DOI: 10.22184/1992-4178.2017.166.6.82.88

СИСТЕМЫ ОБНАРУЖЕНИЯ РАДИОУПРАВЛЯЕМЫХ БПЛА

М.Макушин[1]

УДК 621.396
ВАК 05.12.00

Появление и развитие БПЛА иллюстрирует двойственность научно-технического прогресса: почти каждое открытие можно использовать как в благих, так и в преступных целях. Гражданские БЛПА – одно из ярких подтверждений этого. С одной стороны, устройства применяются в быту, на коммерческих рынках, а с другой, их использование привело к возникновению новых потенциальных угроз национальной и общественной безопасности. Разработки систем обнаружения и определения местоположения БПЛА, а также средств прерывания радиосигнала управления ими обеспечивают снижение уровня возникших угроз.

ТИПЫ БПЛА И ОБЪЕМ ИХ РЫНКА

Появление коммерческих БПЛА привлекло внимание потребителей и предпринимателей, которые предложили много новых, быстроразвивающихся направлений применения устройств – от видеосъемки и контроля посевов до создания инфраструктуры доставки различных товаров. По данным IC Insights, с учетом всех потенциальных сфер использования мировой объем продаж устройств в 2025 году может превысить 10 млрд долл. Однако оценки продаж/поставок БПЛА в стоимостном и натуральном выражении могут сильно различаться – стандартные требования оценки рынка отсутствуют. Решение одной из важнейших задач – управляемости – подразумевает возможность определения местоположения аппарата и реализацию им дистанционно формулируемых команд [1]. Оценки рынка БПЛА, сделанные корпорацией Gartner, приведены на рис.1.

БПЛА трудно классифицировать из-за различия характеристик, обусловленных избыточным наличием конфигураций и компонентов БПЛА. Пока не существует стандартов, определяющих типы устройств и их применение. Так, исследовательская корпорация J'son & Partners Consulting классифицирует БПЛА по следующим основным критериям:

- тип взлета;
- целевое назначение;
- технические характеристики;
- тип питания силовой установки;
- полезная нагрузка;
- тип системы автоматизации;
- система предотвращения столкновений;
- тип навигации;
- тип защиты от глушения сигналов;
- пропускная способность радиочастотного спектра;
- бортовая обработка данных;
- специализация программного обеспечения [2].

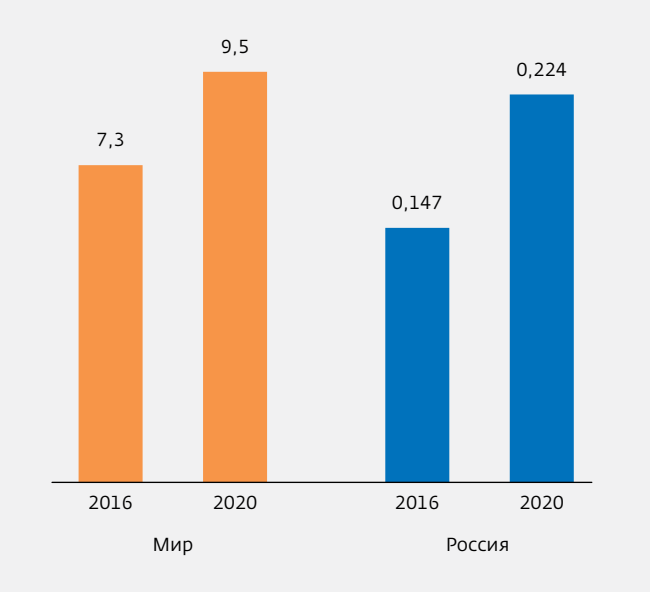

Рис.1. Оценка динамики мирового рынка БПЛА в 2016–2020 годах, млрд долл. *Источник: J'son & Partners Conculting*

[1] АО "ЦНИИ "Электроника", mmackushin@gmail.com.

ГРАЖДАНСКИЕ БПЛА КАК ИСТОЧНИК УГРОЗ

По данным Федерального управления гражданской авиации США (FAA), с начала декабря 2016 года по конец мая 2017-го было зафиксировано около 600 инцидентов, связанных с беспилотниками. Управляемые гражданскими лицами БПЛА создают немало проблем. Среди недавних происшествий можно вспомнить посадку БЛПА у Белого дома, столкновение БЛПА с самолетом British Airway в аэропорту Хитроу при посадке и т.д. В этих случаях опасности не возникло, но в будущем может быть иначе: такие БПЛА могут нести взрывчатые вещества, биологическое или химическое оружие для совершения террористических актов. Устройства также можно использовать для транспортировки контрабанды, наркотиков, глушения GPS-сигналов или Wi-Fi, что приведет к прерыванию связи и передачи данных.

