УДК 004.056

А.В. Винокуров
(Краснодарское высшее военное училище им. генерала армии С.М. Штеменко;
e-mail: vav73@rambler.ru)

ТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Статья посвящена решению научной задачи обеспечения техносферной безопасности комплексов с беспилотными летательными аппаратами (КБЛА), которая рассматривается во взаимодействии с общей теорией информационной безопасности, а БЛА как субъект угроз и как объект, на который направлены деструктивные воздействия нарушителя. Предлагается комплексное решение задачи обеспечения техносферной безопасности КБЛА.

Ключевые слова: беспилотный летательный аппарат, техносферная безопасность, субъект и объект угроз, терроризм.

В настоящее время практически во всех современных вооружённых конфликтах применяются комплексы с ***беспилотными летательными аппаратами (КБЛА)***, представляющие собой совокупность взаимоувязанных в единую функциональную систему БЛА и наземных технических средств, обеспечивающих их боевое применение в воздухе и техническую эксплуатацию на земле [1].

Указом Президента Российской Федерации от 7 мая 2012 года № 603 "О реализации планов (программ) строительства и развития ВС РФ, других войск, воинских формирований и органов и модернизации оборонно-промышленного комплекса" развитие КБЛА и роботизированных ударных комплексов определено в качестве приоритетных направлений.

Современные КБЛА способны выполнять различные задачи, включая воздушную разведку общего и специального назначения, радиоэлектронную борьбу, целеуказание системам оружия с лазерным наведением и др. [2].

В тоже время, развитие и совершенствование новых информационных технологий приводит и к появлению новых угроз, включая использование БЛА для осуществления террористических актов. Например, возможность достижения большой дальности и приемлемой точности БЛА за счёт недорогих и доступных технических решений при достаточно низкой эффективности систем противовоздушной обороны по противодействию малогабаритным и низколетящим БЛА.

Обеспечение информационной безопасности КБЛА в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трёх составляющих проблем [3]:

- защита циркулирующей в КБЛА информации от дестабилизирующего воздействия внешних и внутренних угроз;
- защита элементов КБЛА от дестабилизирующего воздействия внешних и внутренних информационных угроз;
- защита внешней среды от угроз со стороны БЛА.

БЛА, являясь элементом техносферы, при определённых негативных воздействиях на них могут угрожать её безопасности. Рассматривая *техносферную безопасность* как защищённость техносферы от стихийных бедствий, техногенных аварий, катастроф, пожаров и негативных антропогенных воздействий (терроризма, ошибок) [4], можно выделить взаимосвязи проблемы техносферной безопасности КБЛА с общей проблемой информационной безопасности КБЛА, что графически представлено на рис. 1.

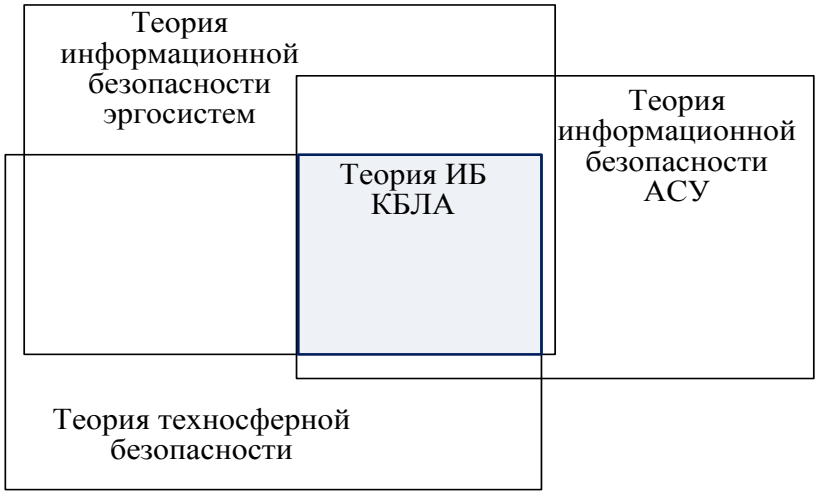

Рис. 1. Система взаимодействия теорий информационной и техносферной безопасности

Решение проблемы защиты КБЛА в рамках техносферной и информационной безопасности предлагается путём рассмотрения БЛА как средства для совершения техногенных аварий и террористических актов, где БЛА выступает субъектом угроз, а с другой стороны рассматривать его как объект, на который направлены деструктивные воздействия [5]. Примерный перечень угроз применения БЛА в террористических целях представлен на рис. 2.

Целью статьи является формирование системы взглядов на проблему техносферной безопасности КБЛА со стороны угроз террористического характера и выработка предложений и рекомендаций по их нейтрализации.

