935-960 МГц (прямые каналы, базовая станция — абонентские терминалы), а также 374 канала в диапазонах 1710-1785 и 1805-1880 МГц. Разнос между каналами составляет 200 КГц. Реально, конечно, используется лишь некоторое количество каналов, на которых может работать базовая станция. Это может быть связано и с распределением сетки частот между различными операторами связи. Итак, будем считать, что все априорные данные нам известны, а задача сводится к энергетическому обнаружению сигнала на интервале времени и оценке его параметра — несущей частоты (или номера частотного канала) в системе GSM.

Как следует из фундаментального соотношения для расчета чувствительности приемника, минимальная мощность обнаруживаемого сигнала увеличивается с ростом полосы анализа (или полосы пропускания приемника):

$$P_{min} = -174 + NF + 10lgB + \dots, [1]$$

NF — ;
— ;
— -

Если сигнал представляет собой радиоимпульс в системе с режимом скачков по частоте FH или по n-частотным каналам, то при общей полосе обнаружения $B = nF$ (где F — полоса частот, занимаемая одним каналом) минимальная мощность обнаруживаемого сигнала, как следует из приведенного выражения, увеличивается по сравнению с одноканальным обнаружителем на величину $10lgB/F = 10lgn$ дБ. Для системы сотовой связи стандарта GSM это $10lg124 = 20,9$ дБ для нижнего и $10lg374 = 25,7$ дБ для верхнего диапазонов соответственно.

Итак, в приведенных примерах широкополосный обнаружитель проигрывает в энергетике обнаруживаемого сигнала согласованному по полосе канала обнаружителю не менее 20 дБ. Однако при достаточно мощном сигнале он гарантирует обнаружение сигнала, в то время как одноканальный обнаружитель в режиме сканирования по каналам имеет ничтожно малую вероятность обнаружения. Понятно, что для сохранения минимальной мощности обнаруживаемого сигнала при гарантированной вероятности его обнаружения (равной единице) необходим многоканальный обнаружитель, в котором число согласованных приемников равно числу частотных каналов в системе, то есть $124 + 374 = 498$ приемников для системы GSM.

СПЕКТРАЛЬНОЕ ОЦЕНИВАНИЕ В ЗАДАЧЕ ОБНАРУЖЕНИЯ

Задачу многоканального обнаружения можно решить, применяя цифровые способы обработки сигналов. Классическим методом обнаружения сигнала является спектральное оценивание составляющих прямого преобразования Фурье для действующей на входе приемника смеси «сигнал + шум». Для получения спектральной оценки необходимо перевести сигнал в цифровую форму и вычислить его спектральное представление на цифровом

процессоре (DSP), используя широко известные алгоритмы, например, быстрое преобразование Фурье (FFT). В идеале принятый сигнал должен быть оцифрован насколько возможно ближе к антенне, так как при этом цифровое представление сигнала будет иметь минимально возможные спектральные потери при дальнейшей цифровой обработке.

Классический путь фильтрации сигнала, то есть выделение узкополосного частотного канала из широкополосной смеси сигнала и шума, требует нескольких частотных преобразований через частоты и соответствующие аналоговые фильтры, пока не будет достигнута требуемая точность (или качество) в разделении каналов. Система цифровой обработки сигнала (ЦОС) обычно использует сигнал, снимаемый с широкополосного выхода промежуточной частоты приемника, значения которой обычно выбирают из стандартного набора: 10,7; 21,4 МГц и т. д.

Иногда используют дополнительное преобразование вниз с целью применения более низкочастотных, но имеющих большее число разрядов и, соответственно, больший динамический диапазон аналого-цифровых преобразователей (АЦП). Частота оцифровки сигнала выбирается в 2-3 раза выше верхней граничной частоты полосы пропускания тракта ПЧ приемника.

Бурное развитие цифровых технологий и появление быстродействующих АЦП с тактовыми частотами до гигагерц и выше в последнее время породило тенденцию все большего смещения систем цифровой обработки сигнала в сторону антенны. При стандартной динамике приемника по выходу ПЧ 60-70 дБ для осуществления цифровой обработки без существенных потерь достаточно использования 12-разрядного АЦП, имеющего собственный динамический диапазон 72 дБ. Подобные АЦП с частотой выборки 65 и 105 МГц производит, например, компания Analog Devices.

