УДК 004.056 Вестник УрФО № 1(55) / 2025, с. 45–54

Костюченко К. Л., Вандышев И. С. DOI: 10.14529/secur250105

ПОЯВЛЕНИЕ НОВЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ ДРОНОВ

В статье показано как инновационное транспортное средство – дрон – может стать угрозой безопасности информации. Представлена классификация современных беспилотных летательных аппаратов. Рассмотрены характеристики и сферы применения дронов. На основе реальных ситуаций и системного прогнозирования описываются угрозы, связанные с противозаконным использованием дронов, в т.ч. угрозы безопасности информации и угрозы объектам информатизации. Комплексный подход исследования заставляет по-новому взглянуть на проблемы обеспечения безопасности. Определяются меры защиты от преступного применения беспилотных летательных аппаратов. Представленный набор схем возможных негативных событий позволяет заранее предпринимать защитные меры.

Ключевые слова: *дрон, беспилотный летательный аппарат, угрозы безопасности информации, защита информации, объекты информатизации, антидроновые системы безопасности.*

Kostyuchenko K. L., Vandyshev I. S.

THE EMERGENCE OF NEW THREATS TO INFORMATION SECURITY WHEN USING DRONES

The article shows how an innovative vehicle – a drone – can become a threat to information security. The classification of modern unmanned aerial vehicles is presented. The characteristics and applications of drones are considered. Based on real-world situations and system forecasting, the threats asso-ciated with the illegal use of drones are described, including threats to information security and threats to informatization facilities. The comprehensive ap-proach of the research forces us to take a fresh look at security issues. Measures to protect against the criminal use of unmanned aerial vehicles are being de-fined. The presented set of schemes of possible negative events allows you to take protective measures in advance.

Keywords: *drone, unmanned aerial vehicle, threats to information security, information protection, objects of informatization, anti-drone security systems.*

Введение

Развитие науки и техники приводит к прогрессивным изменениям в жизни и деятельности человека. Однако в некоторых случаях добавляются и негативные побочные явления. Подобная ситуация сейчас складывается с дронами.

Поэтому целью данной статьи является показ того, как достаточно инновационное транспортное средство – дрон – может стать угрозой безопасности информации. Для этого будут рассмотрены классификация и сферы применения современных беспилотных летательных аппаратов, схемы создания дронами угроз безопасности информации и объектам ин-форматизации, а также меры нейтрализации этих угроз.

Классификация и применение дронов

Под термином «дрон» обычно понимается летательный аппарат без экипажа на борту – беспилотный летательный аппарат (БПЛА) или «беспилотник». Иногда этот термин трактуется шире. Дронами называют все аппараты, входящие в сообщество беспилотных мобильных средств, отличающихся разными средами функционирования (рис. 1) [1]. В разговорной речи термин «дрон», сужается до понятия «коптер» (или «квадрокоптер»), т.е. БПЛА вертолетного типа с несколькими роторами (чаще всего с четырьмя).

Первые дроны появились достаточно давно – в XIX веке – и стали активно использоваться военными. В период Мировых войн это были самолеты-мишени, летающие торпе-

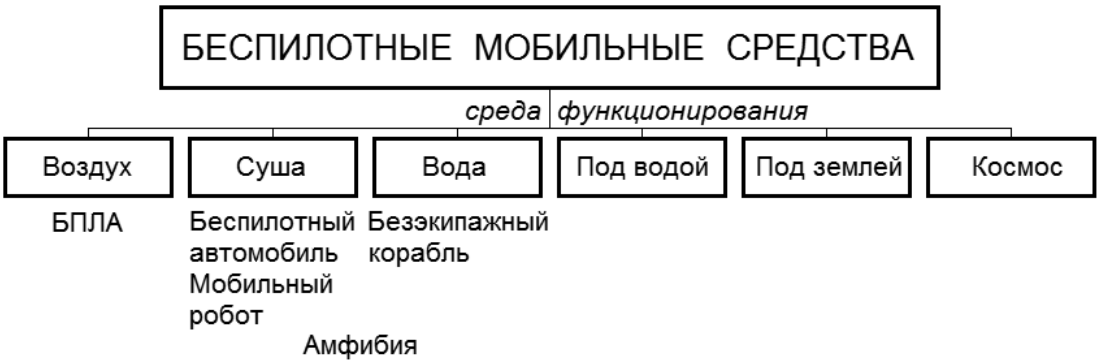

Рис. 1. Классификация беспилотных мобильных средств

Рис. 2. Классификация дронов

ды, реактивные беспилотные разведчики, крылатые ракеты и иные дистанционно-пилотируемые летательные аппараты (ДПЛА). В настоящее время БПЛА имеют различные типы конструкций с самыми разнообразными функциями и областями применения [2].

