

Охота на лис

En Fox hunting

O. A. Vasiliev,
Director
Radioservice Co.
rsjet@mail.ru

This article presents modern tendencies in the development of jamming systems aimed to design universal multi-purpose digital wideband jammer. There are examples of the new jamming systems produced in our country and abroad.

Keywords: digital wideband jammer, DDS technology, unmanned aerial vehicle – UAV

В статье рассматриваются современные тенденции в развитии систем подавления цифровой связи, глобальной навигации, линий управления БПЛА, направленные на построение универсальных многоцелевых цифровых джаммеров. Приводятся примеры новейших систем подобного типа как зарубежного, так и отечественного производства.

Ключевые слова: цифровой джаммер, технология DDS, сотовая связь, беспилотный летательный аппарат – БПЛА

Олег Александрович Васильев,
директор
Компания «Радиосервис»
rsjet@mail.ru

Вы случайно никогда не увлекались радиоспортом? Ну, например, «охотой на лис»? Люди старшего поколения хорошо помнят, как под эгидой ДОСААФ этот вид спорта, кросс или ориентирование с радиопеленгатором, был широко популярен в СССР, даже шел в прокате художественный фильм с аналогичным названием. Если заглянуть в Википедию, то легко обнаружить, что «охота на лис» по-прежнему жива и здорова, и у нас в стране действует Федерация радиоспорта России, культивирующая эту «охоту» и проводящая массу соревнований. Настоящие энтузиасты, честь им и хвала за это! Но мне немного обидно за ребят, увлекающихся этим видом радиоспорта, так как его техническая сторона безнадежно устарела: приемник-пеленгатор крайне примитивен, ну, а пробежать кросс можно и со смартфоном, ориентируясь по GPS.

В современном мире полно технических видов спорта, в том числе и связанных с радио, соответствующих внедрению в нашу жизнь передовых технологий, например, гон-

ки радиоуправляемых дронов. Правда, применительно к России я что-то об этом не слышал, где ДОСААФ? Знаю, однако, есть энтузиасты и у нас: конструируют беспилотники, «по-научному» – БПЛА (беспилотные летательные аппараты), и даже ездят на выставки, конкурсы, соревнования. И места занимают призовые! Вот и наша скромная компания озабочилась, как бы «примазаться» к модному прогрессу. С Илоном Маском, то бишь со Space-X, тягаться в области освоения космоса бессмысленно. Конкурировать с DJI, главным мировым производителем коммерческих БПЛА, тоже не с руки, а вот сообразить нечто в плане защиты от злонамеренно используемых дронов, особенно, если требуется что-то подавить, заблокировать, снуфить в каналах радиуправления БПЛА, – да, это наш профиль!

Для начала предложим читателю небольшой экскурс в мир дронов или БПЛА и кратко перечислим, какие угрозы, в том числе информационные, может нанести такой «не-санкционированный» дрон.

Радиоканалы управления и передачи информации БПЛА

Будем интересоваться, главным образом, коммерческими дронами. Помимо выполнения полезной, часто профессиональной работы, такой

как наблюдение за ситуацией на земле, обеспечение безопасности массовых мероприятий, фото- и видеосъемка, контроль нефте- и газопроводов и т. д., дроны могут использоваться в террористических и других противозаконных целях: для транспортирования и доставки запрещенных грузов (например, наркотиков или взрывчатых веществ), несанкционированной съемки объектов, разведки закрытых территорий и т. д.

Большинство дронов можно отнести к разряду роботов, так как они способны летать автономно, используя для ориентации системы глобальной навигации, в основном GPS и ГЛОНАС, реже – Galileo и BeJue. При этом, по действующим во многих странах законам, оператор обязан держать БПЛА в поле своего зрения, оставляя возможность для их ручного управления с пульта. Кроме того, необходимо наличие радиолиний для оперативной передачи собранной дронами информации. Это не только поток видео, но и различная телеметрия, звук и т. д., передаваемые в режиме реального времени. Сегодня большинство дронов используют частоты нелегальных диапазонов: 433 МГц, 868 МГц, 2,4 ГГц, 5,8 ГГц.

