УДК 004.052
DOI 10.33764/2618-981X-2022-6-39-46

Исследование средств противодействия оптическим каналам утечки информации с использованием беспилотных летательных аппаратов

А. С. Грехов[1]*, *А. Н. Поликанин*[1], *Д. Н. Титов*[1]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: grehov084@gmail.com

Аннотация. В статье приведен краткий обзор систем обнаружения и противодействия беспилотным летательным аппаратам (БПЛА), которые могут быть использованы, в том числе, для перехвата информации по оптическому каналу. В настоящее время малые БПЛА широко используются для несанкционированного наблюдения важных объектов, проведения терактов и диверсий, переноски запрещенных грузов, а также в военном деле. В связи с этим актуализировалась задача противодействия БПЛА, в особенности – малым БПЛА. Проблема противодействия БПЛА, в частности, малым БПЛА, является многогранной и до сих пор эффективно не решенной. Анализ публикаций показывает, что аналитических статей в этой области довольно мало, в особенности в русскоязычном сегменте. В большинстве работ преобладают излишне оптимистичные выводы относительно эффективности противодействия БПЛА существующими средствами. Целью работы является исследование и обзор систем противодействия и подавления БПЛА, а также оценка расстояния, с которого возможно распознать информацию различного характера. В статье представлены результаты анализа различных систем противодействия и подавления БПЛА. Анализ источников позволил выявить основные принципы работы систем противодействия БПЛА. На сегодняшний день в российском сегменте рынка представлены достаточно эффективные системы противодействия, которые позволяют вести борьбу с БПЛА без ущерба инфраструктуре защищаемого объекта. Также в ходе исследований были проведены теоретические расчеты дальности распознавания текста и лица человека с использованием камеры, которая может быть установлена на мини-БПЛА.

Ключевые слова: беспилотный летательный аппарат, противодействие БПЛА, подавление БПЛА, малые БПЛА

Investigation of means of counteracting optical channels of information leakage using UAVs

A. S. Grehov[1]*, *A. N. Polikanin*[1], *D. N. Titov*[1]
[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: grehov084@gmail.com

Abstract. The article provides a brief overview of systems for detecting and countering unmanned aerial vehicles (UAVs), which can be used, among other things, to intercept information via an optical channel. Currently, small UAVs are widely used for unauthorized surveillance of important objects, carrying out terrorist attacks and sabotage, carrying prohibited goods, as well as in military affairs. In this regard, the task of countering UAVs, especially small UAVs, has been updated. The problem of countering UAVs, in particular, small UAVs, is multifaceted and has not yet been effectively resolved. An analysis of publications shows that there are quite a few analytical articles in this area, especially in the Russian-speaking segment. Most of the works are dominated by overly optimistic

conclusions regarding the effectiveness of countering UAVs with existing means. Objective. Research and review of systems for countering and suppressing UAVs, as well as an assessment of the distance from which it is possible to recognize information of a different nature. Results. The article presents the results of the analysis of various systems for countering and suppressing unmanned aerial vehicles. Analysis of the sources made it possible to identify the basic principles of operation of UAV countermeasure systems. To date, the Russian segment of the market has quite effective countermeasure systems that allow combating UAVs without damaging the infrastructure of the protected facility. Also in the course of the research, theoretical calculations were made of the range of recognition of text and a person's face using a camera that can be installed on a mini-UAV.

Keywords: unmanned aerial vehicle, UAV countermeasures, UAV suppression, small UAVs

Введение

Происходившие на протяжении всей новейшей истории промышленные революции стали причиной стремительного научно-технического прогресса во всех областях человеческой деятельности, в том числе, в области разработки и применения летательных аппаратов, в частности беспилотных.

В настоящее время доступ к беспилотным летательным аппаратам (БПЛА) имеет большое число людей, что представляет опасность с точки зрения защиты информации от утечки по оптическому и акустическому каналам, также под угрозой оказывается сфера компьютерной безопасности.

Малые БПЛА активно применяются для незаконного наблюдения за значимыми объектами, проведения террористических актов и диверсий, переноски запрещенных грузов. В связи с этим стала как никогда актуальна задача противодействия БПЛА, в особенности – малоразмерным. Анализ публикаций показывает, что аналитических статей в этой области довольно мало, в особенности в русскоязычном сегменте. В большинстве работ преобладают излишне оптимистические выводы относительно эффективности противодействия БПЛА существующими средствами [3]. Целью работы является исследование и обзор систем противодействия и подавления беспилотных летательных аппаратов, а также оценка расстояния, с которого возможно распознать информацию различного характера.