По основному критерию технической классификации – принципу полета – БПЛА делятся на следующие группы: аэростатического типа (дирижабли); с гибким крылом (мотопарапланы); с машущим крылом; с жестким крылом (самолеты); с вращающимся крылом (вертолетного типа), а различные гибриды (например, автожиры) (рис. 2).

Развитие техники, электроники, энергетики, информационных тех-нологий и программирования в начале XXI века определило тенденции в создании БПЛА:

- повышение энергоемкости тяговых аккумуляторов;
- применение новых конструкционных материалов;
- использование разнообразных конструкторских решений;
- уменьшение размеров (в целом и составных элементов);
- универсализация компоновки аппаратов;
- увеличение длительности полетов;
- повышение стабильности;
- постоянное появление новых функций.

Названные тенденции определили широту применения БПЛА (как гражданского, так и военного) (рис. 3). В гражданском применении это: мониторинг ЛЭП, теплосетей, трубопроводов, дорог, сооружений и иных объектов инфраструктуры; научные исследования (метеорология, эколо-гия, геология, археология); выполнение сторожевых функций; поисково-спасательные работы; фотосъемка и видеорепортажи; доставка грузов и еды (дроны-аэротакси, службы доставки); распыление химикатов (опыле-ние, вызов дождей); использование в системах связи; рекламные акции; свето-динамические шоу и др. В военном применении это: ведение разведки; целеуказание; объективный контроль (в реальном масштабе времени); гранато- и бомбометание; нанесение ударов летающими боеприпасами-«камикадзе»; доставка питания, боекомплекта и медикаментов; создание фиктивных целей; охрана объектов и патрулирование коммуникаций, радиоэлектронное подавление; ретрансляция данных [3]. К сожалению, существует и сфера неправомерного применения дронов (с различными целями: террористическими, криминальными и т.п.).

Большая доля применяемого арсенала дронов – мультироторные БПЛА – коптеры (в основном квадрокоптеры), оснащенные видеокамерой с передачей данных в реальном