Уточним типы каналов связи, а также технологии и виды сигналов, применяемые для БПЛА. В большинстве случаев для управления используют диапазон 2,4–2,483 ГГц, а для достижения высокой помехоустойчивости радиолинии – широкополосные сигналы с технологиями FHSS и DSSS (скачки по частоте и ШПС). Каждый производитель использует свои собственные протоколы для каналов управления, поэтому они несовместимы для БПЛА разных производителей. Для передачи видеоизображения чаще всего используется частотный диапазон 5,6–5,8 ГГц с технологией OFDM. Этот вид модуляции имеет очень высокую скорость информационного потока (*bit rate*), однако гораздо менее помехоустойчив по сравнению с используемыми в каналах управления широкополосными сигналами. Иногда видео передается просто через Wi-Fi. Для передачи телеметрии могут использоваться различ-

ные каналы и протоколы на безлицензионных частотах, например, отдельный канал в диапазоне Wi-Fi 2,4 ГГц, иногда – встроенный в видеоканал, иногда – через Zigbee на частоте 868 МГц.

Необходимо отметить, что использование общего диапазона частот приводит к интерференции сигналов Wi-Fi и каналов управления БПЛА, следствием чего является потеря информации, нарушение связи, искажения в каналах беспроводного доступа вплоть до полной потери управления дроном. Вопрос взаимного влияния систем связи регулируется стандартом ETSI (*European Telecommunications Standard Institute*). Однако, в отличие от DJI, многие производители его не соблюдают. Теперь, зная диапазоны и виды сигналов, мы можем понять, во-первых, что и как требуется подавлять в эфире для нарушения полета дрона, а, во-вторых, то, в каких диапазонах следует искать сигналы управления дроном и поступающую от него информацию. Заметим, что нелегальные частотные диапазоны наиболее опасны и для систем защиты от радиовзрывателей (RIED), поэтому задачи подавления радиоканалов управления БПЛА и защиты от радиовзрывателей в некотором смысле схожи.

Теперь перейдем непосредственно к описанию технологий подавления сигналов и выберем оптимальную для этого стратегию.

Технологии подавления или блокирования сигналов

Какие помехи наиболее «зловредны» для данного вида сигналов? Или по-другому: какой вид сигнала наиболее помехоустойчив? Вопрос, поднимаясь с давних пор и не имеющий точного ответа. Основные постулаты здесь звучат так:

- спектр помехи должен целиком лежать в полосе подавляемого сигнала;
- если структура сигнала известна, но нет точной копии сигнала передаваемого в данный момент времени, то сигнал на входе приемника можно подавить только энер-

гетически, причем форма блокирующего сигнала не имеет определяющего значения.

Это как при кодовом доступе каналов в системе сотовой связи WCDMA. Из практики блокирования сотовой связи и беспроводного доступа известно, что для блокирования сигналов базовой станции 3G (UMTS–WCDMA) необходимо превышение мощности принятого сигнала на входе приемника абонента не менее чем на 26–30 дБ, то есть на 16–20 дБ больше, чем для сигналов GSM!

Исторически сложилось так, что для подавления либо использовали аналоговые ЛЧМ-сигналы (сигналы с линейной частотной модуляцией), либо строили системы защиты по принципу реформера, когда принятый сигнал «корректировался» в приемнике и переизлучался в обратном направлении на источник. Этот способ особенно популярен в военной авиации, подобные устройства стояли практически на всех советских истребителях. Современные аналоги осуществляют описанные операции в цифровом виде и достаточно компактны. Однако в настоящее время первенство захватила технология DDS (прямой цифровой синтез). Рассмотрим как выглядит структура цифрового DDS-джаммера и каковы последние веяния в этой технологии.

В основе джаммера лежит формирователь блокирующих сигналов. Обычно это несколько DDS-чипов, управляемых FPGA (программируемые пользователем вентильными матрицами). Соответственно, программирование под конкретную задачу осуществляется с внешнего компьютера через USB или Ethernet. В настоящее время передовые производители выпускают полностью цифровые формирователи на базе новейших чипов DDS и DAC, имеющих очень высокие тактовые частоты, например, 12,6 ГГц у ЦАП типа AD9173 фирмы Analog Devices. Такой чип позволяет напрямую формировать сигналы с частотой вплоть до 6 ГГц.

