УДК 004.056.53
DOI: 10.33764/2618-981X-2020-6-1-149-154

МЕТОДЫ И СРЕДСТВА ПРОТИВОДЕЙСТВИЯ АКУСТИЧЕСКОЙ И ОПТИЧЕСКОЙ РАЗВЕДКЕ, ПРОИЗВОДИМОЙ С ПОМОЩЬЮ КВАДРОКОПТЕРОВ

Никита Вадимович Игнатенко
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (906)994-60-92, e-mail: nikannor2010@yandex.ru

Алексей Николаевич Поликанин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (913)397-63-51, e-mail: polikanin.an@yandex.ru

В последние несколько лет простота покупки и использования беспилотных летательных аппаратов (БПЛА), их доступная стоимость увеличили спрос на них как компаний, так и частных лиц. Однако эти устройства несут в себе возможность реализации противоправных действий, начиная с контрабанды незаконных веществ, несанкционированной разведки, заканчивая компьютерными атаками. Как следствие, это привело к актуальности разработки эффективных и доступных контрмер для обнаружения и возможной нейтрализации беспилотников, совершающих разведку на объектах с конфиденциальной информацией. Наиболее успешно зарекомендовали себя автономные системы обнаружения и подавления дронов, включающие в себя оптико-электронные, акустические радиолокационные и радиочастотные датчики, информация с которых объединяется на главном компьютере для идентификации угрозы и принятия дальнейших решений. Тем не менее, наблюдение в режиме реального времени является довольно тяжелым процессом, требующем своевременного обнаружения неблагоприятных событий или условий. В связи с чем возникает много сложных задач, таких как обнаружение объектов, классификация, отслеживание нескольких объектов и объединение информации с нескольких датчиков. В последние годы исследователи использовали различные методики для решения этих задач и добились заметного прогресса. Применение глубокого обучения для обнаружения и классификации БПЛА считается новой концепцией. В связи с этим возникла необходимость представить обобщенный обзор технологий борьбы с БПЛА, используемых для разведки, что и является целью данной статьи.

Ключевые слова: глубокое обучение, БПЛА, идентификация, датчики, безопасность, разведка.

METHODS AND MEANS OF COUNTERACTION OF ACOUSTIC AND OPTICAL RECONNAISSANCE UAV

Nikita V. Ignatenko
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (906)994-60-92, e-mail: nikannor2010@yandex.ru

Alexey N. Polikanin
Siberian State University of Geosystems and Technologies 10, Plahotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (913)397-63-51, e-mail: polikanin.an@yandex.ru

For the last few years, the ease of purchasing and using unmanned aerial vehicles (UAVs), their affordable cost has increased the demand for them both by companies and individuals. However, these devices might carry out illegal actions, starting with smuggling of illegal goods, unauthorized intelligence and computer attacks. As a result, this led to the urgency of developing effective and available countermeasures to detect and neutralize drones that perform reconnaissance of objects with confidential information. The most successful are autonomous systems for detecting and suppressing drones, which include optoelectronic, acoustic radar and radio frequency sensors, information from which is combined on the main computer to identify the threat and make further decisions. However, real-time monitoring is a rather difficult process that requires timely detection of adverse events or conditions. This creates many complex tasks such as object detection, classification, tracking multiple objects, and combining information from multiple sensors. In recent years, researchers have used various techniques to solve these problems and made notable progress. Applying deep learning to detect and classify UAVs is considered a new concept. In this regard, it became necessary to provide a generalized overview of UAV control technologies used for reconnaissance.

Key words: deep learning, UAVs, identification, sensors, security, reconnaissance.

Введение

Произведя анализ методов и средств противодействия БПЛА, их условно можно разделить на следующие группы:

- акустические;
- лазерные;
- микроволновые;
- сети;
- противодроны;
- системы радио-электронной борьбы (РЭБ);
- системы перехвата управления беспилотных летательных аппаратов;
- средства обнаружения и идентификации [1].