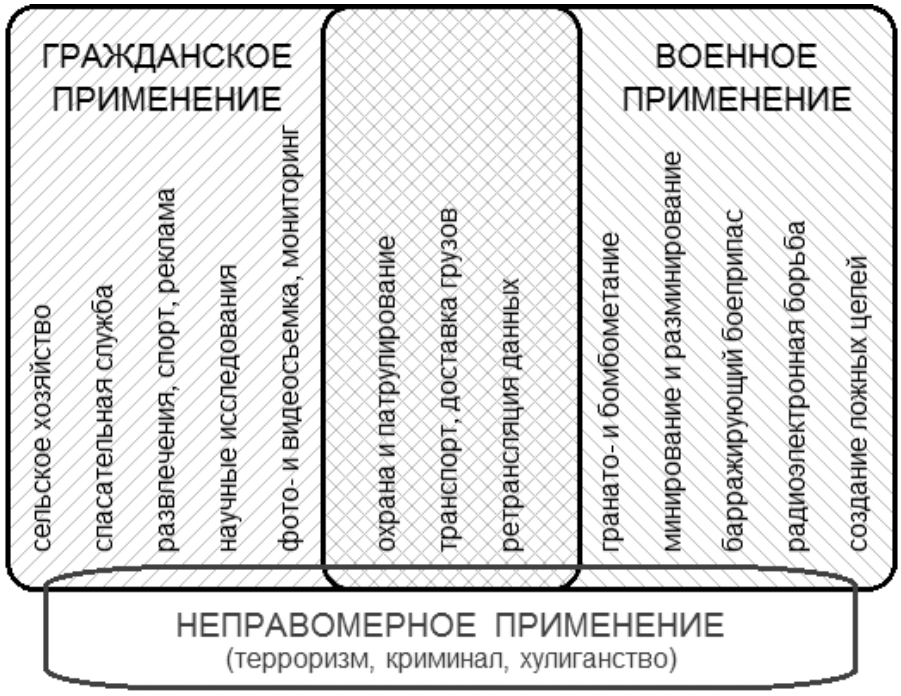

Рис. 3. Структура применения дронов

времени на пульт управления. Это так называемые «FPV-дроны» (First Person View – в переводе с английского – вид от первого лица). Основная особенность – использование оператором помимо обычного телевизионного канала очков виртуальной реальности (VR-очков) [4].

Благодаря своим оптимальным характеристикам, дроны вертолетного типа практически вытесняют остальные типы (может быть, за исключением тяжелых аппаратов самолетного типа).

Расширение сфер применения дронов, а, следовательно, и массовое производство привело к их удешевлению. Так, например, цена FPV-дронов составляет несколько десятков тысяч рублей, а в категории легких дронов – начинается с пары тысяч. Дешевизна и относительная простота конструкции и управления способствует вовлечению населения (молодежи) в новое увлечение (развлечение) – в создание и программирование дронов, а также в участие в конкурсах и различных соревнованиях.

С началом российской Специальной военной операции стало очевидно, что FPV-дроны стали одним из самых эффективных и дешевых вооружений. Дроны уверенно заняли нишу основного оружия на опера-тивно-тактическом уровне, потребовало небывалого расширения их производства. В этих условиях созданием и производством дронов приходится заниматься не только крупным фирмам и конструкторским бюро, но и многочисленным изобретателям-энтузиастам, изготавливающим аппараты практически «в полевых условиях». Разработки сразу проходят проверку в бою, после чего, согласно пожеланиями военных, подвергаются необходимым изменениям конструкции или корректировкам программного обеспечения, в целом подтверждая свои высокие качества.

Государство уделяет должное внимание дронам: в соответствии с потребностями появилась новая специальность – оператор FPV-дронов; в 2024 году начал свою работу национальный проект по развитию беспилотных авиационных систем; выделяются средства на обучение молодежи управлению дронами.

Необходимо отметить, что кроме прогресса в сфере БПЛА существует и значительный негатив, состоящий в противоправном использовании дронов. Резко увеличивающееся число произведенных аппаратов, значительная часть которых является неучтенными; постоянное совершенствование конструкции; расширение возможностей; отработанные тактики применения; низкая заметность; легкость управления; значительное число обученных операторов; отсутствие некоторых правовых норм не могут не привести к нарушению закона.

В криминологии известны похожие примеры, когда возникновение вооруженных конфликтов (и особенно их завершение) при наличии организованной преступности и пробелах в законодательстве влекут за собой неконтролируемое распространение оружия, боеприпасов и взрывных устройств. Вкупе с большим числом свободных обученных специалистов это привело к массе трагических ситуаций: заказные убийства, криминальные взрывы, ранения из-за неосторожного обращения с опасными предметами и т.п.

Для использования дронов в криминальных целях, некоторые из них даже не придется переделывать. Прежде всего, это касается «универсальных» конструкций, успешно используемых и в гражданской и военной сфере (рис. 3). Другие БПЛА могут дорабатываться, а определенная часть – специально выполняться под криминальные и террористические задачи. Такие задачи известны [3]: ведение постоянного наблюдения; доступ за охраняемые периметры; проникновение защищаемые помещения; точечное уничтожение отдельных важных персон; доставка (заброска) различных средств поражения; нанесение повреждений сооружениям, памятникам культуры, объектам инфраструктуры и подвижному составу; пермещение запрещенных средств; распыление опасных веществ; препятствование организации воздушного движения и т.д.

Угрозы безопасности информации и объектам информатизации

Что касается угроз безопасности информации, то применение дронов (чаще всего неправомерное) в составе технических каналов утечки информации только расширяет этот ряд.

Первые подобные эксперименты проводились полвека назад. Была разработана электромеханическая стрекоза со встроенным радиомикрофоном. Ввиду невысокой

энерговооруженности характеристики прообразов нынешних дронов были невысоки.