С учетом этих и других угроз исследовательская организация ASD полагает, что развивающийся рынок систем противодействия БЛПА в 2022 году составит около 16 млрд долл. Таким образом, к тому времени расходы на системы обнаружения, определения местоположения и нейтрализации БПЛА превысят ожидаемый уровень доходов от их продаж в 2025 году (см. рис.1).

Неслучайно сегодня актуальными задачами являются проектирование систем обнаружения местоположения БПЛА, разработка мер и средств по снижению возникающих угроз.

Стандартные полосы частот радиоуправляемых БПЛА (по данным Keysight Technologies)

Обозначение полосы частот	Начало полосы частот	Конец полосы частот	Предельное значение мощности
УВЧ узкодиапазонные устройства	433,05 МГц	434,79 МГц	≤10 мВт ERP*
2,4 ГГц ISM	2,4 ГГц	2,4835 ГГц	≤100 мВт EIRP**
5,8 ГГц ISM	5,725 ГГц	5,85 ГГц	≤100 мВт EIRP

* ERP (effective-radiated power) – эффективная мощность излучения.

** EIRP (effective isotropically radiated power) – эффективная мощность изотропного излучения.

МЕТОДЫ ОБНАРУЖЕНИЯ И ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ РАДИОУПРАВЛЯЕМЫХ БПЛА

Радиоуправление БПЛА обычно осуществляется в одном из трех диапазонов спектра, зарезервированных для приборов с дистанционным управлением (см. таблицу). Данные диапазоны волн могут быть переполнены – особенно ISM 2,4 ГГц, в котором работает большинство коммерческих систем Wi-Fi, Bluetooth и IoT (то есть ZigBee-, Z-Wave-, LoRa-). Сигналы в этих полосах свободно регулируются с использованием правил свободного доступа. Если ISM 2,4 ГГц сейчас значительно загружена, то полосы SRD1 и ISM 5,8 ГГц пока относительно свободны. Однако со временем они могут стать самыми популярными.

Редакция Microwave Journal провела среди специалистов фирм Rohde & Schwarz, Keysight Technologies и Aaronia, которые имеют наибольший опыт в области беспилотных летающих аппаратов, опрос относительно методов определения типа БПЛА.

Отличить БПЛА от других летательных аппаратов непросто, что объясняется следующими факторами:

- виртуальное и звуковое обнаружение затруднено из-за ошибок, вносимых условиями окружающей среды и приводящих к ухудшению производительности системы обнаружения БПЛА;
- радары могут не обнаружить БПЛА малых форм-факторов;
- электрооптические датчики могут оказаться неэффективными в неблагоприятных погодных условиях (дождь или туман).

Радиочастотное обнаружение БПЛА, даже если его данные предварительно запрограммированы в системе (с использованием дискретных GPS промежуточных точек пролета), также может оказаться неэффективным при использовании только одной системы. Средства радиочастотного обнаружения как одни из ключевых элементов систем обнаружения гражданских БПЛА обладают преимуществами перед другими технологиями в скорости обнаружения.

К системам радиочастотного обнаружения предъявляются специальные требования: высокий уровень чувствительности, наличие возможности раннего обнаружения и минимизация ложного срабатывания.

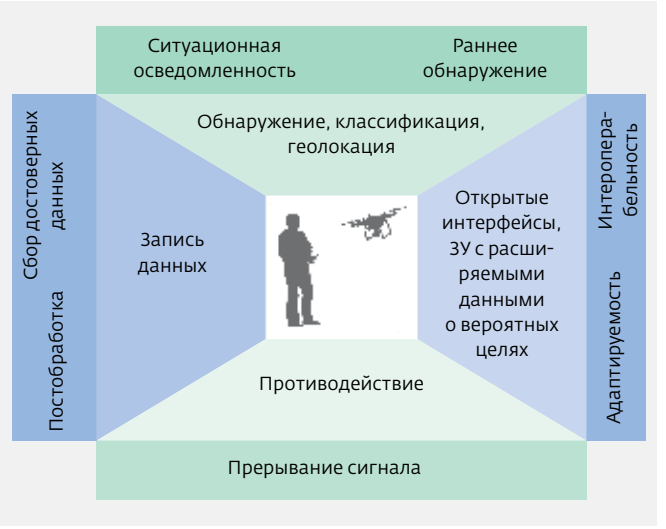

Рис.2. Основные функции систем обнаружения и определения местоположения БПЛА. *Источник: Rohde & Schwarz*

Подобные радиочастотные установки могут быть важным звеном полного интегрированного технологического цикла системы, использующей и другие сенсорные технологии (рис.2).

