

Тихий дрон

En And Quiet Flows the Drone

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

Article provides an overview of drone monitoring technology and Counter-Drone equipment, also known as Anti-Drone or Counter-UAS (C-UAS) technology. Also provide examples of the radars for drone detection, and integration technologies for Counter-Drone equipment in one system.

Keywords: unmanned aerial vehicle (UAV), drone, real time spectrum analyzer, drone monitoring, radar, lidar, jammer, global navigation

В статье представлен обзор технологий мониторинга и противодействия несанкционированным беспилотным летательным аппаратам (БПЛА), или дронам. Приведены примеры наиболее удачных решений в области радиолокации дронов с малой эффективной площадью рассеивания (ЭПР), вплоть до $0,01\text{ м}^2$. Рассмотрена интеграция технологий противодействия дронам в единую систему.

Ключевые слова: беспилотный летательный аппарат (БПЛА), дрон, анализатор спектра, мониторинг дронов, радар, лидар, блокиратор, глобальная спутниковая навигация

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

*Редкий дрон долетит
до середины реки...*

Настоящая статья посвящена рассмотрению вопросов защиты объектов от несанкционированного проникновения беспилотных летательных аппаратов (БПЛА), или дронов, в воздушное пространство над территорией охраняемого объекта. Характерные примеры последних – аэродромы, АЭС, воинские части, структуры пенитенциарной системы и т. д. Таким объектом могут быть массовые мероприятия в пределах городской застройки, стадионы, частные территории, да просто VIP-персоны на прогулке.

Если целью владельца дрона является фото- или видеосъемка, то это ни что иное, как хищение информации, и чтобы ее предотвратить противной стороне потребуется маленькая система ПВО! В связи с этим перед специалистами по безопасности встают весьма непростые задачи выбора соответствующих технических решений ввиду существования

различных методов и технологий, направленных на борьбу с несанкционированными дронами. Среди подобных задач наиболее сложной является объединение этих технологий в единый комплекс. Архитектура таких комплексов может быть абсолютно разной, но всегда будет зависеть от экономической составляющей проекта.

Технологии мониторинга дронов

Как и положено в ПВО, первой задачей является обнаружение дрона, и чем раньше будет обнаружена угроза, тем больше шансов на эффективное противодействие. Для обнаружения угрозы необходимо постоянно осуществлять мониторинг окружающего пространства, или просто мониторинг дронов. Методы обнаружения можно разделить на пассивные и активные. К первым относятся видеонаблюдение, радиомониторинг, акустика, ко вторым – радио- и лазерная локация.

Впрочем, только обнаружения зачастую бывает недостаточно: требуется также решить задачи классификации (или идентификации), локализации и слежения (трекинг). Радар, например, может спутать БПЛА

с птицей. Существуют специальные алгоритмы обработки информации – распознавание и идентификация типа дрона, вплоть до определения модели.

Классификация очень полезна, поскольку дает возможность отличить дрон от иных объектов, таких как самолеты, поезда, автомобили и т. д. Идентификация возможна для моделей дрона с контроллером, управляемым по каналу Wi-Fi (перехват MAC-адреса).

В соответствии с перечисленными выше технологиями, существуют основные типы оборудования для мониторинга дронов:

- анализаторы спектра или мониторинговые радиоприемники;
- акустические сенсоры или микрофоны;
- видеокамеры и тепловизоры (инфракрасные);
- радары или РЛС;
- лидары или лазерные локаторы.

Анализаторы спектра и мониторинговые приемники используются для обнаружения радиокommunikации между дроном и пультом управления (ПУ). Если использовать несколько приемников, то координаты дрона или местоположение ПУ дрона можно определить методом триангуляции. Некоторые производители радиосистем для обнаружения несанкционированных БПЛА и противодействия им, например AARONIA AG, используют для этих целей современные пеленгаторы на базе анализаторов спектра реального времени с антенной системой из равномерно расположенных 16 или 32 широкодиапазонных антенн (рис. 1).