Кроме того, для расширения частотного диапазона анализируемых сигналов приблизительно до значения частоты выборки АЦП можно использовать современные методы разложения входного сигнала на

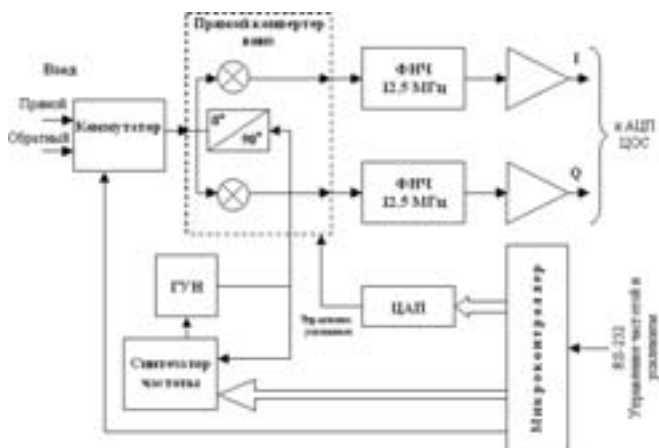


Рис. 1

квадратуры. Практически все цифровые демодуляторы и системы цифровой обработки сигналов в сотовой телефонии, беспроводных компьютерных сетях и т. д. работают по такому принципу. В последнее время на рынке интегральных микросхем для обработки высокочастотных аналоговых сигналов появились и прямые конвертеры вниз (Direct Downconverter — DDC), позволяющие получать на выходе синфазную и квадратурную составляющие преобразованного входного сигнала в частотном диапазоне практически до 100 МГц. Далее синфазная и квадратурная составляющие поступают на два синхронно работающих АЦП. Выборка сохраняется в буферной памяти и затем передается в DSP для вычисления спектра.

РЕАЛИЗАЦИЯ СИСТЕМЫ

Описанный выше принцип использовался разработчиками для решения задачи построения приемной части системы интеллектуального блокирования сотовой связи и беспроводного доступа всех действующих в России стандартов. В качестве примера рассмотрим конкретный приемный тракт, предназначенный для мониторинга в масштабе реального времени прямых или обратных каналов радиолинии сотовой связи стандарта GSM, в частности, для контроля выхода в эфир и определения несущих частот абонентских аппаратов. Суммарный диапазон частот в этом стандарте составляет 100 МГц. Для его контроля используются четыре линейных приемника с полосой пропускания 25 МГц каждый, построенные по принципу прямой конвертации сигналов вниз с разложением на квадратурные составляющие, и автономная система ЦОС. Блок-схема линейного приемника приведена на рис.1.

Входной сигнал через коммутатор, переключающий прямые и обратные каналы, поступает далее на прямой конвертер вниз. Гетеродин содержит ГУН и синтезатор частоты, управляемый системой ЦОС через микроконтроллер по шине RS-232. Система ЦОС управляет усилением конвертера в диапазоне до 46 дБ. Поскольку частота гетеродина выбрана равной центральной частоте диапазона и используется квадратурная обработка, полосы пропускания фильтров низкой частоты выбраны равными половине ширины диапазона, то есть 12,5 МГц. Квадратурные сигналы с конвертера после обработки фильтром низкой частоты поступают на систему ЦОС.

Автономная система ЦОС, выполняющая функции цифрового обнаружителя-анализатора, построена на базе автономного DSP-контроллера типа «Tornado-E67» фирмы MicroLab Systems Ltd, на котором установлена плата дочернего модуля высокоскоростного АЦП/ЦАП с параллельным интерфейсом AD/DA PIOX DCM, как показано на рис. 2.

Контроллер с дочерней платой имеет на входе два 12-разрядных параллельных синхронных АЦП с максимальной скоростью тактирования 65 МГц. Тактирующий генератор установлен на плате. Таким образом, дочерний модуль позволяет оцифровывать два входных сигнала в полосе до 30 МГц и передавать данные, накопленные в буферной памяти FIFO, объемом 256 Кб через параллельный 16-разрядный интерфейс PIOX-16 I/F на материнскую плату DSP-контроллера для дальнейшей обработки. Помимо этого, на входе дочерний модуль содержит два статических 4-разрядных мультиплексора MUX перед АЦП, что позволяет организовать 4 канала квадратурного аналого-цифрового преобразования, последовательно осуществляющих скоростную выборку для расчета спектра по алгоритмам БПФ (Быстрое преобразование Фурье).