Методы и средства противодействия БПЛА

«Акустическая атака» - недавно открытый способ для борьбы с БПЛА, основанный на уязвимости гироскопа, который входит в состав многих из них [2]. Это устройство необходимо для того, чтобы дрон ощущал изменения в наклоне и ориентации в пространстве. У гироскопа, как практически у любой механической системы, есть резонансная частота. Стоит ее подобрать, гироскоп войдет в резонанс и начнет выдавать показания, которые, как показали эксперименты, приводят к аварии дрона. В проведенных экспериментах происходили исследования воздействия звука на дроны в тестовой камере. Атаки в течение 10 секунд во всех случаях хватало, чтобы сбить дрон. Атака мощностью 140 дБ достаточна, чтобы сбивать дрон на расстояниях до 40 метров.

Лазерная противодронная система. Система обычно состоит из лазерной установки и мультиспектральной системы наведения [3]. Питание устройств 220 В, кроме того, есть батареи, которых хватает на несколько десятков выстрелов на расстояние до 4 км.

Микроволновая установка. Состоит из мощного СВЧ излучателя и радара для определения противника. Установка выдает импульс СВЧ излучения, который повреждает бортовую систему управления БПЛА. В отличие от лазерных противодронных систем, которые разрушают дрон механически, за счет его сильного дистанционного нагрева, микроволновая установка, дистанционно формирующая в электрических цепях наведенные токи, способна уничтожать целые группы БПЛА без необходимости перенаправлять фокус излучателя на каждое устройство в отдельности.

Сети являются простым, но достаточно эффективным способом противодействия на низкой высоте. Их достаточно выстреливать в сторону дрона или быстро поднимать по курсу его движения. Сети также могут переноситься так называемыми противодронами [4].

Противодроны. Полиция и другие силовые структуры могут использовать дроны, оснащенные более мощными двигателями, например, дизельными, с более защищенным корпусом и устройствами для разрушения других дронов, например, незаконно запущенных или находящихся на запретных для полетов территориях. Дроны-перехватчики могут автоматически наводиться, например, по шуму двигателей преследуемого дрона или по его изображению в системе "компьютерного зрения" дрона-перехватчика. Дрон-перехватчик может, например, нести сеть для поимки дрона-нарушителя [5].

Среди разрабатываемых безопасных способов противодействия можно выделить следующие: постановка радиопомех, в том числе, против GPS/Глонасс приёмников; ослепление камер инфракрасными прожекторами; создание мощных воздушных вихревых завес вдоль периметра территорий, в том числе «умных завес», включаемых внезапно по сигналам с датчиков и создающих направленный вихрь с целью опрокинуть и разбить нарушивший границы БПЛА; установка защитных сетей, даже создание специальных БПЛА для борьбы с дронами, например, путём сброса сетей на вражеский дрон.

Останавливаясь более подробно на средствах радио-электронной борьбы, можно отметить подавители спутниковых сигналов, которые обычно воздействуют на один (*L1*) или сразу три (*L1-L3*) частотных диапазона GPS. Разработаны и более дорогие модели, способные противодействовать всем существующим навигационным системам (GPS, ГЛОНАСС, Galileo и т.д.). Стоит учесть, что приемники большинства оснащенных системой GPS современных малоразмерных дронов работают только в диапазоне *L1*.

Второй вид блокираторов засоряет помехами каналы связи дрона с пультом управления. Оператор теряет контроль над летательным аппаратом, а на экране его монитора полностью пропадает изображение. Дальнейшее поведение БПЛА зависит от алгоритма, заложенного в его программное обеспечение. Дрон либо приземляется, либо пытается вернуться в исходную точку. В обоих случаях его миссия прерывается, а охраняемый объект остается неприступным. Стандартная дальность действия таких приборов постановщиков помех достигает 500 – 600 метров, самые мощные из них поражают цель на удалении до 3-х километров. Они могут использовать как направленные, так и всенаправленные антенны [6].

Перехват управления беспилотником.

