Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/

Том 9, №1 (2017) http://naukovedenie.ru/vol9-1.php

URL статьи: http://naukovedenie.ru/PDF/13TVN117.pdf

Статья опубликована 20.02.2017

Ссылка для цитирования этой статьи:
Теодорович Н.Н., Строганова С.М., Абрамов П.С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №1 (2017) http://naukovedenie.ru/PDF/13TVN117.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 62

Теодорович Наталия Николаевна
ГБОУ ВО МО «Технологический университет», Россия, Королев[1]
Кандидат технических наук, доцент
E-mail: teonat@rambler.ru
РИНЦ: http://elibrary.ru/author_items.asp?id=518204

Строганова Светлана Михайловна
ГБОУ ВО МО «Технологический университет», Россия, Королев
Старший преподаватель
E-mail: sm306@yandex.ru
ORCID: http://orcid.org/0000-0001-6858-9403
РИНЦ: http://elibrary.ru/author_profile.asp?id=601806
Researcher ID: http://www.researcherid.com/rid/G-5953-2012

Абрамов Павел Сергеевич
ГБОУ ВО МО «Технологический университет», Россия, Королев
Студент
E-mail: abramovpavelr@gmail.com

Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами

Аннотация. В данной статье исследованы способы и методы противодействия беспилотным летательным аппаратам, а также изучены существующие технические решения стран мира и дана оценка их эффективности. Важность вопроса с возрастает с каждым годом в связи с распространением беспилотных летательных аппаратов в коммерции для доставки товаров и мирной жизни для сьемки больших групп людей, поэтому остро стоит вопрос об безопасности их использования. В связи с повышением спроса произошло снижение цен на составляющие, а также повышение распространенности программного обеспечения в свободном доступе, что облегчило деятельность по созданию «кустарных» аппаратов для военного применения террористическими группами. Также, в статье представлены тактики противодействию атакам с применением беспилотных летательных аппаратов и их реализации военными структурами и органами по охране общественного порядка. Анализ, которых выявил, что противодействие и контроль за развертыванием беспилотных летательных аппаратов внутри контролируемых территорий является наименее обеспеченной областью со стороны безопасности. В следствии было предложено усовершенствование системы

[1] 141070, Московская область, г. Королев, ул. Гагарина, 42

противодействия беспилотным летательным аппаратам путем использования современных систем РЭБ.

Ключевые слова: БПЛА; БЛА; дрон; беспилотник; РЭБ; РЭС; безопасность населения; FPV полёты

Беспилотные летательные аппараты (БПЛА) все больше находят широкое применение в нашей жизни. В частности, в сельском хозяйстве БПЛА с GPS-навигацией используются при опылении полей, чем достигается значительная экономия химикатов и более тщательная обработка посевов по сравнению с традиционной пилотируемой авиацией.

БПЛА используются для доставки медикаментов и гуманитарных грузов в труднодоступные районы. Они могут применяться для проверки линий электропередач и трубопроводов. МЧС использует дроны для мониторинга и прогнозирования чрезвычайных ситуаций и контроля за опасными объектами. Отслеживание пробок на дорогах и заторов на реках во время ледохода это малая часть того, что можно поручить беспилотникам.

К сожалению, технический прогресс в области беспилотной летательной техники имеет и обратную сторону - существует возможность использования БПЛА в террористических и разведывательных целях. В последние годы беспилотные летательные аппараты, или БПЛА, стали активно развивающимся направлением авиационной военной техники как в странах Запада, так и в нашей стране. Отсутствие экипажа, а значит и сложных систем жизнеобеспечения на борту, дает возможность БПЛА увеличивать дальность и длительность полёта и полезную нагрузку. Появление беспилотных аппаратов является общей тенденцией роботизации в вооруженных силах разных стран. БПЛА также становятся средством борьбы с международным терроризмом, что достаточно сильно меняет традиционные методы ведения войны.

Рассмотрим теперь более подробно методы противодействия беспилотным летательным аппаратам.

Под беспилотниками обычно понимают большие аппараты с ракетным вооружением. Однако даже самодельный дрон, собранный из находящихся в свободной продаже комплектующих, вполне может быть эффективно использоваться в качестве оружия. Следует отметить, что в некоторых случаях атака небольшого беспилотного аппарата с воздуха гораздо эффективнее любых других способов нападения. Малые размеры позволяют оставаться незаметным, а эффект неожиданности делает атаку дрона, начиненного, например, пластидом и металлическими шариками разрушительной. В данном случае традиционные меры безопасности совершенно бесполезны.