Проблема информационной безопасности КБЛА включает в себя взаимосвязанные нормативные, правовые, организационные, технические и научно-методические составляющие.

Нормативно-правовая составляющая проблемы определяется наличием и содержанием системы документов федерального, ведомственного и регионального уровня. Одной из задач Стратегии экономической безопасности Российской Федерации на период до 2030 г. является повышение уровня безопасности и антитеррористической защищённости критически важных и потенциально опасных объектов. Основными нормативными и правовыми документами в рассматриваемой области являются: Федеральный закон РФ от 28 декабря 2010 г. № 390-ФЗ "О безопасности", Федеральный закон РФ от 6 марта 2006 г. № 35-ФЗ "О противодействии терроризму", Федеральный

закон РФ от 9 февраля 2007 "О транспортной безопасности", Стратегия национальной безопасности РФ до 2020 г., Поручение Правительства РФ от 7 июля 2001 г. "О создании методик категорирования объектов науки, промышленности и жизнеобеспечения по степени их потенциальной опасности и диверсионно-террористической уязвимости".

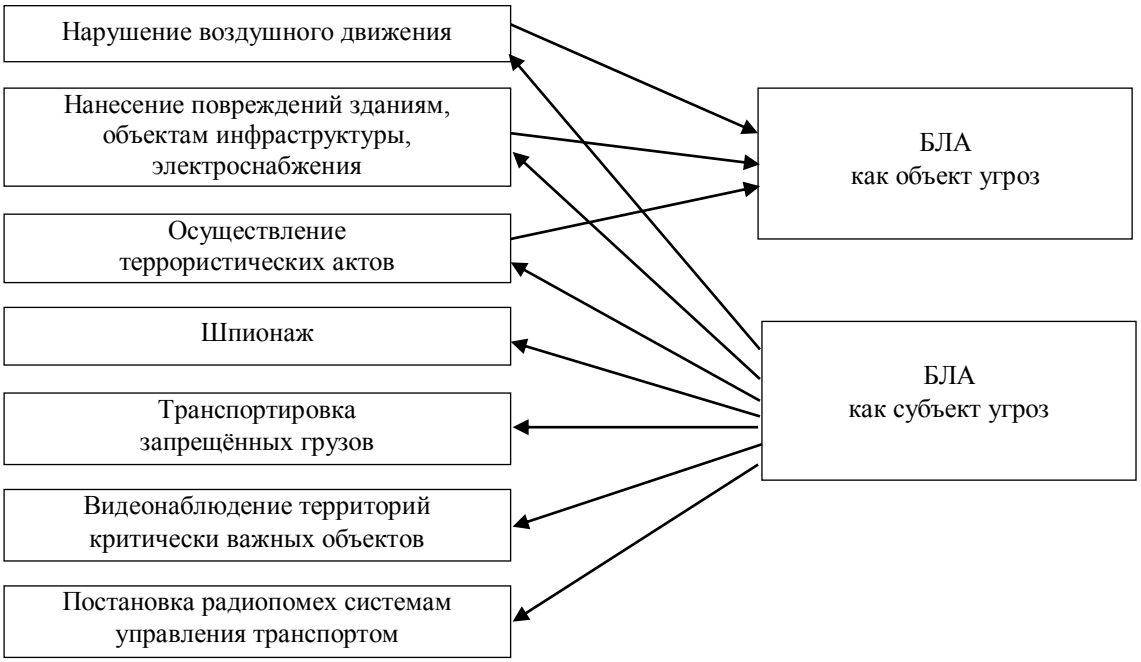

Рис. 2. Угрозы применения БЛА в террористических целях

Задачами совершенствования нормативно-правовой составляющей являются:

- формирование облика беспилотного транспорта;
- совершенствование нормативного регулирования;
- совершенствование государственной информационной системы обеспечения транспортной безопасности;
- совершенствование законодательства в сфере ответственности за нарушение правил эксплуатации БЛА и применения их для совершения противоправных действий.

Организационные меры:

- построение механизма регистрации БЛА;
- совершенствование разрешительной системы управления БЛА;
- построение системы классификаторов и опознавательных знаков, определяющих принадлежность БЛА;
- выделение диапазона частот для БЛА различного назначения в зависимости от их класса;
- унификация радиотракта управления БЛА;
- построение системы ограничений по характеристикам, условиям и территориям применения;
- определение перечня территорий, для ограничения применения БЛА.

Основные способы противодействия БЛА нарушителя можно классифицировать по решению задач их обнаружения и нейтрализации:

1. Обнаружение БЛА:

- радиолокация;
- обнаружение электромагнитного фона;
- сканирование акустических шумов;
- визуальное и инфракрасное наблюдение.