Кроме формирователя для джаммера требуется широкополосный усилитель мощности. Благодаря новейшим технологиям стало возможным производство усилителей мощ-

ности, обладающих хорошим согласованием с нагрузкой в достаточно широкой полосе частот. Наиболее доступны усилители, производимые компаниями MCOM, Minicircuits и рядом южнокорейских фирм. На базе мощных выходных транзисторов или микросборок разрабатываются широкополосные усилители мощности с коэффициентом усиления 40–50 дБ и мощностью до 100 Вт и выше, представляющие собой законченный блок, готовый к использованию и требующий хорошего естественного охлаждения либо достаточно мощной вентиляционной системы. Такой чисто аналоговый усилитель нужен любому джаммеру, будь он хоть трижды цифровой. На рис. 1 представлен широкополосный усилитель мощности, производимый компанией «Радиосервис», имеющий коэффициент усиления 38 дБ и 10 Вт мощности сигнала на выходе в диапазоне 400–3000 МГц либо в диапазоне 2–6 ГГц.

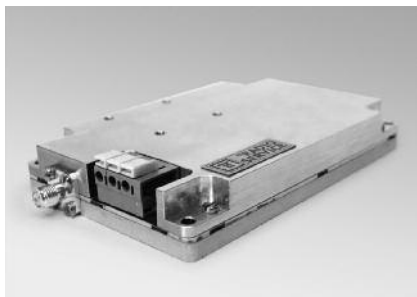


Рис. 1. Широкополосный усилитель мощности производства компании «Радиосервис»

Важным моментом в общей компоновке системы подавления является подбор антенн, особенно для широкополосных программируемых джаммеров. Дело в том, что широкополосные антенны в подавляющем большинстве имеют довольно низкую направленность. В принципе это неплохо, когда надо обеспечить широкий угол атаки или большую по площади ближнюю зону подавления. Однако применение направленных антенн позволяет использовать гораздо меньшую мощность передатчика сигнала подавления в системах противодействия дронам, поэтому мы и видим на вы-

ставках по безопасности бесчисленное множество различных направленных подавителей, где антенная система спроектирована в виде ружья из «Звездных войн» или иного фантастического боевика. Даже концерн «Калашников» не чурался выставить нечто подобное на выставке вооружений в Подмоскowie в прошедшем году.

Тем не менее, чтобы это сработало, требуется наличие системы обнаружения дронов. И тут фантазия разработчиков разыгрывается по-настоящему. Используют обнаружение радиосигналов в полусфере (Aaronia), радиолокацию (Blighter), тепловизоры, приборы ночного видения и т. д. Понятно, что на «ружье» можно разместить разве что оптический прицел и что-то еще по мелочи. Отметим, что направленная антенна даст выигрыш в 10–12 дБ, а это значит, что для создания на входе приемника канала управления дроном помехи, достаточной для подавления, требуется усилитель с меньшей на 10–12 дБ мощностью, например, не 100 Вт, а всего 10 или меньше, а это совсем другие габаритные размеры, время работы от батарей и т. д.

Многие зарубежные производители, например компании KIRINTEC LTD (Mercury BLADE5) и UNIVALGROUP GMBH (XWJ2), позиционируют свои системы подавления как набор универсальных подавителей мощностью от 10 до 100 Вт, из которых можно скомпоновать систему для решения определенных задач. Эти системы могут содержать 1–2 блока (вариант *map pack*, то есть переносной) или 5–6 и более (вариант *vehicle* – автомобильный). Используемое в них программное обеспечение каждый производитель держит в секрете, а некоторые даже оборудуют прибор кнопкой мгновенного стирания настроек системы.

RS6000 – универсальный подаватель сигналов цифровой связи, управления и глобальной навигации

Решающим фактором живучести и эффективности подавителя (джаммера) является наличие возможности его перепрограммирования и дис-

танционного управления, позволяющего менять конфигурацию, управлять спектром и частотным диапазоном. Как показано выше, подобным образом построены все современные системы подавления. Следуя этим тенденциям, компания «Радиосервис» разработала многоцелевой портативный цифровой широкополосный подаватель (джаммер) RS-6000, позволяющий программно менять структуру сигнала блокирования, количество диапазонов, ширину спектра, вид модуляции и другие параметры блокирующего сигнала. Прилагаемое программное обеспечение позволяет делать это дистанционно – как по Wi-Fi, так и по сетевому кабелю (Ethernet).