Беспилотные летательные аппараты (БПЛА, БЛА или, в зарубежной литературе, «дроны») стали частью нашей жизни сравнительно недавно. Оборудованные камерами, они используются как необычный способ съемки: ими снимают с воздуха мероприятия, и летают в качестве простого развлечения (FPV полёты). Рынок чутко отреагировал на появление спроса и в свободном доступе появились недорогие радиоуправляемые модели как самолетов, так и вертолетов с изначально встроенной камерой. Появилось целое FPV-движение, которое породило целую индустрию оборудования, которое предназначено облегчить управление авиамоделью вне прямой видимости [10]. Сюда можно отнести компактные видеокамеры с высоким качеством изображения, мощные передатчики, которые могут в том числе обеспечить передачу видеоряд на расстояние до сотни километров, а также автопилоты, обеспечивающие возвращение БЛА в заданную точку или движение по сложному маршруту.

Признанным лидером в производстве FPV-оборудования является Китай. Не отстают от него США, Австралия и Россия, где уверенно выходят на мировой рынок компании, с собственными разработками [8].

Многие компании, занимающиеся доставкой товаров, намериваются осуществлять ее с помощью беспилотников. Amazon уже проводит испытания новой системы доставки дронами в Канаде, Великобритании и Нидерландах. Единственное, что их пока ограничивает - это законы, запрещающие полёты не сертифицированных летательных аппаратов и беспилотников над крупными населенными пунктами, но компании обещают преодолеть это препятствие к 2018 году.

И в связи с подобным массовым распространением дронов многие структуры, обеспечивающие безопасность своих стран, стали разрабатывать новые технологии противодействия им. Ниже представлены методы и способы нейтрализации беспилотников:

- Акустические
- Лазерные
- Микроволновые
- Сети
- Противодроны
- Системы РЭБ
- Системы перехвата управления беспилотных летательных аппаратов

Одним из недостатков у дронов является конструктивная уязвимость гироскопов. Без этого устройства не обходится практически ни одни дрон - без него невозможен устойчивый полет, и оно отвечает за изменения в пространственной ориентации. Гироскоп, как механическая система имеет резонансную частоту, если ее подобрать, то устройство войдет в резонанс и будет выдавать неверные показания, которые приведут к аварии. [1]

Гироскопы имеют различные конструкции, соответственно у них и различные резонансные частоты, находящиеся в очень широких пределах от слышимого диапазона волн до ультразвука. После проверки исследователями пятнадцати наиболее популярных типов гироскопов, которые применяются в хобби-дронах было выявлено, что семь из них имеют уязвимость к акустической атаке. Эксперимент проводился в тестовой камере и показал, что в каждом случае достаточно десяти секунд, чтобы вывести дрон из строя. По расчетам ученых атака мощностью 140 дБ вполне достаточна, чтобы сбивать дрон на расстояниях до сорока метров.

Однако не все гироскопы идентичны, в некоторых из-за конструктивных особенностей резонанс перекрывает только канал ориентации относительно горизонтальной оси и этого может быть недостаточно для аварии дрона, так как обычно в БЛА используется также магнитометр, который может обеспечить ориентацию по горизонтали.

ВМФ США проводят испытания маломощной лазерной системы, которая способна обнаруживать, отслеживать и уничтожать движущиеся воздушные цели на поле боя. Система разработана компанией Boeing и способна уничтожать приближающиеся к кораблю дроны, артиллерийские снаряды и небольшие низколетящие самолеты. Такие системы принято называть LWS (Laser Weapon System), это одна из самых компактных систем лазерной защиты из числа разрабатываемых в настоящее время, что обеспечивает ей высокую мобильность. Лазер способен обнаруживать цели на расстоянии до 35 км, эффективная зона поражения радиусом до 1.6 км [2].

Основой системы является твердотельный лазер, который работает в инфракрасном диапазоне. Может работать в низкоэнергетическом режиме для выведения из строя сенсоров цели, либо в высокоэнергетическом для уничтожения цели. Мощность до 30 кВт. Время уничтожения цели - порядка 2 секунд.

В отличие от лазерных противодронных систем, которые разрушают дрон механически, за счет его сильного дистанционного нагрева, микроволновые системы, дистанционно формирующие в электрических цепях наведенные токи, способны уничтожать целые группы дронов без необходимости перенаправлять фокус излучателя на каждое устройство в “рое” [3]. Данная технология давно используется для уничтожения техники и реализована в большинстве стран с развитым военным вооружениям.

Выше перечисленные способы борьбы нацелены на уничтожение дрона, что вызывает осложнение если груз, который он содержит, может нанести ущерб при падении или уничтожении в воздухе, а также при необходимости перехвата содержимого.

Сети являются простым, но достаточно эффективным способом противодействия на низкой высоте. Выстреливаемые в сторону дрона или быстро поднимаемые по курсу следования дрона сети. Сети также могут переноситься так называемыми противодронами.