Методы и средства обнаружения

В настоящее время известны различные системы и комплексы обнаружения БПЛА. Они работают на разных физических принципах. Акустические контролируют полосу звуковых частот, характерных для дронов. Радиочастотные анализируют радиоволновые сигналы в диапазонах частот, используемых для управления дроном. Такие устройства имеют более высокую дальность действия. Однако таким устройствам достаточно сложно определить направление, с которого направляется БПЛА [6].

Специально для подавления работы БПЛА на объектах гражданского назначения в НПП «Алмаз» холдинга «Росэлектроника» разработан комплекс «Атака-DBS». Данное оборудование не требует лицензии для приобретения. Особенностью комплекса является способность работать избирательно, не влияя на работу штатных БПЛА и окружающих систем GPS – навигации и связи, что дает воз-

можность использовать комплекс в городских условиях, на территории аэропортов и других технологических сложных объектах [4].

Комплекс обнаруживает БПЛА, блокирует его канал связи и спутниковую навигацию. БПЛА теряет управление и либо возвращается в исходную точку, либо совершает посадку в аварийном режиме. Владелец комплекса будет оповещен о зафиксированной атаке посредством sms-сообщения или электронной почты.

Более совершенные комплексы работают на основе технологии ближней радиолокации. Использование данной технологии позволяет получить полную информацию о передвижениях отслеживаемого объекта: место обнаружения, траекторию движения, скорость, габаритные размеры. Возможна фиксация кадров видеонаблюдения, в том случае, если имеется дополнительная поворотная платформа с видеокамерой или тепловизором. Основные разработки подобных продвинутых решений использования радиолокаторов для обнаружения и борьбы с дронами проводятся в Израиле (MAGOS), США (ICX Technologies Inc., Rockwell Collins), Европе (Prime Consulting and Technologies) и в РФ («ЕНОТ», «Радескан-Антидрон», «Купол-М»).

Радиолокационные антидроны имеют ряд преимуществ перед комплексами, работа которых основана на других физических принципах, а именно:

– способны работать в любую погоду;

– способны обнаружить движущие объекты на низких высотах;

– автоматически «сопровождают» движение цели теле- или тепловизионной камерой;

– способны подавить радиоканалы управления и навигации дрона [9].

Существенным недостатком таких систем является возможность эффективной работы только на открытой местности: акватория, местность без высокой растительности и построек, территории аэропортов, а также влияние на работу гражданских устройств диапазона 433 МГц, Wi-Fi-роутеров и мобильную связь [1].

Опционально для подобных систем могут использоваться средства деактивации БПЛА. Они представляют собой радиотехнический генератор помех, который «ослепляет» дрон, оказывая воздействие на частоты, используемые для управления дроном и связи со спутниками навигации [2].

Излучение, используемое средствами подавления рабочих радиочастот дронов, оказывает большое влияние на функционирование средств гражданского назначения диапазона 433 МГц, *Wi-Fi*-роутеров, мобильную связь. Частоты, на которых происходит управление дроном (433 МГц / 2,4 ГГц / 5,8 ГГц), блокируются в радиусе до 500 м. Частоты, используемые спутниковой навигацией, подавляются в радиусе до 1 км [5].

Пример действия системы обнаружения представлен на рис. 1. На данном рисунке можно наблюдать, что система обнаруживает дрон, отслеживает его перемещение, отображая траекторию движения объекта и, при необходимости, способна посадить его на землю.

Модуль «Атака-Шорох» применяется для защиты объектов гражданского и специального назначения от несанкционированного проникновения малораз-

мерных БПЛА. Оснащение модуля содержит сверхчувствительные микрофоны, позволяющие определять местонахождение приближающегося беспилотника на расстоянии [8].

