

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 623.76, 004.056.53

DOI: 10.21822/2073-6185-2023-50-3-100-109



Обзорная статья / Review article

Защита верхней полусферы объекта критической информационной инфраструктуры

И.А. Лоскутов¹, В.А. Репенко²

¹Научно-производственная корпорация

«Космические системы мониторинга, информационно-управляющие и
электромеханические комплексы имени А.Г. Иосифьяна» (АО «Корпорация «ВНИИЭМ»)),

¹107078, г. Москва, ул. Вольная, 30, стр. 10, Россия,

¹Политехнический колледж им. Н.Н. Годовикова,

¹125130, г. Москва, ул. Зои и Александра Космодемьянских, 19, Россия,

²Национальный исследовательский ядерный университет «МИФИ»,

²115409, г. Москва, Каширское шоссе, 31, Россия

Резюме. Цель. Целью исследования является структурирование общедоступной информации для обеспечения защиты верхней полусферы объектов КИИ. **Метод.** В качестве методов научного познания используются: систематизация, описание, анализ, дедукция. Статья состоит из трех разделов. Вначале проводится анализ текущего состояния вопроса о потребности в защите от БПЛА. Учет идет не только военной инфраструктуры, но и также гражданской. Кроме того, для анализа проводится разделение атак дронов с целью физического уничтожения объекта КИИ / его части или же атаки на техническую составляющую. Во второй части работы проводится анализ нормативно-правовой базы России и стран ЕС. Наибольший акцент делается на отечественное законодательство и выявлении проблемных участков по теме исследования. В третьей части работы приводится проект предложений по защите объектов КИИ от угроз, исходящих от БПЛА. Для этого проведен анализ разновидностей дронов, определяются требования к системе защиты и поиска вторженцев. **Результат.** Проведено исследование проблем защиты объектов КИИ от атак дронов. Отмечен постоянный рост атак БПЛА на гражданскую и военную инфраструктуру; выявлены проблемы нормативно-правовой базы России по направлению, разработано предложение по защите верхней полусферы. **Выводы.** Проведенное исследование носит обзорный характер. Материалы, представленные в работе могут послужить базисом как для дальнейших исследований по направлению, так и для сознания соответствующих нормативных документов.

Ключевые слова: безопасность верхней полусферы, КИИ, угрозы, дроны, БПЛА.

Для цитирования: И.А. Лоскутов, В.А. Репенко. Защита верхней полусферы объекта критической информационной инфраструктуры. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(3):100-109. DOI:10.21822/2073-6185-2023-50-3-100-109

Protection of the upper hemisphere of a critical information infrastructure facility

I.A. Loskutov¹, V.A. Repenko²

¹A.G. Iosifian' Joint Company 'Research and Production Corporation

“Space Monitoring Systems, information management and electromechanical complexes”,

¹30 Volnaya St., p. 10, Moscow 107078, Russia,

¹N.N. Godovikova Polytechnic College,

¹19 Zoe and Alexandra Kosmodemyanskikh St., Moscow 125130, Russia,

²National Research Nuclear University MEPhI,

²31 Kashirskoe highway, Moscow 2115409, Russia

Abstract. Objective. Structuring of publicly available information regarding the protection of the upper hemisphere of CII objects. **Method.** The following methods of scientific cognition are used: systematization, description, analysis, deduction. The article consists of three sections. First, an analysis of the current state of the issue of the need for protection from UAVs is carried out. Accounting is not only military infrastructure, but also civil. In addition, for analysis, the separation of drone attacks is carried out in order to physically destroy the CII object / its part or attack the technical component. In the second part of the work, the analysis of the regulatory framework of Russia and the EU countries is carried out. The greatest emphasis is placed on domestic legislation and the identification of problem areas in relation to the research topic. In the third part of the work, a draft of proposals for the protection of CII objects from threats emanating from UAVs is presented. To do this, the analysis of drone varieties is carried out, the requirements for the system of protection and search for intruders are determined. **Result.** The article investigates the problems of protecting CII objects from drone attacks. A constant increase in UAV attacks on civilian and military infrastructure was noted, problems of the regulatory framework of Russia in the direction were identified, a proposal for the protection of the upper hemisphere was developed. **Conclusions.** The conducted research is of an overview nature. The materials presented in the paper can serve as a basis for further research in the direction and for the development of relevant regulatory documents.

Keywords: upper hemisphere security, cues, threats, drones, UAV

For citation: I.A. Loskutov, V. A. Repenko. Protection of the upper hemisphere of a critical information infrastructure facility. Herald of Daghestan State Technical University. Technical Science. 2023; 50(3):100-109. DOI:10.21822/2073-6185-2023-50-3-100-109

Введение. Современные технологии постоянно развиваются, особенно это касается робототехники. Одним из значимых направлений отмеченной части научно-технического прогресса, стоит считать производство беспилотных летательных аппаратов (БПЛА), которых в просторечье именуют Дронами [1]. Причина популярности данных механизмов кроется в многофункциональности их применения [2]. Среди областей, в которых задействованы БПЛА можно отметить работу в правоохранительных органах [3], внутренних войсках [4], министерства чрезвычайных ситуаций [5], исследование окружающей среды [6] и т.п. Однако, кроме использования в мирных целях, в последнее время набирают обороты атаки при помощи БПЛА на различные объекты, в том числе и на критические информационные инфраструктуры (КИИ) [7].

Постановка задачи. Действительно, нападения дронов на промышленные предприятия и иные значимые объекты все больше начинают волновать специалистов по защите [8], т.к. кроме использования в компьютерных диверсиях, они могут нести взрывчатые и ядовитые вещества, вооружение и т.п. [9]. Кроме того, сложность отслеживания столь малых воздушных объектов [10] создает значимую проблему по их обезвреживанию и недопущению происшествий. Особенно, среди прочих, атакам подвержена верхняя полусфера объектов КИИ. Из чего следует, необходимость в повышении ее защищенности.