Английская компания OpenWorks Engineering представила систему SkyWall 100 - одну из последних разработок в области противодействия дронам. Устройство представляет собой “умный гранатомет”, выстреливающий в сторону беспилотника сеть. Радиус эффективного действия устройства - до 100 метров. Разработанное устройство захватывает цель и помогает оператору навести на неё метательное устройство с помощью системы наведения, которая оценивает расстояние и вектор движения дрона. Сеть с захваченным дроном затем опускается на парашюте [4]. Существует также более дальнобойная система SkyWall 200, которая требует установку на специальной треноге. Существует и SkyWall 300 - дистанционно управляемая стационарная турель.

Силовые структуры, а также полиция могут использовать дроны/противодроны, оснащенные и более мощными дизельными. Такие модели отличаются более высокой защитой корпуса и в них предусмотрены устройства защиты от атак других дронов, находящихся, например, над территорией, где запрещены полеты или нелегально запущенных. Существуют дроны-перехватчики. Они могут автоматически наводиться, реагируя на шум двигателей преследуемого дрона или ориентироваться по заложенному в памяти изображению системы "компьютерного зрения" дрона-перехватчика. Дрон-перехватчик может быть оснащен сетью для обезвреживания дрона-нарушителя, как это было применено в Японии [5].

Сейчас на вооружении многих армий имеется большое количество разнообразных систем радиоэлектронной борьбы (РЭБ). Как уже говорилось ранее, для успешного выведения из строя вражеского дрона требуется установить частоты, на которых производится управление аппаратом, а затем «забить» их помехами. Далеко не все современные беспилотные летательные аппараты имеют на борту автоматику, способную перехватить управление в случае потери или нарушения сигнала от оператора. Также следует отметить и другой момент: при потере связи с оператором становится невозможной и передача разведывательной информации с видеокамер БПЛА. В дальнейшем оставшийся без управления дрон может быть уничтожен стороной, осуществивший перехват, что на самом деле не является сложной задачей. Или трофейный БПЛА может быть использован для каких-то других нужд - его судьба полностью в руках перехватчика.

В некоторых дронах предусмотрен вариант обрыва связи с оператором. В этом случае, если канал связи потерян, дрон переходит в соответствующий режим работы - автоматика перестает реагировать на все сигналы извне и согласно заданной программе ведет БПЛА к

заранее определенному месту посадки, используя систему GPS или ГЛОНАСС. Аппарат использует спутниковую навигацию и определяет свое местоположение, направление движение, расстояние до оператора или точки посадки, чтобы иметь возможность вернуться на базу.

Чтобы не допустить «эвакуацию» дрона, средства радиоэлектронной борьбы должны подавлять не только канал управления, но и сигналы навигационной системы. В результате успешного «глушения» всех этих сигналов противник, с высокой вероятностью, лишится техники, попавшей в зону действия РЭБ.

Стоит выделить возрастающий спектр средств мобильных РЭБ, которые порой называют “кибервинтовками”. И не смотря на простоту и относительную дешевизну по сравнению со станциями РЭБ у нее есть весьма существенный недостаток - она использует возможность передачи сигналов на частоте канала управления беспилотника. Так можно вывести из строя лишь некоторые модели дронов, а не любой существующий аппарат. Автономным беспилотникам, не получающим какой-либо сигнал извне, такая система не угрожает.

Системы перехвата управления беспилотных летательных аппаратов обычно дополняют системы РЭБ или являются самостоятельными комплексами, развернутыми на определенных областях города.

Среди основных способов взлома БПЛА можно перечислить следующие:

1. Взлом шифрованного канала или подмена данных авторизации и получение за счет этого доступа к управлению дроном.
2. Использование уязвимостей программного обеспечения, в том числе переполнение буфера.
3. Использование интерфейсов и каналов данных оригинального программного обеспечения для "протаскивания" стороннего кода.

Дорогостоящие БПЛА, используемые полицией или иными государственными структурами, службами МЧС и отдельными компаниями в частном секторе, достаточно просто взломать и угнать.

Существуют всего две основные уязвимости, благодаря которым возможен угон БПЛА [6]:

- Для связи по Wi-Fi между модулем контроля беспилотного аппарата и устройством управления как правило используется очень слабое шифрование, так как известно, что WEP (Wired Equivalent Privacy) можно взломать за несколько секунд. Причем атакующий может достаточно просто внедриться в соединение между дроном и оператором, находясь на расстоянии порядка ста метров, и послать БПЛА ложную команду или отключить его от исходной сети.