Сегодня проблемы увеличения емкости аккумуляторов во многом решены, и применение дронов может создавать широкий спектр информационных угроз. Некоторые такие угрозы очевидны. Это заброска «жучков», фото- и видеосъемка папарацци, наблюдение за частной жизнью и др. Другие только начинают оформляться либо уже скрыто существуют, но ввиду высокой степени закрытости (в сфере шпионажа, псевдошпионажа, промышленного шпионажа) просто нет никаких сведений.

Пока в статистических данных и в специальной литературе по защите информации и информационной безопасности, даже наиболее свежей, нет упоминания про применение дронов при слежке за человеком [5]. Но то, как дроны могут модифицировать технические каналы утечки информации и создать угрозы безопасности информации и объектам информатизации (ОИ) можно смоделировать. Примерный перечень возможных негативных ситуаций будет выглядеть следующим образом.

1. Фото- и видеосъемка в контролируемой зоне (КЗ) объекта информатизации (рис. 4). БПЛА, в первую очередь малые, ввиду слабой заметности могут достаточно просто проникать в КЗ. Более тяжелые и оснащенные сильной оптикой способны делать снимки на подлете к КЗ.

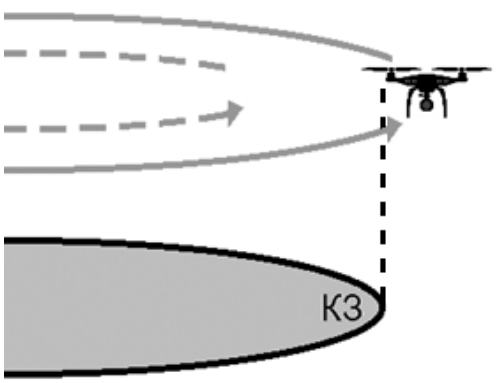

Рис. 4. Схема применения дрона для фото- и видеосъемки в контролируемой зоне (с заходом и без захода в нее)

2. Ретрансляция сигнала от устройства негласного съема информации (закладочного устройства, радиомикрофона), установленного на интересующем объекте (рис. 5). Ввиду того, что дрон может подлетать непосредственно к границе КЗ, радиопередающая часть закладки может быть выполнена менее мощной (и, соответственно, менее габаритной). Из-за этого поисковые мероприятия могут быть значительно затруднены, а для отлетевшего ретранслятора – вообще бесполезны.

Эта схема подходит и для сеансового приема информации, записанной ранее диктофоном (периодические подлеты дрона к границе КЗ).

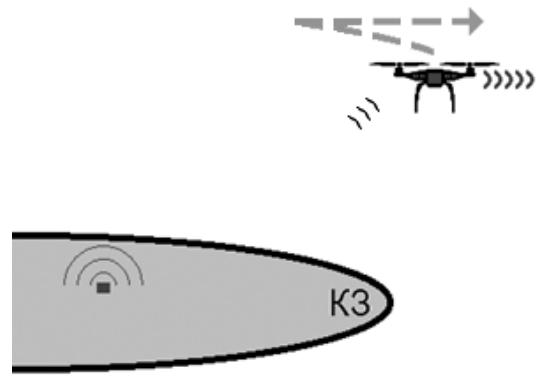

Рис. 5. Схема применения дрона для ретрансляции данных от устройств съема информации

3. Доставка различных устройств съема информации в зоны, где доступ человека затруднен, и в т.ч. не включенные ранее в КЗ (рис. 6).

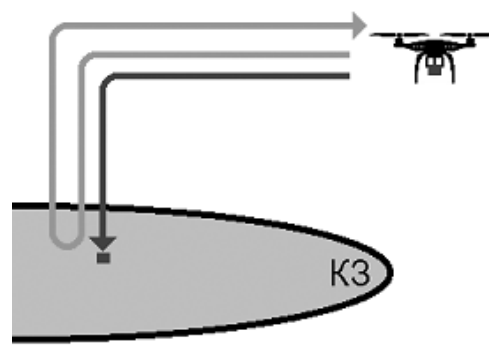

Рис. 6. Схема доставки различных устройств съема информации

4. Доставка в КЗ (или к границе КЗ) другого беспилотного мобильного средства (например, мобильного робота), способного самостоятельно перемещаться по поверхности до необходимой точки (удобной с точки зре-

ния съема или блокировки информации) (рис. 7).