СИТУАЦИОННАЯ ОСВЕДОМЛЕННОСТЬ: ОБНАРУЖЕНИЕ, КЛАССИФИКАЦИЯ И ГЕОЛОКАЦИЯ

Специалисты фирмы Rohde & Schwarz (Бивертон, штат Орегон), в отличие от коллег из Keysight Technologies (Санта-Роза, штат Калифорния), насчитывают большее число частотных диапазонов управления БПЛА. Они уверены, что, хотя большая часть операций радиоуправления БПЛА осуществляется в нелицензируемых ISM-полосах частот 2,4 ГГц или 5,8 ГГц, используются и другие полосы частот, включая 433 МГц и 4,3 ГГц. Кроме того, иногда радиоуправляемые приборы работают на частотах, которые использовались раньше, например, 27; 35; 40,68 и 72 МГц, диапазон управления на этих частотах составляет до нескольких километров. В целях контроля возможных угроз (возможность обнаружения и отслеживания) системы должны быть снабжены широкополосной антенной и приемным блоком, которые способны контролировать все критические полосы частот. Кроме того, поскольку эти ISM-полосы и работающие в них приборы отличаются низкой мощностью (~100 мВт), а неавторизованные пользователи действуют одновременно с авторизованными, используя схожие технологии (наподобие WLAN), то для дистанционного обнаружения сигналов важна высокая чувствительность системы автоматического обнаружения. Надо отметить, что разделить пользователей на авторизованных и неавторизованных (несущих угрозы) может только опытный оператор.

Например, чтобы обнаружить БПЛА, в котором используется FHSS*-технология в полосе ISM 2,4 ГГц, система защиты должна осуществлять мониторинг по всем четырем выделенным каналам в течение некоторого времени по различным параметрам. Объединенный анализ всех параметров позволяет выявить сигнал, перескакивающий с одного канала на другой, его длительность, последовательность перехода между каналами и скорость перемещений в секунду. Это позволяет определить характерные особенности FHSS-дрона и впоследствии легко его распознавать.

Когда среда наблюдения заполнена пользователями, применяющими различные технологии (множественные WLAN-точки доступа и пользовательские терминалы, Bluetooth-технологии и IoT-приборы), FHSS-беспилотник может потеряться из вида. Кроме того, в некоторых БПЛА для управления используются WLAN-сигналы или линия нисходящей передачи видео. В этих условиях для обнаружения движения БПЛА необходимо обеспечить более детальный контроль и расшифровку сигналов WLAN. Специалисты Keysight Technologies считают, что для повышения быстродействия и эффективности защитной системы можно контролировать не весь спектр, а только те полосы частот, которые используются для управления БПЛА. При этом каждую из них можно конфигурировать по разрешающей способности (по полосе пропускания), определяющей размер бина (несущего канала) быстрого преобразования Фурье (наименьшая частота, которую можно различить – RBW). Помимо конфигурирования или одновременно с ним можно применять схемы усредненного отслеживания на основе стандартных полос пропускания и характеристик сигналов управления БПЛА. Например, ширина управляющих сигналов БПЛА в SRD**-диапазоне 400 МГц составляет обычно десятки килогерц. В этом случае применяется узкая RBW (менее 3 кГц). В 2,4-ГГц и 5,8-ГГц ISM-диапазонах ширина управляющего сигнала БПЛА составляет 1–2 МГц. В этом случае выгодно использовать более широкий RBW (20 кГц). Такая ширина RBW позволяет ускорить обработку спектра и повысить

* FHSS (frequency hopping spread spectrum) – система с широкополосными псевдослучайными сигналами и скачкообразной перестройкой частоты, система FHSS.