Блокиратор может состоять из одного, двух и более модулей. Каждый модуль способен подавлять до четырех частотных полос (каналов) шириной до 100 МГц, каждая из которых может быть выбрана пользователем в диапазоне частот от 400 до 3000 МГц либо от 2 до 6 ГГц в зависимости от используемого в конкретном модуле усилителя мощности с отдельной регулировкой выходной мощности в каждом канале. Оператор может создавать коммуникационное окно для своих задач между двумя частотными диапазонами блокирования. Все настройки могут быть сохранены и, в случае необходимости, восстановлены из файла. Система содержит переключаемые фильтры для подавления гармоник и других побочных излучений.

В алгоритмах функционирования используется временное мультиплексирование каналов, позволяющее существенно экономить энергетический ресурс системы. Управлять всей системой и контролировать процесс подавления можно даже с обычного планшета. Оператор имеет возможность выбрать требуемый для блокирования сигнал из набора стандартных или синтезировать его по собственному усмотрению. Так, подаватель может быть запрограммирован для блокирования сотовой связи и беспроводного доступа всех известных стандартов, включая 2G, 3G, 4G, Wi-Fi, Bluetooth и т. д. В случае радиомониторинга аппаратура

позволяет оператору подавлять любые подозрительные сигналы после их обнаружения путем программирования блокиратора на определенный частотный диапазон.

При формировании сигнала используются технологии прямого цифрового синтеза сигналов DDS и мультиплексирования каналов во времени, что позволяет достичь высокой эффективности блокирования и значительно уменьшить энергопотребление, а также минимизировать габаритные размеры и массу прибора и свести до минимума его вредное воздействие на оператора и находящихся в зоне работы джаммера людей. Такие технологии позволяют создать компактную систему блокирования, использующую всего два модуля RS6000 и две встроенные направленные антенны. Подобный портативный подавитель, смонтированный в кейсе (рис. 2) и снабженный интегрированной системой принудительного охлаждения, может быть предназначен для подавления сотовых телефонов и каналов беспроводного доступа всех действующих стандартов, а также для нейтрализации иных выявленных источников несанкционированных радиоизлучений. Также возможно подсоединение внешних направленных или ненаправленных антенн. Та же конструкция, но размещенная в пластиковом рюкзаке, используется для портативного подавителя сигналов управления и передачи информации БПЛА. В этом случае используется внешняя антенная система, монтируемая на прикладе спортивного карабина. Восемь каналов такого подавителя программируются для блокирования сигналов глобального позиционирования и для подавления линий управления БПЛА в нелицензируемых частотных диапазонах 2,4 ГГц и 5,8 ГГц.

Система полностью автономная, каждый модуль имеет собственный IP-адрес, что позволяет оператору осуществлять дистанционный контроль, а также задавать нужные полосы частот и уровни мощности, используя Ethernet или Wi-Fi-соединения. Технические характеристики системы RS6000/2 представлены в табл 1.

Таблица 1. Технические характеристики системы подавления RS6000/2

Диапазон частот подавления	400–6000 МГц
Число каналов подавления	8 (12 опционально)
Регулируемая полоса частот канала	0–100 МГц
Макс. полоса частот канала в диапазоне 4–6 ГГц	200 МГц
Выходная мощность в непрерывном режиме	20 Вт (100 Вт опционально)
Суммарная эффективная мощность в режиме мультиплексирования	80 Вт (400 Вт опционально)
Регулировка выходной мощности	30 дБ
Антенная система	КНД 5–12 дБ, две встроенные направленные антенны
Управление	Компьютер с ОС Windows, планшет или смартфон
Источник питания	Съемные батареи или адаптер переменного тока/зарядное устройство
Тип батарей	Li-Ion 14,8 В
Время работы от одного набора аккумуляторов	1,5–2 ч
Уровень шума системы охлаждения на расстоянии 1 м	Не более 35 дБ
Температурный диапазон	–10 ... +55 °С
Масса (8 каналов со встроенными антеннами в кейсе)	10–12 кг
Габаритные размеры (8 каналов со встроенными антеннами в кейсе)	45×30×20 см