2. Нейтрализация БЛА:

- постановка радиопомех;
- подавление или искажение навигационного поля;
- инфракрасное подавление видеоаппаратуры БЛА;
- постановка воздушных вихревых завес вдоль защищаемых объектов;
- физическая нейтрализация (установка защитных сетей, применение специальных БЛА и вооружения и т.д.).

Реализовать предложенные способы противодействия возможно путём разработки и применения следующих технических средств:

- Стационарные подавители радиолинии БЛА.
- Переносные подавители радиолинии БЛА.
- Акустические детекторы.
- Комплексы искажения (подавления) навигационного поля.
- Детекторы электромагнитного поля.
- Устройства и средства физической нейтрализации.

При рассмотрении *БЛА как объектов угроз* [6] необходимо обеспечить защиту информации, циркулирующей в их радиолиниях, а именно, информацию управления, телеметрическую информацию, информацию с бортовых целевых нагрузок, навигационную информацию.

Задачу обоснованного выбора механизмов защиты можно решать на основе методов принятия решений, например, метода анализа иерархии и др.

Построим модель "с полным перекрытием", представляющую собой триаду "угрозы – уязвимости – объекты защиты" в виде трёхдольного графа, изображённою на рис. 3.

Предлагаемая модель включает три множества:

$Y = \{y_i\}$ – множество угроз безопасности;

$O = \{o_j\}$ – множество объектов (ресурсов) КБЛА;

$X = \{x_r\}$ – множество уязвимых мест КБЛА, определяемое подмножеством декартова произведения $Y \cdot O$: $x_r = \{< y_i, o_j >\}$.

Выбор множества механизмов защиты $S = \{s_k\}$ определяется целью перекрытия всех возможных рёбер в графе $\{<Y, X, O>\}$.

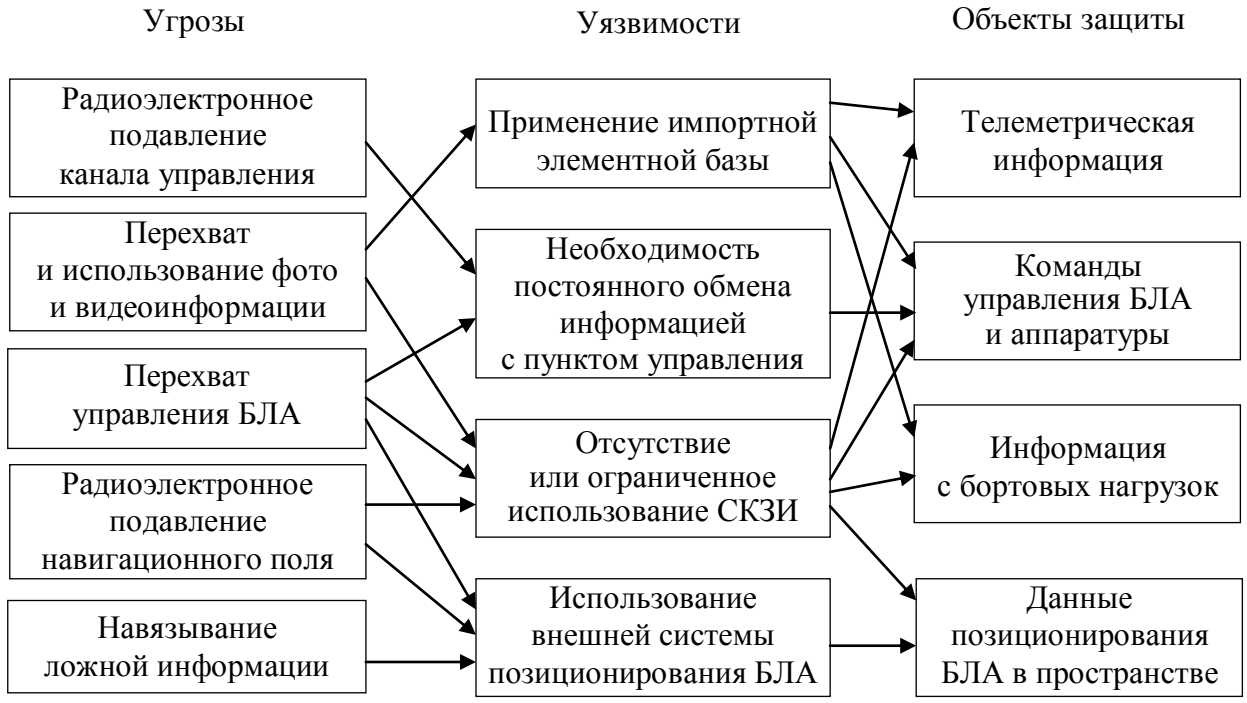

Рис. 3. Модель "угрозы – уязвимости – объекты защиты"

Для обоснованного применения механизмов защиты необходимо оценить уровень угроз на КБЛА. В табл. 1 представлены результаты ранжирования угроз по величине потенциального ущерба.