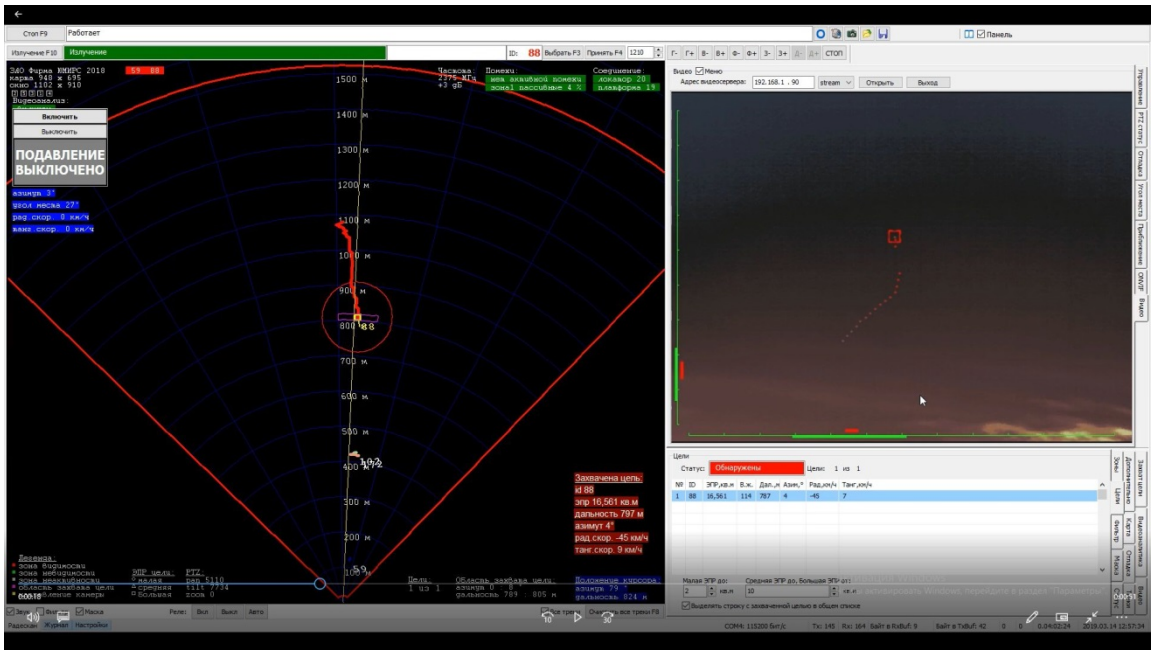

Рис. 1. Пример работы системы обнаружения и сопровождения дрона [8]

Для анализа окружающей обстановки в модуле «Атака-Шорох» используется интеллектуальная система, позволяющая выявлять по характерным шумам чрезвычайные ситуации, правонарушения, массовые скопления людей.

Оборудование имеет возможность интеграции с комплексом «Атака-DBS». При обнаружении дрона модулем акустической разведки комплекс подавляет каналы спутниковой навигации БПЛА [4].

Для оценки эффективности средств противодействия БПЛА необходимо оценить расстояние, на котором БПЛА способны перехватывать информацию. Оценка производилась на примере распознавания текста с экрана монитора и распознавания лица человека. Эквивалентная схема камеры представлена на рис. 2.

Расчет максимальной дистанции съемки L производится по следующей формуле:

$$L = \frac{Y * F}{Y'}, \tag{1}$$

где Y – размер символа, который требуется распознать; L – расстояние съемки; F – фокусное расстояние объектива камеры; Y' – четыре дискретных элемента разрешения матрицы камеры, на которые должно проецироваться изображение одного символа текста.