С начала XXI века, количество нападений с применением БПЛА постоянно растет. Проявляют интерес к современным техническим системам беспилотного управления не только конкурирующие организации [11], но и в том числе различные террористические организации [12]. Именно поэтому государственные структуры пытаются обезопасить особо важные объекты, а также сохранить жизнь простых граждан путем поиска защиты от вновь возникшей угрозы. Для этого уже сейчас создаются спецподразделения в органах внутренних дел [13], разрабатываются специнструменты в армиях мира [14]. Однако, при всем при этом, остается открытым вопрос об оправданности учета дронов в качестве явной угрозы обыкновенным предприятиям, тем из них, что относятся к КИИ.

Безусловно приведенный во введении довод об увеличении количества нападений неголословен, однако ответ на вопросы - насколько значимо это число, насколько сильно оказывается влияние на отмеченные организации? - в данном разделе постараемся

определить. Причем рассмотрение будем вести с наиболее незащищенной области – верхней полусферы. Кроме того, предварительно следует разделить предприятия КИИ на две части – те, что работают с военными, причем не зависимо от того обрабатывается в них информация грифа «Гостайна» или же нет, и те, что работают в открытом частном секторе.

Атаки БПЛА, в свою очередь, тоже условно можно разделить по целенаправленности – физическое уничтожение объекта, его части (применение ракетных снарядов, авиационных бомб и т.п.) и атака на техсоставляющую (с целью вывести из строя компьютерные компоненты, провести компьютерную атаку и т.д.)

Методы исследования. Рассмотрим сведения касательно физических атак на объекты критической информационной инфраструктуры.

Первым примером следует посчитать недавний инцидент в республике Иран [15]. Атака была произведена на оборонное предприятие с помощью авиабомб. В результате было множество разрушений и данный объект на долгое время был выведен из строя.

Второй пример – атака дронов в Саудовской Аравии на объект КИИ, занятый в отрасли нефтепереработки. Функционирование объекта было восстановлено за несколько дней, однако достижения максимальной мощности работы было невозможно в течении нескольких месяцев [16]

Третий пример – атака БПЛА на Брянское КИИ [17]. В результате атаки были повреждены резервуары с нефтепродуктами, возникло возгорание, взрывы, работоспособность предприятия была нарушена.

Кроме отмеченных выше, вследствие проведения специальной военной операции на Украине, интернет версии средств массовой информации имеют различные заголовки о применении БПЛА при атаки (или их попытках) на российские оборонные предприятия в Крыму или континентальной России. Как не сложно догадаться, все атаки проводились в верхней полусфере.

Таким образом сложилась картина значительной опасности подобного рода нападений дронов на оборонные объекты КИИ, и явно наблюдается потребность в обеспечении их безопасного функционирования.

Перейдем ко второму случаю – атакам БПЛА на частный сектор с применением взрыво-ядотехнических средств.

К первому примеру следует отнести новость [18], в которой на сайте информационного портала констатируется возникновение чрезвычайного происшествия в нескольких регионах России, в том числе и в Московской области. Во всех происшествиях виноваты БПЛА, и, как следует из упоминания столичного региона, опасности подвергаются не только районы, находящиеся близ военного конфликта.

Второй пример показан в [19] и затрагивает опять регион Подмосковья. Атака, пусть и не реализована, но направлена она была против гражданской инфраструктуры и рядом расположенной КИИ.

Третий пример [20] затрагивает поселок Адыгей. БПЛА сломал инфраструктуру животноводческого объекта, что привело к финансовым потерям предпринимателя.

Как видно, атаки БПЛА не делают различий между гражданскими и оборонными КИИ, т.е. необходимость в обеспечении комплексной защиты на лицо.

Однако, несмотря на действительную опасность со стороны дронов для КИИ, с точки зрения атаки бомбами или иными средствами взрыво-химотехники, многие руководители отмеченных объектов могут не согласиться с потребностью в покупке дорогого оборудования для борьбы с БПЛА. В том же случае, если рассматриваемые в работе малые летательные аппараты способны уничтожить или «украсть» информацию с объектов, то это уже будет куда более весомым доводом для данных индивидуумов. Потому далее исследуем информационный поток по данному направлению.

В качестве первого примера можно рассмотреть новость [21]. В данном случае, атака проводилась с помощью БПЛА целенаправленно на базу данных (БД) финансовой

компании. Специалисты службы информационной безопасности (ИБ) случайно смогли отследить данное устройство, хотя по сути оно уже работало продолжительное время.

Вторым примером является атака дрона на банк [22]. В данном случае два БПЛА подключились к внутренней WiFi сети, перехватили пару «логин-пароль» и внедрили внутрь БД корпоративной сети. Однако, служба ИБ успела вовремя заметить подозрительную активность и найти данные устройства.

Другой подобный случай закончился уже в пользу взломщиков [23]. В результате физического использования дрона, злоумышленники смогли украсть 150000 евро из банкомата.

Таким образом складывается неблагоприятная картина и, как и в предыдущих двух случаях, потребность в обеспечении верхней полусферы КИИ не вызывает сомнений.

Поскольку приведенные ранее примеры относились к объектам гражданской инфраструктуры, в дополнительных доводах о потребности в защите оборонных предприятий нет необходимости.

Как уже было определено, угрозы, исходящие от дронов для объектов КИИ значительны и применение специальных средств борьбы – необходимость. Однако, для обеспечения комплексной безопасности объектов, всегда необходимо наличие двух главных компонентов – непосредственно системы защиты и нормативно-правовой базы. Именно последняя и будет рассмотрена в данном разделе.