Известные производители – это упомянутая AARONIA AG, Rohde & Schwarz (ARDRONIS) и Keysight (Keysight Surveyor 4D System). Понятно, что данные решения весьма дорогостоящие, и их применение не имеет особого смысла для защиты от коммерческих дронов, где частоты каналов управления и телеметрии хорошо известны. Отметим, что компания «Радиосервис» решала подобную задачу в диапазоне 0,5–18 ГГц, где антенная система состояла из 24 широкополосных антенн. В мобильном варианте она крепилась на крыше микроавтобуса. В настоя-

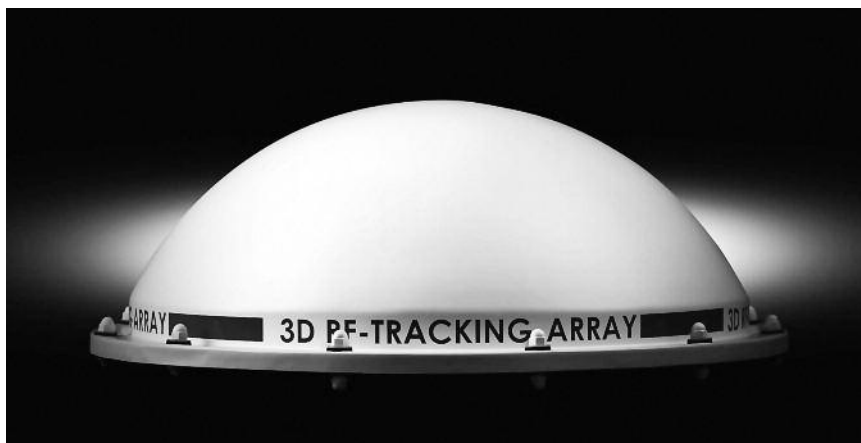


Рис. 1. Антенная система IsoLOG 3D DF-160

щее время мы вернулись к подобной системе, и рассчитываем показать ее на одной из ближайших выставок. В качестве базового мониторингового приемника используется двухканальный анализатор спектра реального времени «Spectrum Jet – 3,0» [1].

Надо отметить, что пассивная радиосистема не способна обнаруживать и сопровождать автономные дроны, работающие по координатам GPS или же по записанному ранее видеосигналу с вмонтированных в БПЛА видеокамер (до 8 штук в одной из моделей DJI). Однако, если у злоумышленника есть возможность управлять своим злым умыслом, он ею непременно воспользуется.

Для акустического мониторинга используются микрофонные решетки (Array), улавливающие звук от дрона и вычисляющие направление на него. Их недостатки – малая дальность обнаружения (300–500 м) и плохая работа при наличии городских шумовых помех.

Оптические сенсоры (камеры) – наиболее часто используемое оборудование для обнаружения и наблюдения за приближающимся БПЛА. Помимо стандартных дневных видеокамер требуются также инфракрасные (тепловизионные) – для ночного наблюдения. Видеокамеры обладают лучшим разрешением (точность автоматического наведения – вплоть до пикселя), однако невозможность работы в плохих погодных условиях (туман, дождь и т. д.) сводит на нет эти их преимущества перед радаром.

Насчитывается огромное множество производителей оборудования

для видеонаблюдения, в том числе и российских, использующих в своих изделиях, главным образом, импортную оптику и матрицы. В таких системах применяются объективы с 30- или 50-кратным оптическим увеличением. Аппаратуру для оптического мониторинга несложно подобрать в Интернете.

В данной статье основное внимание будет уделено радарам как наиболее эффективному оборудованию для обнаружения объектов в воздушном пространстве. Надо отметить, что радары имеют ряд существенных преимуществ перед остальными обнаружителями: большой диапазон расстояний (дальность), непрерывное сопровождение, высокоточная локализация, обработка множества целей, независимость от условий видимости, погоды, обнаружение и сопровождение автономных дронов. Изначально недостатком являлась невозможность различения дронов и птиц, однако теперь проблема преодолена, о чем будет рассказано далее.

Большинство радаров спроектировано для обнаружения и сопровождения больших объектов (целей), таких как самолет, ракета, автомобиль и т. д. С появлением БПЛА, особенно малоразмерных дронов, и следующих от них угроз, возникла потребность в устройствах, способных обнаруживать малые цели как на больших, так и на малых расстояниях. Причем такая аппаратура должна была стать портативной, переносной и приемлемой по энергетическим показателям. Наиболее близкой к подобному классу РЛС



Рис. 2. Радар R8SS-3D

были радары для охраны границ объектов от нарушителей и вертолетные радары для посадки в плохих погодных условиях. Первые работают в разрешенном частотном диапазоне 2,4 ГГц, вторые – в миллиметровом диапазоне (вплоть до 100 ГГц).