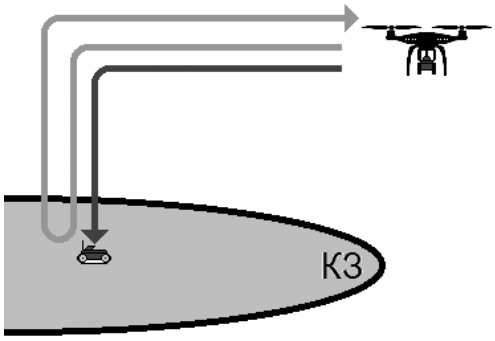

Рис. 7. Схема доставки беспилотного мобильного средства для съема или блокировки информации

5. Пролет дрона в КЗ с последующим превращением в устройство съема информации или источник электропитания (аналог дрона-камикадзе) (рис. 8).

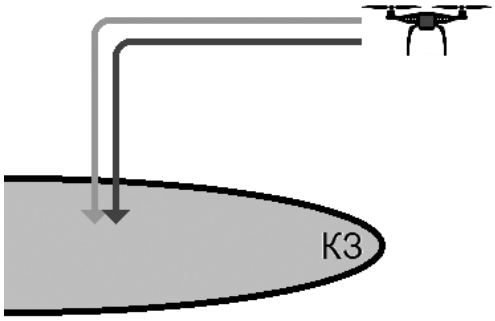

Рис. 8. Схема пролета дрона в КЗ с последующим превращением в устройство съема информации или источник электропитания

6. Пролет в КЗ с целью изъятия (кражи) носителей информации (документов, образцов и отходов производства) (рис. 9).

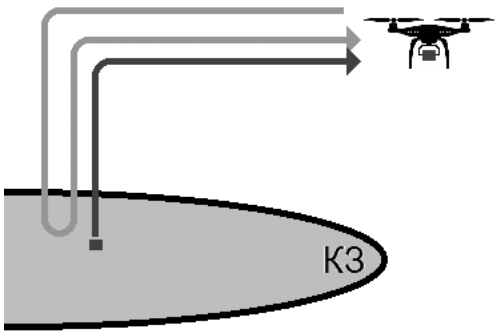

Рис. 9. Схема изъятия дроном носителей информации

7. Подавление сетей связи и цифровых каналов передачи данных (блокираторы, глушилки), как с заходом в КЗ, так и без этого (рис. 10).

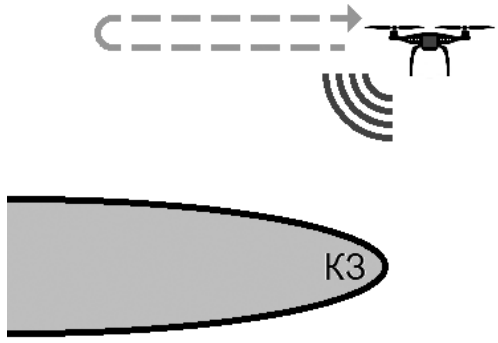

Рис. 10. Схема подавления дроном сетей связи и цифровых каналов пере-дачи данных

8. Различные варианты использования группы (роя) дронов, как в техническом, так и в тактическом плане, например, для отвлечения или перегрузки систем защиты (рис. 11).

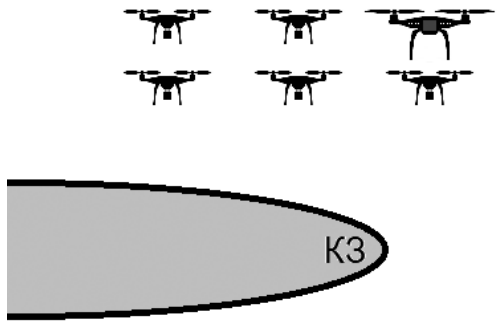

Рис. 11. Схема использования группы дронов

9. Столкновения дронов (в т.ч. случайные) объектами информатизации, ЛЭП, электрораспределительными устройствами (рис. 12). С повреждением устройств, линий, с отключением связи или электропитания.