Обратимся к нормативной правовой базе (НПБ) Европейского союза (ЕС). Причина – наиболее активное обсуждение проблем с дронами [24].

Регламенты: 923/2012 [25]; 1035/2011 [26].

В отмеченных документах жестко регламентируется понятие БПЛА, его допустимые характеристики и параметры. Кроме того, в документах приводится одна из классификаций дронов. На основании отмеченных регламентов и близкородственных НПБ, реализованных на их базе, в странах – участницах ЕС строятся правила использования БПЛА, особенности регистрации, учета, использования. Кроме того, данные регламенты заложили принципы работы с дронами больших размеров.

Отметим, что в других странах, в целом, аналогичный подход. Например, в нашем отечестве существует постановление №658 от 2019 года [27], заставляющее пользователей ставить БПЛА на учет. Более подробно нормы использования дронов по большинству стран представлены в документе [28]. Кроме того, применительно к Российской Федерации, нельзя не отметить, что из-за принадлежности БПЛА к авиационной технике, на них автоматически распространяются НПБ по направлению. Наиболее подробно они показаны в работе [29]. В данном случае учитывается не только требования по сертификации, узаконивание права собственности, но и также правила полета, особенности применения в спасательных мероприятиях и т.п.

Кроме вышеперечисленных, нельзя обойти внимание санкции, которые вводятся относительно владельцев-нарушителей БПЛА. Так, в соответствии с кодексом России [30], на нарушителей территорий и воздушного пространства, к коей в полной мере относится верхняя полусфера объекта КИИ, налагается штраф в размере от двух тысяч рублей до полумиллиона.

Однако, нельзя обойти вниманием тот факт, что законодательно, в рассматриваемом документе, статья 11, предусмотрена возможность доказать непричастность пилота к потенциальному вреду объекта КИИ, что говорит о печальных последствиях для защищаемого комплекса [31] и не проработанности законодательного акта.

Учитывая, что кроме свода НПБ об административных правонарушениях, в Российской Федерации существует и уголовный кодекс [32], рассмотрим его с точки зрения защиты верхней полусферы. В данном документе также имеется ряд статей, указывающих на ответственность нарушителя. Так, на основании Статьи 263.1 – за нарушение транспортной безопасности, максимальный срок обозначен вплоть до пяти лет; Статьи 271.1 за нарушение использование пространством над объектом КИИ с соответствующими последствиями – до трех лет. Как видно, данная НПБ подразумевает больше санкций относительно злоумышленника, однако, в текущем случае все может быть перекалифицировано как

в сторону административного нарушения, так и уголовного, от чего необходимо дальше продолжить рассмотрение уголовного кодекса.

Как уже было верно подмечено в первом разделе, атаки дронов с верхней полусферы могут носить желание нарушения хищения информации или же уничтожения ее и техники. Соответственно, о наказании за совершение подобных злодеяний ответственны Статьи 167 (слом имущества), Глава 27 (кибер преступления различного характера).

Максимальный срок за совершение данных злодеяний равняется семи годам, хотя большинство держатся в среднем на планке между тремя – четырьмя годами.

Также, говоря о регулировании защиты верхней полусферы, нельзя не отметить значимое решение радиочастотного комитета № 07-20-03-001 от 2007 года [33]. Так, в соответствии с отмеченным документом, проводится жесткая регламентация частот, на которых осуществляется управления БПЛА. Важность данного НПБ сводится к тому, что в случае нарушения периметра объекта КИИ, можно использовать специальные технические средства, которые будут создавать помехи и / или перехватывать управление над незаконно вторгшемся дроном.

Также, интересным следует считать законопроект №323987-8, поскольку он направлен на создание новых правок в НПА в части противодействия БПЛА. Так, в Статье 4 отмечается охрана объектов, к коим в полной мере относятся КИИ. Наиболее значимым в отмеченном параграфе следует считать стремление законодателей в обязательном порядке иметь средства пресечения незаконного попадания дронов. Более того, в последнем абзаце явно выделяются ответственные за защиту объектов КИИ. Кроме того, в поддержку необходимости введения данного законопроекта следует практический опыт, полученный в результате специальной военной операции [34].

Обсуждение результатов. Рассматриваемые в статье КИИ, по своей сути, представляют не обязательно военные объекты. Как показывает практика, при поиске способов обеспечения защиты верхней полусферы, в большинстве случаев будут рассматриваться гражданские системы. От того и методологию защиты следует выбирать особым способом. В частности, для формирования предложений по защите, лучше абстрагироваться от разработок, подобных [35] и тем более [36], поскольку они используют активные методы защиты - снаряды и их заменители, т.е. недоступные и опасные для большинства окружающих системы.

В целом, первоначально следует обратиться к уже отмеченному во втором разделе требованию законодателей России в части выделения определенных радиочастот для БПЛА. Заранее зная каналы передачи информации «человек-машина», значительно проще определить геоположение дронов. Так, из источника [37] следует, что данный процесс достаточно тривиален, соответственно и обезопасить себя КИИ сможет тоже за малые деньги. Однако, кроме стандартных «усовершенствованных игрушек», возможны и другие варианты исполнения летательных механизмов. К первым будут относиться самодельные БПЛА. Действительно, не имея явных ограничений, творцы-создатели подобного рода дронов могут использовать нестандартные модули и специфическую программно-аппаратную часть, что вызовет проблемы в части обеспечения безопасности. Однако тут важно заметить, что подобные системы дороги и от того не всем предприятиям следует беспокоиться о возможности нападения на них. Объекты КИИ с низкими финансовыми потоками будут с минимальной долей вероятности атакованы подобными средствами.