Чип Xbee, который используется многими моделями дронов, небезопасен. Несмотря на то, что Xbee поддерживает шифрование, но из-за проблем с производительностью и для исключения задержек между командами оператора и реакцией БПЛА, оно просто отключено. Вследствие чего злоумышленник имеет возможность осуществить атаку man-in-the-middle, находясь на расстоянии двух километров от дрона. Атакующий может перенаправить пакеты, заблокировать настоящего оператора, или пропускать все пакеты через себя, но большинство атакующих предпочитают похищение дронов.

Подводя итог применяемым методам и способам противодействия, можно дать достаточно высокую оценку существующей в России возможности противостоять дронам.

Стоит выделить мобильные РЭБ «Автобаза» и «Красуха», которые уже несколько лет успешно используются в военной сфере. Существующие разработки позволяют создавать зоны, недоступные для современных управляемых дронов, используя системы подавления и перехвата вокруг них [7], но существует опасность развертывания устройства непосредственно в самой зоне [9].

Однако все еще остро стоит вопрос в области защиты граждан в связи с массовым распространением дронов, которые часто применяют для сьемки больших групп людей во время мероприятий. Поэтому вопрос об отслеживании БПЛА и контролем за разрешенной для них деятельностью на сегодняшний момент остается одним из самых актуальных.

ЛИТЕРАТУРА

1. Дроны: Еще один способ сбивать дроны - акустический удар! Электронный ресурс. Режим доступа: http://www.mforum.ru/news/article/113554.htm (дата обращения: 21.11.2016).
2. US Marines Test Boeing Laser To Knock Down Drones, Enemy Artillery. Электронный ресурс. Режим доступа: http://www.ibtimes.com/us-marines-test-boeing-laser-knock-down-drones-enemy-artillery-2011610?ft=h6k97 (дата обращения: 21.11.2016).
3. The Army's Real-Life "Phaser" Would Knock Out an Entire Drone Swarm With One Shot. Электронный ресурс. Режим доступа: http://www.popularmechanics.com/military/weapons/a23881/the-army-is-testing-a-real-life-phaser-weapon/ (дата обращения: 21.11.2016).
4. Tokyo's solution to rogue drones? Drones with nets. Электронный ресурс. Режим доступа: https://www.engadget.com/2015/12/11/tokyo-drone-net/ (дата обращения: 21.11.2016).
5. The SkyWall 100 bazooka captures drones with a giant net. Электронный ресурс. Режим доступа: http://techcrunch.com/2016/03/04/the-skywall-100-bazooka-captures-drones-with-a-giant-net/ (дата обращения: 21.11.2016).
6. Исследователь показал, как взломать полицейских дронов, имея аппаратуру за $40. Электронный ресурс. Режим доступа: https://xakep.ru/2016/04/05/uav-flaws/ (дата обращения: 21.11.2016).
7. Apolloshield web-site http://www.apolloshield.com/ (дата обращения: 21.11.2016)
8. Атакующие БПЛА и системы противодействия им, обзор Электронный ресурс. Режим доступа: http://savepearlharbor.com/?m=201506&paged=339 (дата обращения: 21.11.2016).
9. Результаты конференции «Индустрия беспилотных авиационных систем». Электронный ресурс. Режим доступа: http://www.helirussia.ru/ru/dlya_smi/press_relizyi/2016/05/31/uas_conference_results/339 (дата обращения: 21.11.2016).
10. БЕСПИЛОТНИКИ: ЧТО ЖДЕТ НОВУЮ ОТРАСЛЬ В РОССИИ Электронный ресурс. Режим доступа: http://www.aviaport.ru/digest/2016/05/24/387099.html (дата обращения: 21.11.2016).

Teodorovich Nanalia Nikolaevna
University of technology, Russia, Korolyov
E-mail: teonat@rambler.ru

Stroganova Svetlana Mikhaylovna
University of technology, Russia, Korolyov
E-mail: sm306@yandex.ru

Abramov Pavel Sergeevich
University of technology, Russia, Korolyov
E-mail: abramovpavelr@gmail.com

Methods for detection and control of small-sized unmanned aerial vehicles

Abstract. This article investigates the techniques and methods to counter unmanned aerial vehicles, and explored existing technical solutions around the world and assesses their effectiveness. The importance of the issue to the increasing every year due to the spread of unmanned aerial vehicles in commerce to deliver the goods, and a peaceful life for filming large groups of people, so sharply is the question of the safety of their use. In connection with the increasing demand occurred on the components price reductions, and increasing distribution of the software in the public domain that easier work on the creation of "handicraft" devices for military use by terrorist groups. In addition, the article presents tactics to counter the attacks with unmanned aerial vehicles and their implementation by military structures and local police. Analysis of which are founded that counteracting and control over the deployment of unmanned aerial vehicles in controlled areas is the poorest area of the security. The result was the proposed improvement of the system to counter unmanned aerial vehicles with using of electronic warfare systems.

Keywords: UAV; drone; EW; ECM; public safety; First Person View