Выделяют следующие основные способы взлома беспилотников:

1) получение доступа к управлению за счет взлома шифрованного канала связи или подмены данных авторизации;

2) использование уязвимостей ПО, включая переполнение буфера;

3) использование интерфейсов и каналов данных оригинального ПО для «протаскивания» стороннего кода [7].

Система глубокого обучения

Ещё одним важным аспектом борьбы с БПЛА является его своевременное обнаружение и распознавание. Для этих целей применяется конструкция, состоящая из статической широкоугольной камеры на платформе и вращающейся башни, где установлена узкоугольная камера (рис. 1) (получено из открытых источников интернета) [8]. Статическая широкоугольная камера служит в качестве основного средства обнаружения воздушных объектов, с помощью которого беспилотные летательные аппараты могут быть обнаружены на относительно большом расстоянии (до одного километра) при размере изображения в несколько десятков пикселей Идентификация и визуальные признаки проверяются узкоугольной камерой на вращающейся башне

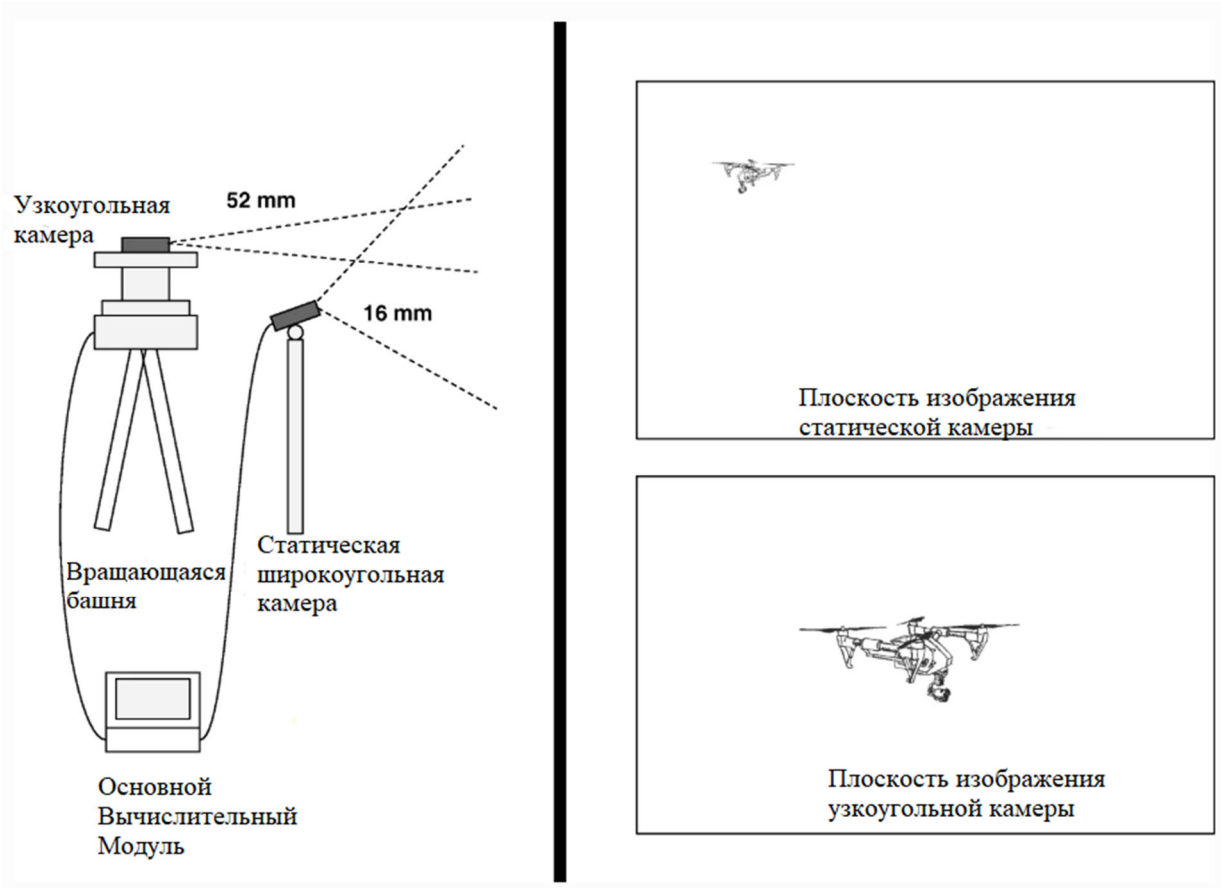

Рис. 2. Система обнаружения БПЛА [8]