** SRD (short-range device) – беспроводные приборы ближнего радиуса действия, радиопередатчики, обеспечивающие одно- или двунаправленную связь и не создающие больших помех другим радиосистемам. Могут использоваться во многих областях, таких как дистанционный контроль автоматических устройств на производстве и в быту; беспроводные датчики; автомобильная электроника (бесконтактные замки, системы удаленного запуска и т.д.); системы сигнализации; беспроводное управление аудио- и видеотехникой.

Рис.3. Портативная система R&S® ARDRONIS-D фирмы Rohde & Schwarz, объединяющая функции обнаружения, классификации и геолокации. *Источник: Rohde & Schwarz*

возможность прерывания передачи сигнала радиоуправления БПЛА.

Для надежного обнаружения сигнала БПЛА большое значение имеет автоматическая классификация – от оператора трудно ожидать, что он сможет понять и оценить все сигналы во всех диапазонах частот одновременно. Простая система сигнализации на основе порога различимости радиосигнала, имеющаяся во многих основных системах мониторинга спектра, может привести к ложной тревоге при обнаружении этого порога. Автоматическая система классификации должна распознавать обстановку и быть способной находить систему передачи для классификации характерных признаков (сигнатур) ожидаемой угрозы по библиотеке известных сигналов дронов. Большим преимуществом радиочастотной системы обнаружения во время установления связи является минимальная длительность процесса установления связи, что улучшает ситуационную осведомленность.

Один из надежных методов автоматического обнаружения управляющего сигнала БПЛА – обнаружение относительно минимального уровня шума. Первоначально метод был разработан фирмой Keysight Technologies для ВЧ-диапазона (2–32 МГц). Его алгоритм содержит несколько переменных, относящихся к границам рабочего режима, сегментации и сглаживанию. При правильной настройке переменных автоматическое определение порога может "скакать" вверх и вниз по активным Wi-Fi-каналам, при этом правильно отклоняясь и выделяя управляющие сигналы БПЛА из фона других сигналов.

Специалисты Rohde & Schwarz, рассматривая ситуацию присутствия в наблюдаемом районе большого числа

Рис.4. Мобильный вариант системы Drone Detector. *Источник: Aaronia AG*

БПЛА, предположили возможные ситуации появления "дружественных" БПЛА (так называемый "белый лист"), осуществляющих мониторинг периметра, участвующих в полицейском расследовании или наблюдающих за скоплением людей. Знание индивидуальных идентификационных данных известных "дружественных" сигналов дает возможность оценить, где опасные БПЛА ("черный список") сосуществуют во времени и пространстве с БПЛА из "белого списка". В свою очередь это позволяет определить число возможных угроз в охраняемом районе.

ОДНОВРЕМЕННОЕ РАСПОЗНАВАНИЕ БПЛА РАЗЛИЧНЫХ ТИПОВ

Быстрая классификация сигналов в среде со многими угрозами – трудная задача, особенно с учетом сложности разделения сигнатур большого числа коммерческих БПЛА, использующих на одной и той же полосе частот технологии FHSS, WLAN и Bluetooth. Кроме того, в зоне защиты может оказаться любое число БПЛА, работающих на других частотах. Во время процесса классификации проблема не только в этом: не все технологии пеленгации одинаково способны реализовать геолокацию в окружающей среде с сигналами большого числа БПЛА. Это особенно верно по отношению к технологиям пеленгации, не способным различать на одной и той же частоте одновременно несколько сигналов, даже если они излучаются под разными углами.

Специалисты Rohde & Schwarz рекомендуют при выборе технологии пеленгования оценивать возможность системы не только определить географическое местоположение (геолокация) одновременно возникающих в одной и той же полосе частот угроз, но и функционировать на всей ожидаемой рабочей полосе частот. Важно, чтобы технологии, составляющие основу системы защиты, предоставляли пользователю информацию в максимально понятной форме, чтобы можно было выбрать оптимальные методы противодействия

угрозам. Не менее важно обеспечить обнаружение одновременного прибытия потенциальных угроз и "дружественных" БПЛА, угол вхождения в охраняемую зону и потенциальную траекторию движения.

Системы радиочастотного обнаружения играют большую роль в системах обороны от БПЛА. Однако существуют технологии БПЛА, способные работать на основе GPS или других GNSS*-технологий, вейпойнт**-системах, не излучающих радиочастотных сигнатур. В этом случае использование для защиты объектов высокой ценности (аэропортов, правительственных зданий, АЭС и т.д.) только системы радиочастотного обнаружения будет недостаточно.