Второй вариант – применение специальных БПЛА военного образца. Тут важно отметить, что их тоже условно можно подразделить на: 2.1 – массового исполнения, 2.2 – тактического. В первом подварианте уже создаются значительные угрозы объектам КИИ, поскольку частоты их работы отличаются от вышеупомянутых требований. Кроме того, как и следует ожидать, данные устройства очень неплохо защищены от перехвата и имеют несколько контуров связи и поддержания заданного курса [38]. Второй подтип использует уже сверхсовременные БПЛА, такие как Global Hawk или Triton [38], которые на данный момент ни разу не были перехвачены. Данные аппараты представляют наивысшую угрозу для объектов КИИ. Следует констатировать один важный факт – интерес подобного рода

дронов возможен только к очень узкому кругу предприятий, поскольку они крайне дороги и, если первые еще можно попытаться найти на «черном» рынке, то последние – без шансов. Однако даже в первом случае вопрос цены будет колоссальным, соответственно информационные ограбления, показанные в первом разделе данной работы просто будут нерентабельны для них. По большей части данные дроны будут использоваться только военными, из-за чего и объекты обрабатывающие данные с грифом «Гостайна» – чуть ли не единственные потенциальные цели для них.

Определив некоторые особенности нападений дронов на объекты КИИ, можно перейти к разработке предложений по защите верхней полусферы.

В данном случае необходимо, чтобы система отвечала определенным требованиям. Они верно подмечены в работе [39]:

1. Система защиты от беспилотных летательных аппаратов (СЗоБПЛА) должна глушить частоты передачи телеметрии и иной управляющей информации;
2. СЗоБПЛА должна уметь определять наличие оптических средств съема информации у дронов и слепить их;
3. СЗоБПЛА должна применять активные средства защиты невоенного дела (система ускорения потоков воздуха, дым и т.п.);
4. СЗоБПЛА должна комплексно взаимодействовать с физическими элементами защиты (сети, решетки и т.п. ограждения, не дающие попасть дрону в воздушное пространство объекта КИИ);
5. СЗоБПЛА должна содержать аналогичные атакующим системы защиты (дропо-перехватчиков).

Таким образом должна решаться в СЗоБПЛА комплексная задача, состоящая из трех глобальных частей [33]:

1. Определение нарушителей-дронов;
2. Перехват управления БПЛА;
3. Анализатор состояния защищаемой области.

Кроме того, в СЗоБПЛА обязательно должны быть заложены принципы защиты на подобие тех, что описаны в работе [40], т.е. реализовать всевозможные угрозы БПЛА, среди которых GPS-spoofing из-за доказанной эффективности [41] должен занимать лидирующие позиции.

Главными требованиями к СЗоБПЛА [42]:

1. Эффективность работы должна быть на уровне вне зависимости от внешней окружающей среды;
2. Система должна входить в рабочее состояние после простоя / ремонта или иного подобного действия за минимальное количество времени;
3. Программное обеспечение должно состоять из компонентов интуитивно понятных пользователю, способное самостоятельно информировать о возможных угрозах верхней полусферы объекта КИИ.

Кроме того, в качестве борьбы с БПЛА может быть предложена идея о дистанционном выключении двигателей. В результате крушения дрона, угроза соответственно автоматически будет нивелирована. В данном случае изначально необходимо СЗоБПЛА определить какой тип двигателя установлен на летательном аппарате [43] и как его отключить. Например, при использовании двигателей внутреннего сгорания (ДВС) можно использовать тот же дым. С одной стороны, визуальная составляющая будет снижена, с другой потенциальное засорение ДВС приведет к падению дрона. Сам комплекс СЗоБПЛА должен содержать все доступные системы поиска дронов-нарушителей, среди которых [44]: радиолокационные; радиотехнические; оптико-электронные; акустические.

Вывод. Проведенный в работе анализ носит обзорный характер и затрагивает ключевые моменты, связанные с защитой верхней полусферы объекта КИИ и потребностью в данном деянии. Постоянный рост атак БПЛА на гражданскую и военную инфраструктуру

позволяет судить об угрозе всем объектам КИИ, вне зависимости от обрабатываемой в них информации. Отдельно важно отметить, что рассмотренная в статье НПБ показала весьма неутешительную картину – на данный момент нет явной структурированной базы и накопленного мирового опыта по безопасности верхней полусферы. Законодательные акты разрознены, нововведения распределены по старым законам, но мало друг с другом синергируют. Безусловно имеется законопроект №323987-8, направленный на решение отмеченной проблемы, но он пока не принят. Кроме того, даже при его включении в НПБ возможны правовые коллизии, вследствие отсутствия явных приказов федеральных органов исполнительной власти, а также документов, посвященных тематике.

В статье указывается на те минимальные требования к безопасности верхней полусферы которые должны быть прописаны в законе и учитывают возможности большинства игроков. При создании защитных механизмов зачастую неоправданно опираться на разработки активной борьбы с БПЛА, реализованных посредством ракетно-технической составляющей вследствие ее опасности для окружающих и недоступности большинству объектов КИИ. Среди главных параметров определения положения дронов в пространстве оправдан геолокационный поиск по частотам, наиболее распространенным (законодательно) на потребительском рынке БПЛА. Важно учитывать тот факт, что большую опасность для объектов КИИ будут представляла дроны, созданные кустарными методами, поскольку защиту от стандартных модификаций относительно легко реализовать, а вероятность применения военных технологий для большинства КИИ крайне маловероятна. Для борьбы с БПЛА рационально применять дымовую завесу, т.к. она сильно вредит дронам с ДВС и с высокой вероятностью вызовет его отказ. Параллельно необходимо выполнять показанные требования к СЗОБПЛА и использовать все возможные системы поиска. Именно такая синергия обеспечит максимальную защищенность объектов КИИ.