В новых разработках используют как импульсные, так и непрерывные локаторы. В работе [2] описывается РЛС с короткими наносекундными импульсами, что повышает разрешающую способность радара на фоне городской застройки. Однако большинство подобной аппаратуры использует непрерывный частотно модулированный сигнал FMCW radar (*Frequency Modulated Continuous Wave*). Подобную структуру, в частности, имеют РЛС компаний Blighter, FLIR (рис. 2) и Robin, в частно-

сти, радар Elvira, технические характеристики которых приведены ниже. Elvira разработан как доплеровский радар, способный определять направления и скорость вращения пропеллеров и тип дрона, а также отличать его от птиц.

Далее уделим внимание отечественным разработкам.

Предвидя острую необходимость в системах защиты от несанкционированных дронов и чувствуя общую суету вокруг этой проблемы, активизировались российские производители радаров для систем охраны периметра, в частности, аэропортов и госграницы, главным образом, модернизируя или просто приспособив радар к охране воздушного пространства и экспериментируя на доступных БПЛА. Приведем в каче-

стве примера радар «Радескан-Антидрон» (ЗАО «ЮМИРС»). Это моноимпульсный радар, работающий в диапазоне 2,4 ГГц, не требующем лицензирования. Трудно сказать, как он будет работать в городских условиях, где функционирует множество точек доступа Wi-Fi. Да и линии коммуникации дрона также могут работать в этом диапазоне частот. Компания «Стилсофт» из Ставрополя предлагает радар STS-177, работающий также в нелицензируемом диапазоне 5350–5650 МГц. Однако наибольший интерес, с нашей точки зрения, представляют изделия компании «ЭЛВИС» из Зеленограда и АО РТИ им. А. Л. Минца. Зеленоградское изделие «Енот», по-видимому, также «вырос» из производимого для охраны периметра радара Orwell-R, но является продуктом достаточно высокого уровня, во многом не уступающим зарубежным аналогам, например, радарам компании Robin, при этом обладающим существенно меньшими габаритными размерами и массой. Разрабатываемый в АО РТИ им. А. Л. Минца радар ЭЛИК [3] – еще меньше и сопоставим с ним по массе. Этот радар в дальнейшем может найти широкое применение и как бортовой локатор БПЛА или вертолета, и в качестве наземной аппаратуры для обнаружения несанкционированных дронов.

Основные технические характеристики всех упомянутых выше радаров сведены для удобства сравнения в [таблицу](#).

Таблица

Наименование	Тип радара	Диапазон	Дальность ЭПР 0,01м ²	Разрешение	Р-излучение	Габаритные размеры, масса	Примечание
Blighter A402	FMCW	Ku 15,6–17,2 ГГц	Мин.: 10м Макс.: 2,4 км	Нет данных	4 Вт	67×50×13 см 25 кг	90 град. пассивная антенная решетка (PESA)
FLIR Ranger R8SS-3D	FMCW	X-band	Мин.: 10м Макс.: 1,2 км	1,3 м / 0,8 град. по азимуту	Нет данных	37×36×11 см 10,5 кг	90 град. пассивная антенная решетка (PESA)
ELVIRA Robin radar	FMCW	X 9,65ГГц	Макс.: 3 км (DJI Inspier)	0,6 м	4 Вт	Диаметр: 91,8 см Высота: 106 см Масса: 79 кг	360 град. механизм сканирования
Радескан-Антидрон	Моно-импульсная РЛС	ISM 2,3–2,5 ГГц	Мин.: 20 м Макс.: 1,5 км	1,0 м/0,5 град. по азимуту	100 мВт в среднем	38×38×9,5 см	90 град. пассивная антенная решетка
STS-177 Стилсофт	Моно-импульсная РЛС	5,35–5,65 ГГц	Мин.: 20 м Макс.: 2,3 км	1,0 м/0,25 град. по азимуту	400 мВт в среднем	47×53×31,5 см 15 кг	Луч: 8 град. Обзор: 360 град.
Енот	Нет данных	X 8,2–9,5 ГГц	Макс.: 1,8 км	2,0 м/2 град. по азимуту	Нет данных	Диаметр: 64,5 см Высота: 31,5 см Масса: 14 кг	Обзор: 360 град.