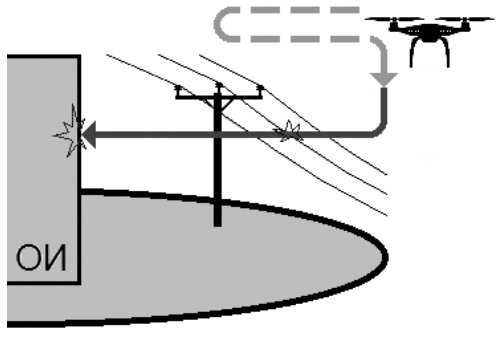

Рис. 12. Схема столкновений дронов (в т.ч. случайных) объектами информатизации, ЛЭП и т.п.

10. Сбрасывание различных предметов, листовок, фольги (или иных электропроводящих материалов над ЛЭП) (рис. 13). С нарушением работы различных устройств, с короткими замыканиями в ЛЭП и открытых распределительных электроустановках.

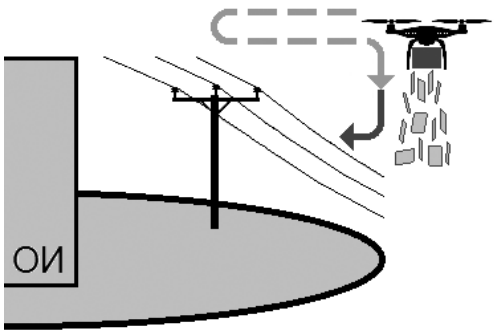

Рис. 13. Схема сбрасывания дронами фольги, листовок

11. Создание надписей на различных поверхностях (рис. 14). В зависимости от обстоятельств (как и сбрасывание листовок) может быть расценено правонарушением или преступлением (например, с антиконституционными призывами). По подобной схеме возможно и проецирование видеоинформации.

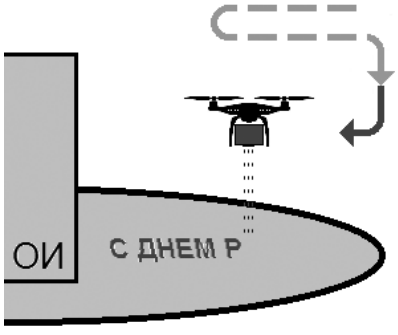

Рис. 14. Схема создания дронами надписей на различных поверхностях

12. Громкое звуковещание (с хулиганскими намерениями или для отвлечения сотрудников безопасности) (рис. 15).

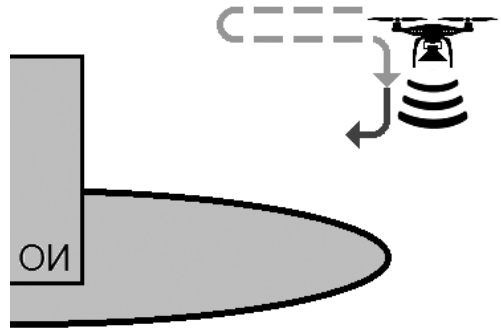

Рис. 15. Схема громкого звуковещания (например, для отвлечения)

Меры нейтрализации угроз

Обнаружить и нейтрализовать дроны достаточно сложно. Они постоянно совершенствуются, что делает перечисленные угрозы еще более актуальными. Поэтому необходимы надежные меры защиты от дронов. Их можно условно разделить на пассивные и активные (представлены на рис. 16). К пассивным мерам можно отнести организационно-правовые (требования законодательства и нормативных правовых актов; процедуры лицензирования; своевременное информирование) и инженерно-строительные (создание защищенных сооружений и специальных конструкций), а к активным мерам – реальное физическое противодействие – обнаружение; остановка; перехват управления; захват; ликвидация. Обнаружение может быть акустическим, оптическим, радарным и радиочастотным, а также их комбинацией. Противодействие может осуществляться при помощи радиоэлектронного подавления систем навигации и радиосвязи; воздействия СВЧ-излучения (для функционального поражения электроники дронов); перехвата (захвата) с использованием специальных дронов-перехватчиков, клейких и вязких аэрозолей, специально подготовленных птиц. В крайних случаях это может быть поражение при помощи огнестрельного оружия (прежде всего – дробового), лазерных систем, горючих химических смесей и т.п. [3, 6-8].