Библиографический список:

1. Тимченко Б.Г. Исследование задачи посадки БПЛА на судно-носитель. - СПб, 2018. - 41 с.
2. Жолымбаев А.О. Особенности гражданского применения беспилотных летательных аппаратов на примере возможностей их использования при ликвидации чрезвычайных ситуаций // Научный альманах. - 2016. - № 1-3(15). - С. 23-30
3. Дронова О.Б., Храмова Е.С. Генезис совершенствования функциональных возможностей беспилотных летательных аппаратов, используемых в качестве технико-криминалистических средств // Сибирские уголовно-процессуальные и криминалистические чтения. - 2022. - №1 (35). - С. 77-87
4. Терех Е.Г., Мещеряков С.А. Применение беспилотных летательных аппаратов в интересах МЧС и внутренних войск республики Беларусь // Обеспечение безопасности жизнедеятельности : проблемы и перспективы : сборник материалов IX международной научно-практической конференции молодых ученых: курсантов (студентов), слушателей магистратуры и адъюнктов (аспирантов) : в 2-х ч. Ч.1. - Минск : КИИ, 2015. С.136-137
5. Воропаев Н.П. Применение беспилотных летательных аппаратов в интересах МЧС России // Научно-аналитический журнал «Вестник Санкт-Петербургского государственного университета Государственной противопожарной службы МЧС России». - 2014. - № 4. - С. 13-17
6. Полякова Е.В. Возможности подспутникового ДЗЗ с использованием беспилотного летательного аппарата CropCam в условиях Европейского Севера // Arctic Environmental Research. - 2010. - №2. - С.22-26
7. Запорожцев Д.В. Критически важные инфраструктурные объекты Каспийского региона как цели террористических атак и диверсий // Вестник Академии военных наук. - 2022. - № 1(78). - С. 33-37
8. В РФ растёт количество атак на информационные системы и физическую инфраструктуру предприятий, согласно данным от «Лаборатории Касперского». - URL: <https://www.ixbt.com/news/2022/12/12/v-rf-rastjot-kolichestvo-atak-na-informacionnye-sistemy-i-fizicheskuju-infrastrukturu-predpriyatij-soglasno-laboratorii.html> (дата обращения 24.03.2023)
9. Шилов О.В. Защита верхней полусферы объектов ТЭК и промышленности от атак с воздуха с применением искусственного интеллекта // Деловая Россия. ТБ Форум. Технологии защиты периметра и верхней полусферы для крупных и распределенных объектов. - 2023. - 25с.
10. Дажунц Б.Э., Тазетдинов А.А., Бабушкин И.Н., Лушпай И.В. Вопросы управления и обеспечения защиты беспилотных летательных аппаратов от помех // Студенческий форум. - 2022. - № 17-2(196). - С. 67-68
11. Захаров А.Н. Корпоративная безопасность фирмы в контексте развития Арктических регионов России // Мировые цивилизации. - 2021. - Т.6. - № 1. - С. 44-49
12. Блохин К.В., Вихрян А.П. Высокотехнологический терроризм – угроза цивилизации XXI века // Международный правовой курьер. - 2020. - №5. - С.8-13
13. На Кубани создадут подразделение полиции по пресечению атак беспилотников. - URL: <https://www.kommersant.ru/doc/5889828> (дата обращения 24.03.2023)
14. Защиту от боевых дронов отработали на пунктах управления Каспийской флотилии. - URL: https://function.mil.ru/news_page/country/more.htm?id=12273065@egNews (дата обращения 12.03.2023)