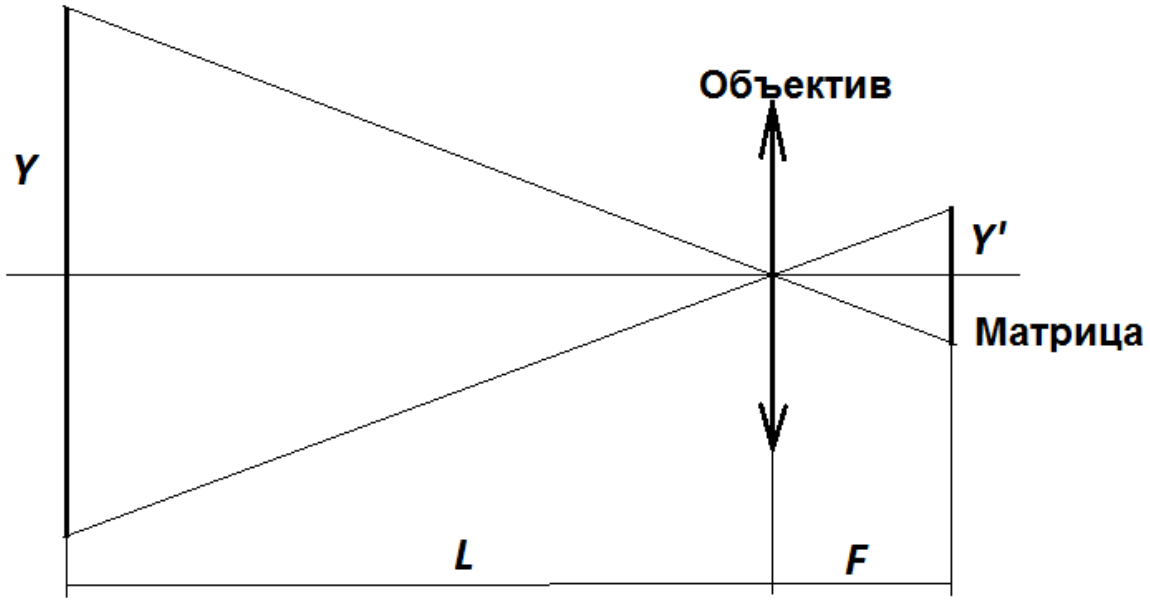

Рис. 2. Эквивалентная схема камеры

В большинстве случаев размер буквы или символа на экране монитора не превышает 3 мм. Такой же размер можно взять и для символа на бумажном носителе. В данном случае для нахождения Y' необходимо взять ширину объектива из таблицы с форматом матрицы 1/2,3″ и поделить на количество пикселей по горизонтали. Получится размер пикселя в миллиметрах [10].

Результаты

В результате выполненных исследований был проведен расчет расстояния, с которого возможно распознать символ текста на экране монитора, либо лицо человека. Для проведения расчета использовалась камера с разрешением 5280x3956, форматом матрицы 1/2,3″ и размером 6,3×4,7 мм, фокусным расстоянием объектива 45 мм. Количество пикселей на матрице используемой камеры составляет 20 887 680 пикселей.

Размер одного пикселя:

$$1\ пиксель = \frac{4,7}{3956} = 0,0012\ \text{мм}. \qquad (2)$$

Главным условием распознавания символа, буквы или цифры является отображение ее минимум четырьмя элементами матрицы камеры по горизонтали и вертикали (рис. 3).

Для четырех пикселей размер будет равен 0,0048 мм. Результаты расчетов для распознавания символа текста представлены ниже

$$L = \frac{3*45}{0.0048} = 28.1\ \text{м}. \qquad (3)$$

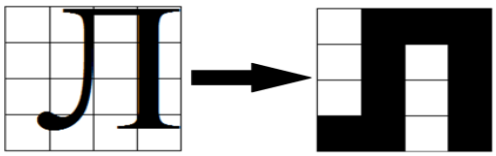

Рис. 3. Распознавание символа

Для распознавания лица человека требуется его отображение минимум 30 элементами матрицы камеры по горизонтали и вертикали. Следовательно, для 30 пикселей размер будет 0,036 мм [7]. Средний размер лица человека составляет 200 мм. Результаты расчетов дальности для распознавания лица человека представлены ниже

$$L = \frac{200 * 45}{0.036} = 250 \text{ м}. \quad (4)$$

Несмотря на относительно небольшое расстояние распознавания текста, полученное в результате расчетов, злоумышленник, используя мини-БПЛА в комплексе с камерой с указанными характеристиками, способен несанкционированно получить желаемую информацию. Примером может являться здание администрации Ленинского района г. Новосибирска. Здание расположено таким образом, что с территории прилегающей организации возможно использовать БПЛА для съема информации из помещений администрации при условии наличия окон, выходящих на западную сторону (рис. 4).