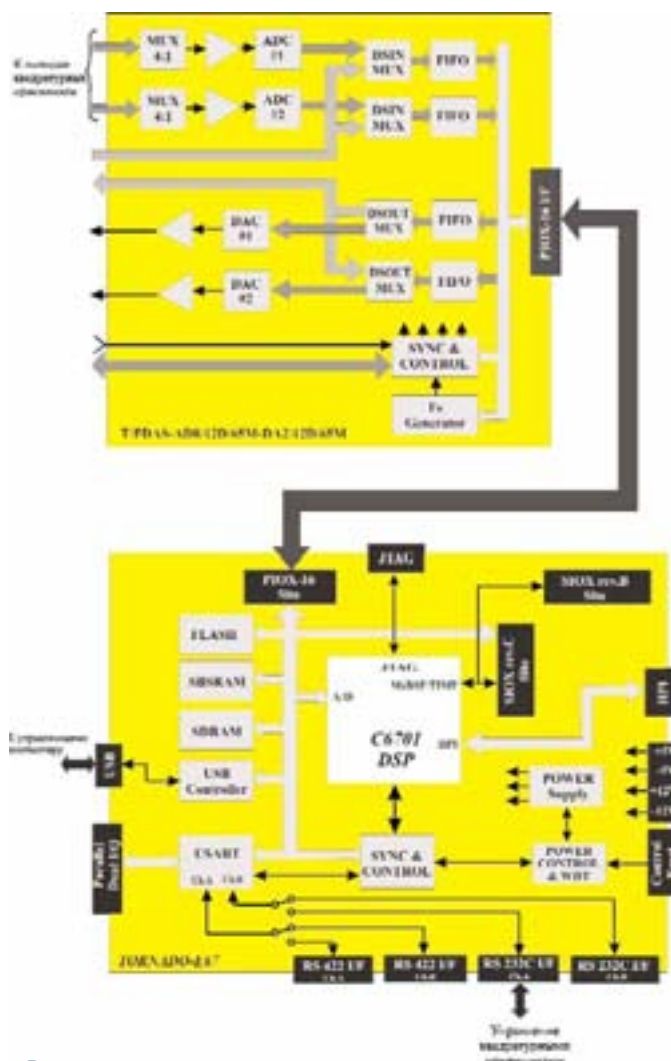


Рис. 2

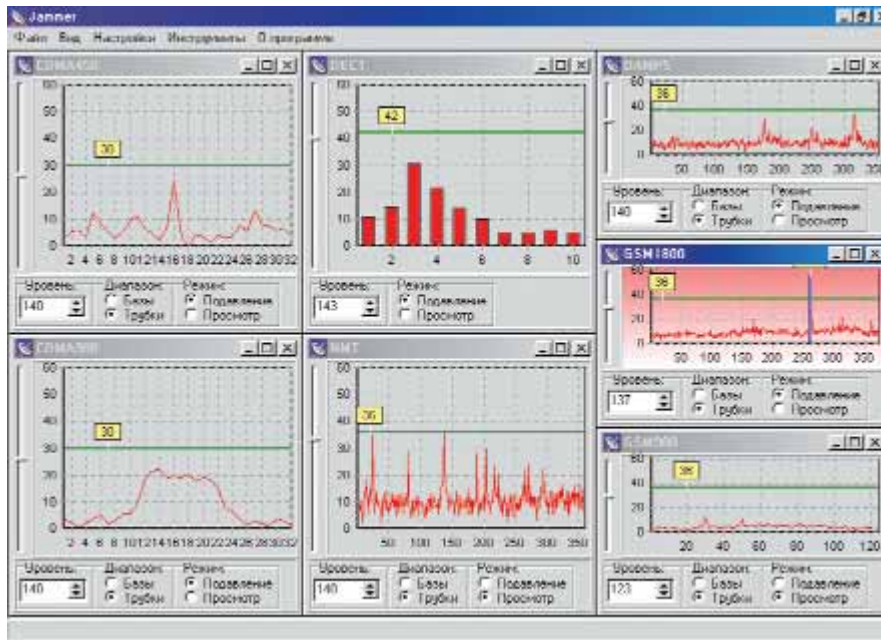


Рис. 3

Основным ядром контроллера «Tornado-E67» является цифровой сигнальный процессор TMS 320C6701 (32 бита, плавающая запятая 1000 MFLOPS) фирмы Texas Instruments, чья архитектура оптимизирована под параллельные вычисления. На плате установлена микросхема высокоскоростной синхронной пакетной (burst) SRAM (SBARAM), синхронной SDRAM и флэш-памяти FLASH. На плате имеется 2-канальный универсальный синхронно/асинхронный приемопередатчик USART (10 Мбит/с) с двумя двухканальными интерфейсами RS422 I/F (10 Мбит/с) и RS232 (115 кбит/с), а также USB-контроллер для подключения по шине USB управляющего компьютера. Плата содержит параллельный интерфейс PIOX-16 для подключения дочернего модуля, последовательный интерфейс SIOX для управления внешними устройствами и порт JTAG для подключения эмуляторов. Для обработки данных и расчета комплексного спектра 2 по 1024 точек по алгоритму FFT контроллеру требуется время не более 17 мкс. Отладка аппаратно-программных средств с помощью скан-эмуляторов TI XDS510 и MicroLAB Systems MIRAG-5100 осуществлялась при поддержке интегрированной среды разработки ПО Code Composer Studio IDE фирмы TI.

Суммарное время накопления выборки и расчета комплексного

спектра составляет 20 мкс, что позволяет трижды за время действия импульса запроса со стопроцентной вероятностью обнаружить сигнал. Решив задачу обнаружения импульса запроса в соответствии с протоколом стандарта, система ЦОС вычисляет канал и временной интервал, в которых базовой станцией будет передана информация, предназначенная конкретному абоненту, выдавшему запрос. Управляя быстрыми синтезаторами частоты блока подавления, можно без проблем поставить точечную помеху приемнику абонента и пресечь возможность получения требуемой информации для проведения аутентификации. Абонентская трубка, сделав ряд попыток произвести соединение, возвращается в режим покоя, оставаясь на обслуживании в сети.