15. Появились подробности атаки дронов на оборонный завод в Иране. - URL: <https://www.mk.ru/politics/2023/01/29/poyavilis-podrobnosti-ataki-dronov-na-oboronnnyy-zavod-v-irane.html> (дата обращения 12.03.2023)
16. Атака XXI века: как маленькие дроны нанесли огромный урон Саудовской Аравии. - URL: <https://tech.onliner.by/2021/06/26/malenkie-drony-nanesli-ogromnyj-uron> (дата обращения 10.03.2023)
17. Брянское предприятие пострадало после атаки беспилотников. - URL: <https://bel.ru/news/2022-12-06/bryanskoe-predpriyatie-postradalo-posle-ataki-bespilotnikov-2608444> (дата обращения 12.03.2023)
18. СК выяснит обстоятельства атак беспилотников на объекты на территории России. - URL: <https://www.forbes.ru/society/485524-sk-vyasnit-obstoatelstva-atak-bespilotnikov-na-ob-ekty-na-territorii-rossii> (дата обращения 18.03.2023)
19. Власти подтвердили атаку БПЛА на объект гражданской инфраструктуры в Подмосковье. - URL: https://www.dp.ru/a/2023/02/28/Vlasti_podtverdili_ataku (дата обращения 18.03.2023)
20. Атака беспилотников на российские города и закрытие неба в Петербурге. Что известно. - URL: <https://rtvi.com/news/ataka-bespilotnikov-na-rossijskie-goroda-i-zakrytie-neba-v-peterburge-chto-izvestno/> (дата обращения 18.03.2023)
21. Финансовая компания обнаружила, что ее пытаются взломать с помощью дрона с WiFi Pineapple на борту. - URL: <https://xaker.ru/2022/10/13/drone-hacking/> (дата обращения 20.03.2023)
22. Хакеры использовали дроны DJI для взлома банка. - URL: <https://quadronews-ru.turbopages.org/quadronews.ru/s/hakery-vzlomali-bank-dronom-dji.html/> (дата обращения 20.03.2023)
23. Высокотехнологичное ограбление банка с помощью дрона DJU Mini. - URL: <https://dronomania.ru/news/vysokotehnologichnoe-ograblenie-banka-s-pomoshhyu-drona-dju-mini.html?ysclid=leypr8qf8q9192940977> (дата обращения 20.03.2023)
24. Мотасова Д.Д. Международно-правовое регулирование использования беспилотных летательных аппаратов // Транспортное право и безопасность. - 2019. - № 1(29). - С.116-128
25. Commission Implementing Regulation (EU) No 923/2012 of 26 September 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation and amending
26. Регламент за изпълнение (ЕС) No 1035/2011 на комисията от 17 октомври 2011 година за определяне на общи изисквания при доставянето на аеронавигационни услуги
27. Постановление Правительства Российской Федерации от 25.05.2019 г. № 658 Об утверждении Правил учета беспилотных гражданских воздушных судов с максимальной взлетной массой от 0,25 килограмма до 30 килограммов, ввезенных в Российскую Федерацию или произведенных в Российской Федерации
28. Курченко Н.Ю., Труфляк Е.В. Нормативно-правовая база использования беспилотных авиационных систем. - Краснодар : КубГАУ, 2020 - 45 с.
29. Анализ современного состояния нормативной правовой базы Российской Федерации в области использования воздушного пространства беспилотными авиационными системами и разработка предложений по ее совершенствованию. - URL: <https://russiandrone.ru/publications/4-analiz-sovremennogo-sostoyaniya-normativnoy-pravovoy-bazy-rossiyskoy-federatsii-v-oblasti-ispolzov/> (дата обращения 28.03.2023)
30. Закон N 195-ФЗ от 30.12.2001 «Кодекс Российской Федерации об административных правонарушениях»
31. Винокурова В.В., Вытовтов А.В., Шумилин В.В. Административно правовое регулирование использования беспилотных летательных аппаратов в Российской Федерации // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций. - 2015. - №1. - 6 с.
32. Закон N 63-ФЗ от 13.06.1996 «Уголовный кодекс Российской Федерации»
33. Решение ГКРЧ при Мининформсвязи России от 07.05.2007 N 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия»
34. Депутаты Госдумы запустили реформу защиты РФ от беспилотников. - URL: <https://ura.news/news/1052630111> (дата обращения 28.03.2023)
35. Пат. 2755951 Российская Федерация, МПК F41H 11/02, F41H 13/00. Способ активной защиты объекта со стороны верхней полусферы / В.А. Подгорнов, М.Ю. Наumenko, С.Г. Вагин, А.Е. Кипкаев, Г.А. Крестьянинов, С.В. Подгорнов ; заявитель и патентообладатель Федеральное государственное унитарное предприятие «Российский федеральный ядерный центр – ВНИИТФ им. Акад. Е.И. Забахина» - № 2020144323 ; заявл. 29.12.2020 ; опубл. 23.09.2021, Бюл. №27
36. Пат. 185949 Российская Федерация, МПК F41H 11/04, B64D 1/00, F41H 13/00. Устройство борьбы с беспилотными летательными аппаратами / А.Г. Нескин, В.И. Бзыта, А.Н. Зеленов, М.Л. Соколов, В.А. Подгорнов, А.Е. Кипкаев ; заявитель и патентообладатель Федеральное государственное унитарное предприятие «Российский федеральный ядерный центр – ВНИИТФ им. Акад. Е.И. Забахина» - № 2018131051 ; заявл. 08.10.2018 ; опубл. 25.12.2018, Бюл. №36
37. Атакующие БПЛА и системы противодействия им, обзор. - URL: <https://habr.com/ru/post/365625/> (дата обращения 29.03.2023)
38. Уязвимость каналов управления штатовскими тактическими БПЛА: технологические моменты. - URL: <https://topwar.ru/106252-uyazvimost-kanalov-upravleniya-shtatovskimi-takticheskimi-bpla-tehnologicheskie-momenty.html> (дата обращения 29.03.2023)
39. Противодействие БПЛА. Защита от дронов и квадрокоптеров. - URL: <https://www.a0-avtomatika.ru/media/blog/protivodeystvie-bpla-zashchita-ot-dronov-i-kvadrokoptero-#%D0%92%D0%B8%D0%B4%D1%8B%20%D1%81%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%D1> (дата обращения 29.03.2023)
40. База знаний об атаках на беспилотные летательные аппараты / Е.С. Басан, А.С. Басан, А.В. Некрасов [и др.] // Системный синтез и прикладная синергетика : сборник научных работ X Всероссийской научной конференции, пос. Нижний Архыз, 28 сентября – 02 октября 2021 года. – Ростов-на-Дону, Таганрог: Южный федеральный университет, 2021. С. 170-178

41. Кривенков Д.В. Противодействие несанкционированному добытию информации дронами // Технические и математические науки. Студенческий научный форум : Электронный сборник статей по материалам II студенческой международной научно-практической конференции. Том 2 (2) : ООО «Международный центр науки и образования», 2018. - С. 34-39
42. Методы против БПЛА. - URL: <https://arsenal-otechestva.ru/article/1601-metody-protivodejstviya-bpla> (дата обращения 29.03.2023)
43. Костюченков А.Н., Минин В.П., Клементьев С.А., Федин А.В. Научно-технические проблемы создания и производства роторно-поршневых двигателей для БПЛА за рубежом // Инноватика и экспертиза: научные труды. - 2019. - № 3(28). - С. 143-156
44. Макаренко С.И. Противодействие беспилотным летательным аппаратам. Монография. - СПб.: Наукоемкие технологии, 2020. - 204 с.