Указанный спектр мер противодействия в основном используется в военных условиях. Для гражданской сферы он сужается до разработки антидроновых систем с модуля-

ми направленной генерации помех. Характерным примером является постоянно совершенствующийся программно-аппаратный комплекс Kaspersky Antidrone, основанный на искусст-венном интеллекте и нейронных сетях, а также ему подобные системы [9].

Заключение

1. Дроны, несмотря на инновационное их применение в различных сферах, в других – могут становиться не только серьезными террористическими и криминальными угрозами, а и угрозами безопасности информации и объектам информатизации.

2. Несмотря на единичные зарегистрированные случаи противоправного использования дронов, уровень риска реализации таких угроз будет возрастать в связи с постоянным развитием науки и технологий, а также с происходящими социальными процессами (вооруженные конфликты, массовое хобби – конструирование и управление дронами и др.). При этом количественные показатели уровень риска можно рассчитать по появляющимся новым методикам [10].

3. Противоправное применение дронов во многом требует переосмысления некоторых базовых понятий информационной безопасности (контролируемая зона, физическая защита информации и др.).

4. Объекты информатизации и инфраструктуры в настоящее время требуют мер защиты от опасного использования дронов, которые заключаются в появлении новых специальных инженерно-строительных и конструкторских решений, а также в разработке программно-технических антидроновых систем.

5. Важным фактором, сдерживающим от неправомерного применения дронов, должно стать своевременное принятие необходимых норма-тивных правовых актов в сфере регламентации оборота беспилотных мобильных средств с последующим созданием эффективных механизмов их реализации.

6. Всё вышеописанное относительно дронов в определенной мере справедливо и для всей группы беспилотных мобильных средств. Поэтому можно заранее подготовить необходимые средства и планы противодействия возможным угрозам.

Рис. 16. Классификация средств противодействия противоправному применению дронов

Литература

1. Беспилотная авиация: терминология, классификация, современное состояние / В.С. Фетисов, Л.М. Неугодникова, В.В. Адамовский, Р.А. Красноперов; Под ред. В.С. Фетисова. – Уфа: ФОТОН, 2014. – 217 с.

2. Костюченко К. Л., Фараносов Д. А. Беспилотные мобильные средства: инновации и угрозы // Инновационный транспорт. 2024. №1 (50). С. 36-41.

3. Макаренко С.И., Тимошенко А.В., Васильченко А.С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный аппарат как объект обнаружения и поражения // Системы управления, связи и безопасности. 2020. № 1. С. 109-146.

4. Меринов К. FPV-дроны: технология, тактическое применение и будущее // Деловая газета «Взгляд». 15 сентября 2023 г. [Электронный ресурс]. URL: https://vz.ru/information/2023/9/15/1230301.html (дата обращения: 25.10.2023).

5. Новиков В.К., Краснов М.Г., Рекунков И.С. Средства, технологии, системы и технические каналы утечки информации для осуществления киберслежки за человеком и его деятельностью. – М.: Горячая линия – Телеком, 2023. – 160 с.

6. Макаренко С. И., Тимошенко А. В. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 2. Огневое поражение и физический перехват // Системы управления, связи и безо-пасности. 2020. № 1. С. 147-197.

7. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101-175.

8. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 4. Функциональное поражение сверхвысокочастотным и лазерным излучениями // Системы управления, связи и безопасности. 2020. № 3. С. 122-157.

9. Kaspersky Antidrone – экосистема мониторинга и защиты от дронов // Лаборатория Касперского [Электронный ресурс]. URL: https:// antidrone.kaspersky.com/ru/ (дата обращения: 30.01.2025).

10. Повышев А. А., Соколов А. Н., Мищенко Е. Ю. Универсальная классификация угроз безопасности информации и её применение для разработки модели угроз и оценки рисков // Вестник УрФО. Безопасность в информационной сфере. 2023. № 3(49) С. 68–80.