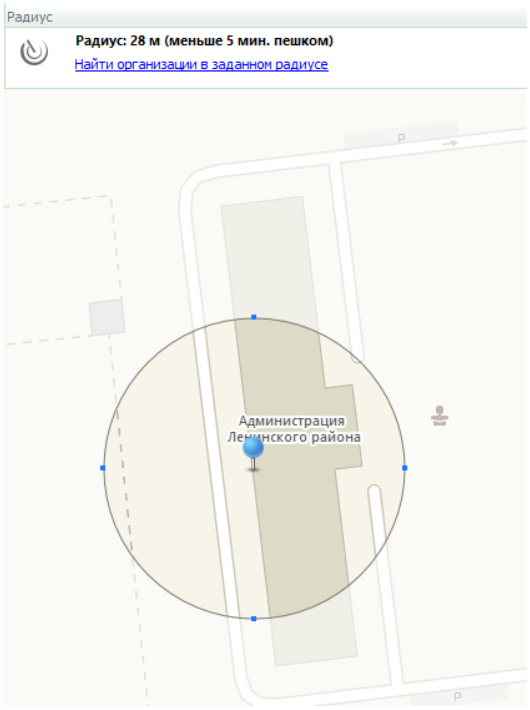

Рис. 4. Схема расположения здания администрации Ленинского района г. Новосибирска

Заключение

Анализ характеристик рассмотренных средств противодействия БПЛА позволяет сделать вывод о том, что системы противодействия БПЛА являются эффективными, поскольку способны перекрыть достаточно большой радиус воздушного пространства. Однако проблема на сегодняшний момент остается не до конца решенной, так как контролируемое воздушное пространство может не находится на территории объекта защиты и даже при обнаружении БПЛА существует большая вероятность возникновения оптического канала утечки информации. Также средства видеонаблюдения, интегрируемые на БПЛА, с каждым годом становятся более высокопроизводительными и позволяют увеличить дальность несанкционированного съема информации, что уменьшает контролируемую зону защищаемого объекта. Расчеты, проведенные в ходе работы, показывают, что расстояние, с которого может производится съем информации может быть небольшим, но при этом съем информации будет производиться с территории прилегающих организаций, что представляет серьезную угрозу для обеспечения защиты информации. Одним из возможных путей решения данной проблемы является разработка методики обнаружения БПЛА, которая будет в комплексе использовать существующие средства их обнаружения и противодействия, учитывая сильные стороны используемых средств обнаружения.

Таким образом, в дальнейшем полученные результаты будут использованы для построения методики по обнаружению БПЛА с использованием различных средств обнаружения, в том числе и тепловизионного оборудования. После разработки методики обнаружения БПЛА будет произведена ее апробация и оценка эффективности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бюро научно-технической информации: официальный сайт. – URL: http://www.bnti.ru/index.asp (дата обращения: 18.04.2022) – Текст : электронный.

2. Военно-промышленный комплекс: официальный сайт. – Москва. – Обновляется в течение суток. – URL: https://vpk.name (дата обращения: 10.05.2022). – Текст: электронный.

3. Военное обозрение: официальный сайт. – URL: https://topwar.ru (дата обращения: 28.03.2022). – Текст: электронный.

4. Годунов А. И., Шишков С. В., Юрков Н. К. Комплекс обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами /А. И. Годунов, С. В. Шишков, Н. К. Юрков. – Текст: непосредственный // Надежность и качество сложных систем, 2014. – № 2 (6). – С. 62–70.

5. Еремин Г. В., Гаврилов А. Д., Назарчук И. И. Малоразмерные беспилотники – новая проблема для ПВО /Г. В. Еремин, А. Д. Гаврилов, И. И. Назарчук. – Текст: непосредственный // Армейский вестник, 2015. – С. 24.

6. Информационный портал «Российские беспилотники» : : официальный сайт. – URL: (дата обращения : 10.12.2021). – Текст : электронный.

7. Национальная библиотека им. Н.Э. : официальный сайт. – URL: https://ru.bmstu.wiki/index.php (дата обращения : 01.05.2022). – Текст : электронный.

8. НПО «Алмаз»: официальный сайт. – URL: https://almaz-rpe.ru (дата обращения: 28.03.2022). – Текст: электронный.

9. Портал Российские беспилотники: официальный сайт. – URL: https://russiandrone.ru (дата обращения: 12.10.2021). – Текст: электронный.

10. Филин Е. Д., Киричек Р. В. Методы обнаружения малоразмерных беспилотных летательных аппаратов на основе анализа электромагнитного спектра / Е. Д. Филин, Р. В. Киричек. – Текст: непосредственный // Информационные технологии и телекоммуникации. – 2018. – Т. 6. – № 2. – С. 87–93.