References

1. Timchenko B.G. Issledovanie zadachi posadki BPLA na sudno-nositel'. SPb, 2018; 41. (In Russ)
2. Zholymbayev A.O. Especially civil applications of unmanned aerial vehicles on the example of the possibilities of their use in emergency situations. *Nauchnyj al'manah*. 2016;1-3(15): 23-30 (In Russ)
3. Dronova O.B., Khramova E.S. The Genesis of Improving Functional Capabilities of Unmanned Aerial Vehicles Used as Forensic Equipment. *Siberian Criminal Procedure and Criminalistic Readings*. 2022;1(35): 77-87 (In Russ)
4. Tereh E.G., Meshcheryakov S.A. The use of unmanned aerial vehicles in the interests of the Ministry of Emergency Situations and internal troops of the Republic of Belarus. Ensuring life safety: problems and prospects: collection of materials of the IX international scientific and practical conference of young scientists: cadets (students), master's students and adjuncts (graduate students): in 2 hours. Part 1. - Minsk: KII, 2015;136-137
5. Voropaev N.P. Use of unmanned aerial vehicles in the interests of emercom of Russia. Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". 2014.;4: 13-17(In Russ)
6. Polyakova E.V. Possibilities of undersatellite remote sounding of the earth with use of CropCam unmanned aerial vehicles in the conditions of the European North. *Arctic Environmental Research*. 2010; 2:22-26
7. Zaporozhtsev D.V. Critical infrastructure facilities in the Caspian region as targets of terrorist attacks and sabotage *Vestnik Akademii voennyh nauk*. 2022;1(78):33-37(In Russ)
8. V RF rastyot kolichestvo atak na informacionnye sistemy i fizicheskuyu infrastrukturu predpriyatij, soglasno dannym ot «Laboratorii Kasperskogo». - URL: <https://www.ixbt.com/news/2022/12/12/v-rf-rastyot-kolichestvo-atak-na-informacionnye-sistemy-i-fizicheskuyu-infrastrukturu-predpriyatij-soglasno-laboratorii.html> (date of request 24.03.2023) (In Russ)
9. Shilov O.V. Protection of the upper hemisphere of fuel and energy complex and industrial facilities from air attacks using artificial intelligence. *Business Russia. TV Forum. Perimeter and upper hemisphere protection technologies for large and distributed objects*. 2023; 25. (In Russ)
10. Dazhunts B.E., Tazetdinov A.A., Babushkin I.N., Lushpay I.V. Issues of managing and ensuring the protection of unmanned aerial vehicles from interference. *Student Forum* 2022;17-2(196): 67-68(In Russ)
11. Zakharov A.N. Corporate security of the company in the context of the development of the Arctic regions of Russia. *World civilizations*. 2021;6(1): 44-49(In Russ)
12. Blokhin K.V., Vikhryan A.P. High-tech terrorism is a threat to civilization of the 21st century. *International Legal Courier*. 2020;5:8-13(In Russ)
13. A police unit will be created in Kuban to suppress drone attacks. - URL: <https://www.kommersant.ru/doc/5889828> (access date 03/24/2023) (In Russ)
14. Protection against combat drones was practiced at the control points of the Caspian flotilla. - URL: https://function.mil.ru/news_page/country/more.htm?id=12273065@egNews (date accessed 03/12/2023) (In Russ)
15. Details have emerged of a drone attack on a defense plant in Iran. - URL: <https://www.mk.ru/politics/2023/01/29/poyavilis-podrobnosti-ataki-dronov-na-oboronnyy-zavod-v-irane.html> (access date 03/12/2023) (In Russ)
16. Attack of the 21st century: how small drones caused huge damage to Saudi Arabia. - URL: <https://tech.onliner.by/2021/06/26/malenkie-drony-nanesli-ogromnyj-uron> (date accessed 03/10/2023)
17. The Bryansk enterprise suffered after a drone attack. - URL: <https://bel.ru/news/2022-12-06/bryanskoe-predpriyatie-postradalo-posle-ataki-bespilotnikov-2608444> (date accessed 03/12/2023)
18. The Investigative Committee will find out the circumstances of drone attacks on objects on Russian territory. - URL: <https://www.forbes.ru/society/485524-sk-vyasnit-obstoatelstva-atak-bespilotnikov-na-obekty-na-territorii-rossii> (access date 03/18/2023)
19. Authorities confirmed a UAV attack on a civilian infrastructure facility in the Moscow region. - URL: https://www.dp.ru/a/2023/02/28/Vlasti_podtverdili_ataku (access date 03/18/2023) (In Russ)
20. Drone attacks on Russian cities and the closure of the sky in St. Petersburg. What is known. - URL: <https://rtvi.com/news/ataka-bespilotnikov-na-rossijskie-goroda-i-zakrytie-neba-v-peterburge-cto-izvestno/> (date accessed 03/18/2023) (In Russ)
21. A financial company discovered that they were trying to hack it using a drone with WiFi Pineapple on board. - URL: <https://xakep.ru/2022/10/13/drone-hacking/> (date accessed 03/20/2023) (In Russ)
22. Hackers used DJI drones to hack a bank. - URL: <https://quadronews-ru.turbopages.org/quadronews.ru/s/hakery-vzломali-bank-dronom-dji.html/> (date accessed 03/20/2023) (In Russ)
23. High-tech bank robbery using a DJU Mini drone. - URL: <https://dronomania.ru/news/vysokotekhnologichnoe-ograblenie-banka-s-pomoshhyu-drona-dji-mini.html?ysclid=leyp8qf8q9192940977> (date accessed 03/20/2023) (In Russ)
24. Motasova D.D. International legal regulation of the use of pilotless aerial vehicles. *Transport law and security*. 2019;1(29):116-128(In Russ) (In Russ)
25. Commission Implementing Regulation (EU) No 923/2012 of 26 September 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation and amending