В качестве программного обеспечения для обнаружения возможных дронов используется упрощенная версия алгоритма глубокого обучения YOLO, который в последнее время стал популярным вариантом, благодаря своей надежности и быстродействию [9]. Это упрощенная структура активно обучена обнаруживать дроны с размером изображения 6×6 пикселей. Для обучения алгоритма использовался расширенный массив данных (около 10 000 изображений).

При этом используется метод представления, при котором кадры узкоугольной камеры накладываются на кадр широкоугольной камеры. Таким образом, обнаружение и идентификация может выполняться одновременно (рис. 2) (получено из открытых источников интернета). Это позволяет непрерывно отслеживать воздушные объекты на плоскости основного изображения, в то время как система может идентифицировать возможные угрозы с помощью камеры вращающейся башни.

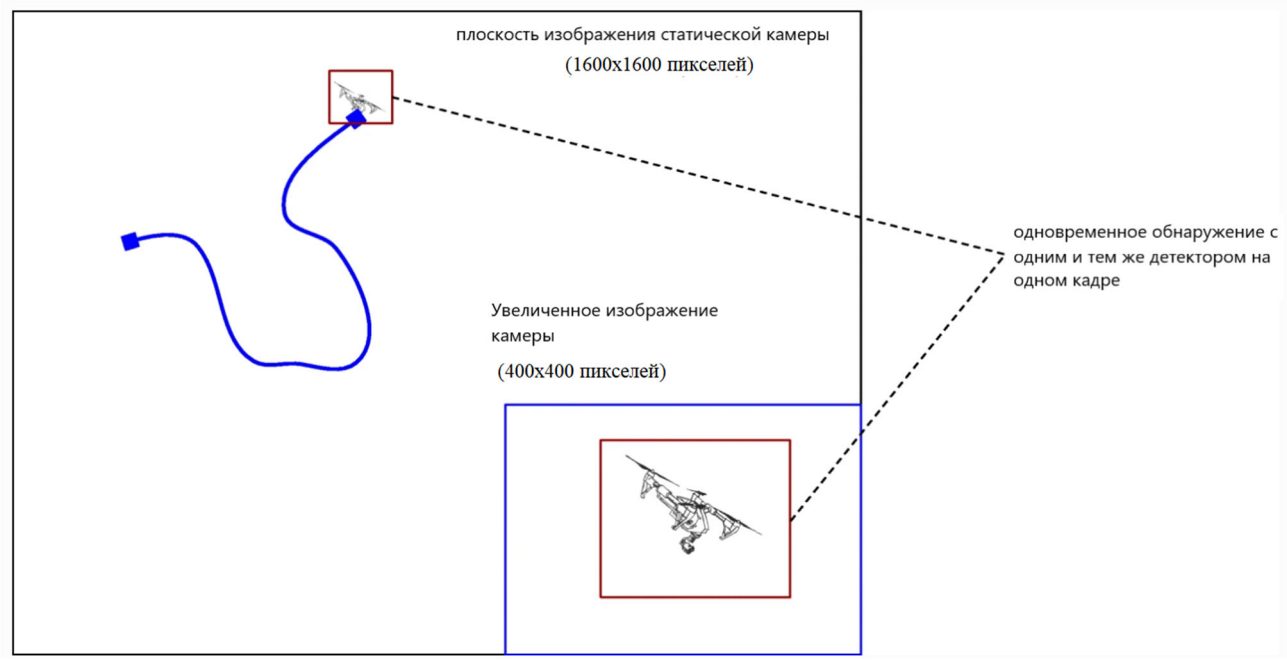

Рис. 3. Метод обнаружения и идентификации объектов [8]