Рис. 2. Смонтированный в кейсе портативный подавитель

Интеллектуальный режим (Reactive Jamming)

Поддаватель RS6000 может функционировать и как интеллектуальный блокиратор, активируемый только тогда, когда появляется сигнал абонента связи или обнаружен несанкционированный сигнал, например, сигнал управления БПЛА. В интеллектуальном режиме (*Reactive Jamming*), а также для контроля работы джаммера, используется новейшая версия анализатора спектра (приемника) реального времени **Spectrum Jet 3.0** (рис. 3). Цифровая плата анализатора имеет интерфейс USB-3.0, позволивший обеспечить скорость мониторинга вплоть до 30–50 ГГц/с при разрешении 10 КГц.

Линейный приемник анализатора выполнен в новом конструктиве на единой плате в экранированном корпусе. Он содержит преселектор, двойной супергетеродин и управляющий контроллер. С выхода промежуточной частоты (ПЧ) сигнал поступает на 16-битный АЦП, прямой цифровой конвертер вниз (*Direct*



Рис. 3. Анализатор спектра (приемник) **Spectrum Jet 3.0**

Down Converter – DDC), реализованный на ПЛИС, и далее на коммуникационный контроллер интерфейса USB-3.0. Дальнейшая обработка сигналов осуществляется в компьютере по классической схеме SDR (*Soft Defined Radio*). Основные технические характеристики анализатора представлены в табл. 2.

Специализированное ПО **Spectrum Jet 3.0/Jammer** позволяет решать задачи контроля заданных диапазонов, обнаружения радиосигна-

лов и включения передатчика подавителя.

Еще раз напомним, что все настройки сохраняются до следующего включения аппаратуры. Изменять же их можно даже в процессе работы подавителя. Для быстрой перестройки можно использовать заранее заготовленные профили. Портативный джаммер, использующий технологию прямого цифрового синтеза (DDS), не привязан к конкретному стандарту или диапазону и может быть запрограммирован как для блокирования сотовой связи, так и под задачу подавления каналов управления несанкционированным БПЛА. В заключение, приведем *основные особенности системы RS6000*:


- прямой цифровой синтез сигналов блокирования (DDS-технология);
- мультиплексирование каналов во времени;
- малая масса и высокий уровень выходной мощности;
- подавление всех существующих стандартов связи (2G, 3G, 4G, Wi-Fi);
- подавление каналов систем глобального позиционирования;
- подавление каналов управления БПЛА и транслируемого видео;
- программируемые частотные каналы;
- низкий уровень внеполосных излучений;
- высокая энергетическая эффективность;
- малые габаритные размеры и дизайн под заказ;
- направленная зона покрытия. 

Таблица 2. Технические характеристики анализатора спектра реального времени (RTSA) **Spectrum Jet 3.0**

Диапазон частот	9 КГц – 6 ГГц
Скорость сканирования с разрешением 10 КГц	30–50 ГГц/с
Промежуточная частота	140 МГц
Полоса ПЧ	24 МГц
Полосы пропускания анализатора спектра	160 КГц – 32 МГц
Отображаемый средний уровень шумов (DANL) 30 МГц – 6 ГГц,	–155 дБ/Гц
Коэффициент шума	Не более 12 дБ
Избирательность по зеркальному каналу	Не менее 70 дБ
Динамический диапазон, свободный от интермодуляционных составляющих (SFDR)	Тип. 80 дБ
Время перестройки линейного приемника не более	150 мкс
Фазовый шум гетеродина при отстройке на 10 кГц (на частоте 1 ГГц)	Не более –86 дБн/Гц
Долговременная нестабильность гетеродинов	10 ppm
Максимальный уровень входного ВЧ-сигнала	Не более 20 дБм
Рабочий диапазон температур	–20 ... +60 °С
Габаритные размеры	174×80×32 мм
Масса	400 г



Компания «Радиосервис»

125130, Москва,
Стропетровский проезд,
д. 7а, стр. 25
Тел./факс: +7 (495) 627-57-17
e-mail: rs@radioservice.ru
http://www.radioservice.ru