26. Reglament za izp"nenie (ES) No 1035/2011 na komisijata ot 17 oktomvri 2011 godina za opredelyane na obshchi iziskvaniya pri dostavyaneto na aeronavigacionni uslugi
27. Decree of the Government of the Russian Federation of May 25, 2019 No. 658 On approval of the Rules for accounting for unmanned civil aircraft with a maximum take-off weight from 0.25 kilograms to 30 kilograms imported into the Russian Federation or produced in the Russian Federation (In Russ)
28. Kurchenko N.Yu., Truflyak E.V. Regulatory framework for the use of unmanned aerial systems. - Krasnodar: KubSAU, 2020; 45. (In Russ)
29. Analysis of the current state of the regulatory legal framework of the Russian Federation in the field of use of airspace by unmanned aircraft systems and development of proposals for its improvement. - URL: <https://russiadrone.ru/publications/4-analiz-sovremennogo-sostoyaniya-normativnoy-pravovoy-bazy-rossiyskoy-federatsii-v-oblasti-ispolzov/> (date accessed 03/28/2023) (In Russ)
30. Law No. 195-FZ of December 30, 2001 "Code of the Russian Federation on Administrative Offences" (In Russ)
31. Vinokurova V.V., Vytovtov A.V., Shumilin V.V. Administrative and legal regulation of the use of unmanned aerial vehicles in the Russian Federation. Problems of ensuring security during the liquidation of consequences of emergency situations. 2015;1: 6. (In Russ)
32. Law No. 63-FZ of June 13, 1996 "Criminal Code of the Russian Federation" (In Russ)
33. Decision of the SCRF under the Ministry of Information and Communications of Russia dated 05/07/2007 N 07-20-03-001 "On the allocation of radio frequency bands to short-range devices"
34. State Duma deputies launched a reform of the protection of the Russian Federation from drones. - URL: <https://ura.news/news/1052630111> (access date 03/28/2023) (In Russ)
35. Pat. 2755951 Russian Federation, MPK F41H 11/02, F41H 13/00. Method of active protection of an object from the upper hemisphere / V.A. Podgornov, M.Yu. Naumenko, S.G. Vagin, A.E. Kipkaev, G.A. Krestyaninov, S.V. Podgornov; applicant and patent holder Federal State Unitary Enterprise "Russian Federal Nuclear Center - VNIITF named after Academician E.I. Zabakhin" - No. 2020144323; application 12/29/2020 ; publ. 09/23/2021, Bulletin. No. 27(In Russ)
36. Pat. 185949 Russian Federation, MPK F41H 11/04, B64D 1/00, F41H 13/00. Device for combating unmanned aerial vehicles / A.G. Neskin, V.I. Bzyta, A.N. Zelenov, M.L. Sokolov, V.A. Podgornov, A.E. Kipkaev; applicant and patent holder Federal State Unitary Enterprise "Russian Federal Nuclear Center - VNIITF named after Academician E.I. Zabakhin" - No. 2018131051; application 10/08/2018 ; publ. 12/25/2018; 36(In Russ)
37. Attacking UAVs and systems to counter them, review. - URL: <https://habr.com/ru/post/365625/> (access date 03/29/2023) (In Russ)
38. Vulnerability of control channels for US tactical UAVs: technological aspects. - URL: <https://topwar.ru/106252-uyazvimost-kanalov-upravleniya-shtatovskimi-takticheskimi-bpla-tehnologicheskie-momenty.html> (access date 03/29/2023) (In Russ)
39. Countering UAVs. Protection against drones and quadcopters. URL: <https://www.ao-avtomatika.ru/media/blog/protivodeystvie-bpla-zashchita-ot-dronov-ikvadrokopterov/> #%D0%92%D0%B8%D0%B4%D1%8B1%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%20% (date of access 03/29/2023) (In Russ)
40. Knowledge base about attacks on unmanned aerial vehicles / E.S. Basan, A.S. Basan, A.V. Nekrasov [and others] // System synthesis and applied synergetics: collection of scientific works of the X All-Russian scientific conference, pos. Nizhny Arkhyz, September 28 – October 2, 2021; Rostov-on-Don, Taganrog: Southern Federal University, 2021; 170-178(In Russ)
41. Krivenkov D.V. Countering unauthorized acquisition of information by drones Technical and mathematical sciences. Student Scientific Forum: Electronic collection of articles based on materials from the II Student International Scientific and Practical Conference. LLC "International Center for Science and Education", 2018;2: 34-39(In Russ)
42. Methods against UAVs. - URL: <https://arsenal-otechestva.ru/article/1601-metody-protivodeystviya-bpla> (date accessed 03/29/2023) (In Russ)
43. Kostyuchenkov A.N., Minin V.P., Klementyev S.A., Fedin A.V. Scientific and technical problems of the creation and production of rotary piston engines for UAVs abroad. Innovation and expertise: scientific works. 2019; 3(28):143-156(In Russ)
44. Makarenko S.I. Countering unmanned aerial vehicles. Monograph. St. Petersburg: High technology, 2020; 204.(In Russ)

Сведения об авторах:

Лоскутов Иван Андреевич, Инженер – конструктор, отдел 55; преподаватель автоматизации; faxvex@ya.ru

Репенко Виктор Андреевич, Магистрант, faxvex@ya.ru

Information about the authors:

Ivan A. Loskutov, Engineer-constructor in the Department 55, faxvex@ya.ru

Viktor A. Repenko, Master's student; faxvex@ya.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 28.06.2023.

Одобрена после рецензирования / Reviced 20.07.2023.

Принята в печать /Accepted for publication 20.07.2023.