References

1. Bespilotnaya aviaciya: terminologiya, klassifikaciya, sovremennoe sos-toya-nie / V.S. Fetisov, L.M. Neugodnikova, V.V. Adamovskij, R.A. Krasnope-rov; Pod red. V.S. Fetisova. – Ufa: FOTON, 2014. – 217 s.

2. Kostyuchenko K. L., Faranosov D. A. Bespilotnye mobil'nye sredstva: innovacii i ugrozy // Innovacionnyj transport 2024. № 1 (50). S. 36-41.

3. Makarenko S.I., Timoshenko A.V., Vasil'chenko A.S. Analiz sredstv i sposobov protivodejstviya bespilotnym letatel'nym apparatam. CHast' 1. Bes-pilotnyj letatel'nyj apparat kak obekt obnaruzheniya i porazheniya // Sistemy upravleniya, svyazi i bezopasnosti. 2020. № 1. S. 109-146.

4. Merinov K. FPV-drony: tekhnologiya, taktic heskoe primenenie i bu-dushchee // Delovaya gazeta «Vzglyad». 15 sentyabrya 2023 g. [Elektronnyj resurs]. URL: https://vz.ru/information/2023/9/15/1230301.html (дата обращения: 25.10.2023).

5. Novikov V.K., Krasnov M.G., Rekunkov I.S. Sredstva, tekhnologii, sistemy i tekhnicheskie kanaly utechki informacii dlya osushchestvleniya kiber-slezhki za chelovekom i ego deyatel'nost'yu. – M.: Goryachaya liniya – Tele-kom, 2023. – 160 s.

6. Makarenko S. I., Timoshenko A. V. Analiz sredstv i sposobov protivodejstviya bespilotnym letatel'nym apparatam. CHast' 2. Ognevoe porazhenie i fizicheskij perekhvat // Sistemy upravleniya, svyazi i bezopasnosti. 2020. № 1. S. 147-197.

7. Makarenko S. I. Analiz sredstv i sposobov protivodejstviya bes-pilotnym letatel'nym apparatam. CHast' 3. Radioelektronnoe podavlenie sistem navigacii i radiosvyazi // Sistemy upravleniya, svyazi i bezopasno-sti. 2020. № 2. S. 101-175.

8. Makarenko S. I. Analiz sredstv i sposobov protivodejstviya bes-pilotnym letatel'nym apparatam. CHast' 4. Funkcional'noe porazhenie sverhvy-sokochastotnym i lazernym izlucheniyami // Sistemy upravleniya, svyazi i bezopasnosti. 2020. № 3. S. 122-157.

9. Kaspersky Antidrone – ekosistema monitoringa i zashchity ot dronov // Laboratoriya Kasperskogo [Elektronnyj resurs]. URL: https:// anti-drone.kaspersky.com/ru/ (дата обращения: 25.10.2023).

10. Povyshev A. A., Sokolov A. N., Mishchenko E. YU. Universal'naya klassifi-kaciya ugroz bezopasnosti informacii i eyo primenenie dlya razrabotki mo-deli ugroz i ocenki riskov // Vestnik UrFO. Bezopasnost' v informaci-onnoj sfere. 2023. № 3(49) S. 68–80.

КОСТЮЧЕНКО Константин Леонидович, кандидат технических наук, доцент кафедры «Информационные технологии и защита информа-ции» федерального государственного бюджетного образовательного учреждения высшего образования «Уральский государственный университет путей сообщения». 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: KKostyuchenko@usurt.ru.

ВАНДЫШЕВ Иван Сергеевич, аспирант кафедры «Информационные технологии и защита информации» федерального государственного бюджетного образовательного учреждения высшего образования «Уральский государственный университет путей сообщения». 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: vandyschev.iwan@yandex.ru

KOSTYUCHENKO Konstantin Leonidovich, Candidate of Technical Sciences, Associate Professor of the Department of Information Technology and Information Protection of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, Kolmogorova st., 66. E-mail: KKostyuchenko@usurt.ru.

VANDYSHEV Ivan Sergeevich, postgraduate student of the Department of Information Technology and Information Protection of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, Kolmogorova st., 66. E-mail: vandyschev.iwan@yandex.ru.