В последние годы очень сильно развивается направление лазерной локации различных объектов (заметим, что в этом случае локатор называется лидаром). Достигнутые для лидара дальности пока не соответствуют требованиям рассматриваемых систем, однако они, как и радары миллиметрового диапазона, находят широкое применение для обеспечения безопасности самих дронов от столкновений с препятствиями в виде деревьев, стен зданий, заборов и т. д. Быстрыми темпами развивается и микроэлектроника для лидаров и радаров миллиметрового диапазона, применяемых в автомобилестроении для обеспечения безопасности на дорогах. Этот вопрос выходит за рамки данной статьи, но остается потрясающе интересным и заслуживает отдельной публикации.

Оборудование для противодействия дронам

Получив информацию о приближающемся дроне (направление, координаты, скорость) требуется обеспечить его сопровождение (трекинг), рассчитать, спрогнозировать траекторию и решить вопрос о принятии соответствующих мер. Если дрон представляет угрозу, то есть не идентифицирован как легальный, защитные действия могут заключаться в нейтрализации дрона или перехват управления таковым, что применимо при условии определения модели коммерческого дрона. Альтернативой этому будет его физическое уничтожение. Необходимо заметить, что в большинстве стран даже нейтрализация БПЛА требует лицензирования и законодательно запрещена. Рассмотрим далее основное оборудование и методы подавления дронов и противодействия им.

Джаммеры (блокираторы) излучают достаточно мощные шумоподобные радиосигналы в диапазонах работы радиолиний управления дроном и передачи информации и служебных данных (телеметрии) от дрона оператору. Подавление сигналов линии управления должно сопровождаться блокированием приема сигналов систем глобального позиционирования: GPS, GLONASS, GA-



Рис. 3. «Антидрон Rex-1»



Рис. 4. Самый экстравагантный способ борьбы с дронами

LILEO. Возможно несколько сценариев поведения дрона при воздействии на него сигналов подавителя:

- мягкая посадка в точке текущего позиционирования;
- возвращение на домашнюю позицию (это может быть и позиция цели);
- бесконтрольное падение на землю;
- дрон улетает в хаотическом бесконтрольном направлении.

Наиболее распространенным исполнением блокиратора каналов управления и навигации БПЛА является аппаратура в виде ружья, которое можно наводить на цель, используя оптику или лазер в качестве прицела. Эстетически да и технически удачной выглядит разработка ижевской фирмы ZALA, представленная на рис. 3.

Но «человек с ружьем» должен всегда находиться на посту, что далеко не всегда удобно, поэтому более подходящим вариантом является комплекс противодействия, со-

вмещающий функции обнаружения и слежения с подавителем, на котором антенны подавителя закреплены на общем опорно-поворотном устройстве (ОПУ).

Имеют место также системы, использующие спуфинг – подмену данных, передающихся с навигационного спутника, данными с передатчика спуфера, в результате чего последним позиция дрона может контролироваться.

Можно упомянуть и некоторые весьма экзотические способы противодействия дронам, в частности, уничтожение сверхмощным электромагнитным импульсом, выжигание видеоматрицы высокоэнергетическим лазером, стрельба сетками и, наконец, наиболее экстравагантный – захват и доставка дрона заказчику обученным орлом (не двуглавым, конечно) (рис. 4). Правда, процесс дрессировки такого «перехватчика» не быстрый – свыше года, но адресок можем дать.



Рис. 5. Полностью интегрированная система противодействия AUSS



Рис. 6. Комплекс «Радескан-Антидрон»

Если рассматривать только коммерческие дроны, то проблем с выбором частот блокирования вроде бы и не наблюдается, так как нелегализуемые диапазоны, в которых работают линии управления, передачи видео и телеметрии хорошо известны, так же, как и частоты GNSS (глобальной навигации). Обычно подавляют диапазоны 2,4–2,483 ГГц и 5,725–5,875 ГГц, широко используемые в дронах компании DJI (занимают около 60 % мирового рынка), и два-три диапазона глобальной навигации, например, L1, L2 и L3, GPS и GLONASS.