При формировании комплексного решения необходимо рассмотреть другие технологии, дополняющие общее решение преимуществами и преодолевающие в рамках этого решения свои недостатки. При этом важно наличие открытого системного интерфейса, который при необходимости может "переставить" на руководящую позицию оборонной системы любую из используемых технологий. При организации передачи сигнала тревоги или оповещения на другие системы также необходимо рассмотреть визуальные или акустические методы, передачу SMS на заранее определенные группы мобильных телефонов, XML-сообщения через IP-сети.

Технологии БПЛА продолжают совершенствоваться, коммерческие приборы оснащаются новыми радиочастотными интерфейсами. В этих условиях при формировании оборонной системы важно использовать масштабируемый подход, позволяющий расширять возможности и включать в ее библиотеку новые радиочастотные сигнатуры по мере их появления. Постоянная бдительность в отношении новых радиоинтерфейсов и возможность наращивания системы защиты против новейших угроз – обязательные условия.

АКТИВНЫЕ И ПАССИВНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ БПЛА

Одним из примеров активной системы является **R&S® ARDRONIS** (рис.3), которая уже зарекомендовала себя в качестве приемлемой для обеспечения высоких уровней безопасности. Составляющие ее основу технологии уже использовались для защиты закрытых объектов от несанкционированного проникновения дистанционно управляемых БПЛА при проведении экономического саммита G7 в замке Эльмау (Германия) и во время посещения в 2016 году президентом США Б.Обамой Ганноверской промышленной ярмарки.

Данная автоматическая система – комплексное решение со специализированными возможностями обнаружения, классификации, определения географических координат, записи сигнатур и нарушения линии дистанционного управления БПЛА. В результате успешных испытаний с развертыванием у основных заказчиков, отвечающих за охрану важных и публичных мероприятий, а также VIP-персон, система R&S® ARDRONIS была признана эффективной с технической точки зрения.

Система R&S® ARDRONIS обеспечивает надежное обнаружение и наблюдение за активностью БПЛА, раннее предупреждение, ориентирование операторов по направлению поиска активных БПЛА и пультов дистанционного управления ими. То есть у спецслужб появляется возможность поимки злоумышленника с поличным. Соответственно, можно вовремя развернуть меры противодействия проникновению радиоуправляемых БПЛА в охраняемую зону за счет нарушения линии радиосвязи.

Недавно фирма Aaronia (Штрикшайд, Германия) представила пассивную систему **Drone Detector**, особенность которой состоит в возможности фиксации радиочастотного излучения, испускаемого бортовыми системами БПЛА (рис.4). Цель разработки – создание более надежного метода обнаружения небольших БПЛА злоумышленников. Возможности обнаружения РЧ-сигнала в реальном масштабе времени и методика запуска поиска, осуществляемого комбинацией сигналов, обеспечивают своевременное предупреждение о появлении в охраняемой области любых БПЛА или блоков управления ими.

Военные каналы связи в целях снижения возможности перехвата данных часто используют такие методики, как быстрая перестройка частоты. Однако разработчики БПЛА, выпускающие недорогие продукты, иногда снабжают свою продукцию сходными методиками. В результате линии связи БПЛА с аппаратной точки зрения являются дешевыми, простыми подсистемами, которые могут обеспечить скрытность (невидимость,

* GNSS (Global Navigation Satellite System) – глобальная система спутниковой навигации.

** waypoint system – вейпойнт-система, набор точек в 3D-среде с достижимостью установления связей между ними.

неопределяемость) аппарата. Однако для большей части гражданских БПЛА и их блоков управления характерна ограниченная дальность, а система Drone Detector обладает более сложными средствами приема и работает на большей дальности, чем операторы подобных БПЛА.

Система Drone Detector оснащена двумя 3D-антеннами радиопеленгации: IsoLOG 3D80 (8-секторная с 16 антеннами) и IsoLOG 3D160 (16-секторная с 32 антеннами). Обе покрывают частотный диапазон от 680 МГц до 6 ГГц. Кроме того, при использовании средств расширения они могут охватывать ОНЧ-, НЧ-, СЧ- и ВЧ-частоты (от 9 кГц до 680 МГц), а также диапазон 6–20 ГГц. Таким образом, покрываются все частоты, обычно используемые для дистанционного радиоуправления БПЛА. Система Drone Detector выпускается как в мобильном, так и в стационарном исполнении.