Широкоугольная камера имеет объектив с фокусным расстоянием 16 мм, которое соответствует приблизительно 110 градусам поля зрения. Камера на вращающейся башне имеет объектив с фокусным расстоянием 300 мм и полем зрения 8,2 градусов. Длиннофокусная камера имеет возможность масштабирования в 35$^{\times}$, давая возможность обнаружить небольшие беспилотные летательные аппараты и иметь возможность идентифицировать их на большом расстоянии.

Алгоритм распознавания обнаруживает движение мелких объектов. Далее их перемещение и визуальные сигнатуры могут быть проверены путем поворота башни в их направлении и проанализированы с помощью длиннофокусной камеры. Программное обеспечение использует python в качестве основного языка

программирования, благодаря его универсальности и высокой производительности. Алгоритмы глубокого обучения для обнаружения и классификации основаны на архитектуре darknet (нейросеть с открытым исходным кодом) YOLO, которая написана на языке Си, но может быть интегрирована в python [10].

Заключение

Таким образом современные средства борьбы с БПЛА включают в себя не только способы их разрушения и подавления, но и высокоинтеллектуальные средства обнаружения и идентификации.

Из всего вышеперечисленного можно сделать вывод, что лучшим решением в борьбе с разведкой с использованием беспилотников будет сочетание вышеуказанных технологий. Эффективность этой системы будет зависеть от конкретных условий использования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Теодорович, Н. Н., Строганова, С. В., Абрамов, П. С. Способы обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами [Электронный ресурс]. – Режим доступа: https://russiandrone.ru/publications/ sposoby-obnaruzheniya-i-borby-s-malogabaritnymi-bespilotnymi-letatelnymi-apparatami (дата обращения: 01.04.2020).
2. Дроны: Еще один способ сбивать дроны - акустический удар [Электронный ресурс]. – Режим доступа: http://www.mforum.ru/news/article/113554.htm (дата обращения: 01.04.2020).
3. Реальный армейский «Фазер» одним выстрелом выбил бы целый рой дронов [Электронный ресурс]. – Режим доступа: https://www.popularmechanics.com/military/weapons/a2388-1/the-army-is-testing-a-real-life-phaser-weapon (дата обращения: 03.04.2020).
4. How To Defend Your Home And Your Family From Drone Attacks [Electronic resource]. – Mode of access: https://survivallife.com/drone-defense/ (дата обращения 26.03.2020).
5. О борьбе с беспилотными летательными аппаратами [Электронный ресурс]. – Режим доступа: https://topwar.ru/98134-o-borbe-s-bespilotnymi-letatelnymi-apparatami.html (дата обращения: 08.03.2020).
6. What can you do to protect yourself from a drone attack? [Electronic resource]. – Mode of access: https://www.quora.com/What-can-you-do-to-protect-yourself-from-a-drone-attack (дата обращения 20.04.2020).
7. Современные методы борьбы с квадркоптерами [Электронный ресурс]. – Режим доступа: https://zen.yandex.ru/media/rc_plane/sovremennye-metody-borby-s-kvadrkopterami-5df9322b3d5f69615a99b272 (дата обращения: 12.02.2020).
8. Deep learning-based strategies for the detection and tracking of drones using several cameras [Electronic resource]. – Mode of access: https://link.springer.com/article/10.1186/s41074-019-0059-x (дата обращения: 08.03.2020).
9. Deep Learning on Multi Sensor Data for Counter UAV Applications—A Systematic Review [Electronic resource]. – Mode of access: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6891421 (дата обращения: 03.04.2020).
10. How to protect yourself when drones go rogue [Electronic resource]. – Mode of access: https://www.gearbrain.com/drone-deterrent-defend-protect-privacy-2493022072.html (дата обращения 25.02.2020).