Система ЦОС выполняет функции дискретного спектрального анализа, а также управления приемниками и всей системой в целом. Один DSP-контроллер полностью обеспечивает обнаружение и анализ сигналов сотовой системы стандарта GSM в масштабе реального времени, поскольку этот анализ требует наибольших вычислительных ресурсов. Аналогичный DSP-контроллер одновременно обрабатывает сигналы сотовой телефонии стандартов AMPS/DAMPS, CDMA, NMT-450, WCDMA и беспроводного доступа DECT. Система может

работать в полностью автономном режиме либо с выводом данных на управляющий компьютер через шину USB. Загрузка программ для DSP и параметров системы производится также через USB-порт. Пользовательский интерфейс показан на рис. 3.

Эффективность подавления заградительной помехи прицельной помехой для систем с временным разделением доступа (TDMA) определяется тем же соотношением полосы всего диапазона заградительной помехи и полосы канала, в котором действует прицельная помеха, то есть 20-26 дБ в нижнем и верхнем диапазонах стандарта GSM. Однако, учитывая то, что прицельная помеха является кратковременной (пачка в четыре импульса длительностью 200-300 мкс), а заградительная действует постоянно, реальная (интегральная) эффективность интеллектуального подавителя несоизмеримо выше эффективности системы с заградительной помехой.

Описанная выше аппаратура предназначена для предотвращения утечки информации по каналам сотовой телефонии и беспроводного доступа при проведении закрытых мероприятий и совещаний в больших помещениях и залах. Для обеспечения тишины она может быть использована в театрах, концертных залах и т. д.

ЛИТЕРАТУРА:

1. Громаков Ю.А. Стандарты и системы подвижной радиосвязи. М.: Мобильные ТелеСистемы-ЭкоТрендз, 1997.
2. Марпл-мл. С.Л. Цифровой спектральный анализ и его приложения. М.: Мир, 1990.
3. Васильев О.А., Егоров Д.О., Кадыков А.Н. Цифровая обработка сигналов в системе радиомониторинга // Инженерная микроэлектроника (Chip News). — 2003. — № 6.

Компания «Радиосервис»

127287, Россия, Москва,
Петровско-Разумовский пр-д, д. 28
тел/факс: (095) 214-61-21, 214-76-62
214-85-93, 214-67-62

тел: (095) 798-75-99
e-mail: rserv@radioservice.ru
http://www.radioservice.ru