При помощи базовых компонентов пользователь может создать собственную конфигурацию необходимой сложности. Самый простой вариант состоит из одной IsoLOG 3D и мобильного или стационарного анализатора спектра. Этого достаточно для наблюдения местности в диаметре 8–10 км. Если требуется полностью мобильное решение, система может устанавливаться на транспортном средстве (работа от аккумулятора), включая водное, – антенны устойчивы к воздействию соленых брызг или водяной пыли.

При обнаружении сигнала его приблизительный пеленг показывается с точностью два-три градуса. Точность пеленга зависит от модели антенны. Стандартная антенна IsoLOG 3D80 обеспечивает точность пеленга как минимум четыре-шесть градусов на один сектор. В случае необходимости покрытия большей площади к одному централизованному ПК подключают несколько антенн и анализаторов спектра, которыми ПК будет управлять одновременно. Чем шире зона покрытия, тем больше антенн и анализаторов необходимо использовать. Любой сигнал угрозы, скорее всего, будет принят несколькими антеннами, благодаря чему результаты можно триангулировать, получив подробную и достоверную информацию о местоположении БПЛА и/или его оператора.

Поскольку система создана для распознавания радиосигналов, связанных с БПЛА, она не будет подавать тревожных сигналов в случае обнаружения радиосигналов другого типа. При появлении нескольких БПЛА система сможет обнаружить все независимо от того, одного они типа или разных.

Среднее время, необходимое для обнаружения БПЛА, составляет от 10 до 500 мс. Это зависит от таких факторов, как сложность разворачиваемой системы и число используемых антенн. В условиях прямой видимости между антеннами и БПЛА или его оператором достигаются лучшие результаты, при этом система может обнаруживать источник радиочастотных сигналов, загороженный деревьями, кустами, толпой людей и т.д. Система является пассивной, то есть не излучает собственных сигналов, способных помешать деятельности объектов (аэропортов и т.д.) или предупредить оператора БПЛА о своем присутствии. Производительность системы не зависит от темноты или плохой погоды – если метеоусловия позволяют БПЛА летать, то они будут обнаружены [1].

Итак, слабым местом БПЛА является уязвимость каналов связи. Сигналы GPS-навигаторов, как и любые сигналы, принимаемые и отсылаемые летательным аппаратом, можно глушить, перехватывать и подменять. Подобные методики позволяют перехватить БЛПА и посадить его в нужном месте. Так, несколько лет назад иранцам удалось перехватить и посадить сверхсекретный БПЛА RQ-170 Sentinel, изготовленный корпорацией Lockheed Martin с применением технологии Stealth по заказу ЦРУ США. Иран отказался отдать его и создал на его основе собственные аппараты [3].

В 2012 году учеными из Техасского университета (Остин, штат Техас) была доказана возможность взлома и перехвата управления БПЛА путем так называемого GPS-спуфинга, но только для тех аппаратов, которые используют незашифрованный гражданский сигнал GPS [4].

Соответственно, создание и применение систем перехвата управления и посадки/уничтожения гражданских БПЛА вещь вполне осуществимая. Работы в этом направлении активно ведутся примерно с 2010 года. Число стран, осуществляющих подобные разработки, превысило два десятка. Кстати, в Воздушный кодекс РФ 5 июля 2017 года были внесены поправки, предусматривающие обязательную регистрацию гражданских БПЛА в органах МВД [5].

ЛИТЕРАТУРА

1. **Patrick Hindle.** Drone Detection and Location Systems. Microwave Journal, June 14, 2017
2. Рынок беспилотных летательных аппаратов/дронов (БПЛА) в России и в мире. Октябрь 2016 г. http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-bespilotnyh-letatelnyh-apparatov-dronov-i-perspektivy-v-rossii-20161121111941
3. Иран отказался вернуть США сверхсекретный беспилотник https://lenta.ru/articles/2011/12/13/sentinel
4. Охота на беспилотников. Военные будут ловить БПЛА. newsrussia.today, 2 апреля 2017 г. https://newsrussia.today/tehnologii/6545-ohota-na-bespilotnikov-voennye-budut-lovit-bpla.html
5. В России вступила в силу обязательная регистрация беспилотников. РИА "Новости", 05.07.2017. https://ria.ru/economy/20170705/1497842595.html