Успех зависит от выбора структуры сигнала блокирования, его мощности и в большой степени от направленности антенн. Разница в коэффициенте направленного действия двух антенн в 10 дБ при их

одинаковом удалении от цели и равной мощности излучения создаст в 10 раз большую напряженность электромагнитного поля в требуемой точке, то есть мощность передатчика можно уменьшить также в 10 раз. Однако широкополосные антенны не обладают достаточной направленностью. Приходится выбирать, чем поступиться. Мощность подавителей обычно простирается от единиц до сотен ватт. Цена растет резко с увеличением мощности и частоты. Ну что ж, остается отправить читателя на сайт компании «Радиосервис», где представлены системы блокирования с дистанционно изменяемыми параметрами (мощность усилителей – до 100 Вт).

Интеграция технологий в единой системе

Лучшим решением при построении комплекса противодействия дронам является использование (компиляция) наиболее эффективных для поставленной задачи технологий. Например, для обнаружения радиолиний управления и передачи информации необходим анализатор спектра или мониторинговый радиоприемник, причем высокоскоростной и определяющий направление на источник сигнала, фактически – пеленгатор. В комплексе AARTOS DDS производства AARONIA AG – это основной инструмент в системе обнаружения. В то же время в комплексе AUSS совместного производства британских компаний Blighter Surveillance Systems Ltd, Chess Dynamics Ltd и Enterprise Control Systems Ltd анализатора спектра нет, в них основой является радар. На рис. 5 представлена полностью интегрированная система противодействия БПЛА. На выдвижной штанге штатива неподвижно закреплен радар с четырьмя управляемыми электронной антенными решетками и суммарным рабочим углом по азимуту 360 град. В верхней ее части на опорно-поворотном устройстве закреплена платформа с коллимированно направленными видеосистемой, оснащенной тепловизором, и антеннами системы блокирования каналов управления дрона и сигналов систе-

мы глобальной спутниковой навигации. В состав комплекса входит консоль оператора и ПО для управления и принятия решений.

В предлагаемом российской компанией Umirs комплексе «Радескан-Антидрон» обнаружение осуществляется с помощью моноимпульсного радара, работающего в нелегализуемом диапазоне 2,4–2,5 ГГц. Рабочий сектор антенны – 90 град., для кругового обзора требуется 4 антенны. В простейшей комплектации добавляются видеочасть и тепловизор в защитном кожухе, закрепленные на ОПУ. Дальность обнаружения для целей с ЭПР 0,01 м² и 0,1 м² равна 1000 м и 1500 м соответственно. Для нейтрализации БПЛА используется подавление сигналов глобальной навигации и каналов управления на частотах, используемых коммерческими дронами, в данном случае – 433 МГц, 2,4 ГГц и 5,8 ГГц. На рис. 6 представлен комплекс «Радескан-Антидрон» в комплектации без подавителей глобальной навигации и каналов управления.

В заключение хотелось бы обратить внимание читателя на сложность оборудования, предназначенного для защиты от несанкционированных дронов. Множество предлагаемых на рынке «ружей» для «охоты» на БПЛА – всего лишь вершина айсберга. Чтобы сдвинуть ледяную гору с места, нужно объединить усилия разработчиков, специалистов по разным технологиям, программистов, дизайнеров. Наиболее удачные решения должны быть доступны для всех заинтересованных в создании актуального продукта. Компания «Радиосервис» открыта для сотрудничества (www.radioservice.ru). ■

ЛИТЕРАТУРА

1. Васильев О. А. Тайны реального времени // Защита информации. Инсайд. – 2019. – № 1 (85). – С. 36–40.
2. Ананенков А. Е., Марин Д. В., Нуждин В. М., Расторгуев В. В., Соколов П. В. К вопросу о наблюдении малоразмерных беспилотных летательных аппаратов // Труды МАИ. – 2016. – № 91 [Электронный ресурс]. – Режим доступа: <http://trudymai.ru/published.php?ID=75662/>.
3. Дороженко О. Начинается эпоха ЭЛИКов // INTEL&TECH. Интеллект и технологии. – 2019. – № 2 (23). – С. 40–43.