Таблица 1

Ранжирование угроз КБЛА по величине потенциального ущерба

Уровень	Угрозы	Степень угрозы
1	Раскрытие содержания общедоступной видеоинформации	Малая
2	Раскрытие телеметрической информации	Малая
3	Раскрытие протоколов взаимодействия	Малая
4	Искажение телеметрической информации	Средняя
5	Искажение навигационного поля	Средняя
6	Подавление командной информации	Средняя
7	Раскрытие содержания видеоинформации, ограниченного распространения	Высокая
8	Навязывание ложного навигационного поля	Высокая
9	Навязывание ложной командной информации	Высокая

Научно-методическая составляющая проблемы обеспечения техносферной безопасности КБЛА определяет следующие направления:

1. Формирование принципов обеспечения техносферной и информационной безопасности КБЛА.

В данном направлении можно выделить следующие принципы:

конечной цели (создания системы защиты информации КБЛА для достижения максимальной эффективности функционированию КБЛА, то есть сохранения требуемого качества информационного обеспечения, где под качеством понимается не только обеспечение его защищённости, но и ценности);

обоснованности защиты информации (определение информационных

потоков, подлежащих защите, нахождение компромисса в защите исходя из ресурсов надсистемы);

гарантированного результата (защита информации должна обеспечивать её требуемое качество в любых условиях обстановки, включая неопределённость влияющих факторов);

оптимального перераспределения сил (затраты на защиту должны соответствовать уровню угроз и вероятности их появления);

согласованности мер защиты (противодействие БЛА нарушителя должно носить целенаправленный характер и не влиять на функционирование легитимных средств).

2. Разработка моделей, методов и способов обнаружения БЛА, подавления радиолинии и физической нейтрализации БЛА.

По данному направлению для решения первой задачи (*БЛА – субъект угроз*) можно предложить следующую группу исследований:

- применение методов искусственного интеллекта для визуальной идентификации малоразмерных БЛА;
- совершенствование методов акустической идентификации БЛА;
- совершенствование методов подавления оптико-электронного оборудования БЛА;
- совершенствование методов перехвата управления БЛА;
- совершенствование методов радиоэлектронного подавления БЛА.

Для решения второй задачи (*БЛА – объект угроз*):

- применение криптографических методов защиты информации, например, на основе реализации криптографических чипов [7];
- разработка методов идентификации и защиты от навязывания ложной информации и искажения навигационного поля;
- совершенствование методов защиты от помех на физическом и канальном уровне обработки информации.

Выводы

Теоретической новизной является рассмотрение проблемы техносферной безопасности КБЛА во взаимодействии с общей проблемой информационной безопасности КБЛА. В результате двух аспектного рассмотрения КБЛА как субъекта и объекта угроз предложен комплекс нормативных, правовых, организационных, технических и научно-методических мер по обеспечению их техносферной безопасности.

Практическая значимость работы заключается в обоснованных предложениях и рекомендациях по построению системы обнаружения и нейтрализации БЛА нарушителя.

Литература

1. *Полтавский А.В., Жумабаева А.С., Бикеев Р.Р.* Многофункциональные комплексы беспилотных летательных аппаратов: развитие в системе вооружения // Надёжность и качество сложных систем. 2016. № 1 (13). С. 39-46.

2. *Скотников А.П., Якубов В.И., Шиховцев С.В.* Роль и место беспилотных комплексов в системе вооружения Российской армии // Военная мысль. № 4. 2007. С. 62-68.

3. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пос. для вузов. М.: Горячая линия – Телеком, 2004. 280 с.

4. *Ефремов С.В.* Управление техносферной безопасностью: краткий курс. СПб., 2013. 46 с. http://www.bzhd.spbstu.ru/docs/Upr.teh.bez.pdf.

5. *Винокуров А.В.* Разработка и совершенствование методов защиты информационного обеспечения комплексов с беспилотными летательными аппаратами как задача противодействия информационному терроризму // Матер. Южного форума информационной безопасности Инфофорум-Крым, 2017. https://infoforum.ru/conference/sevastopol-17.

6. *Винокуров А.В.* Анализ уязвимостей беспилотной авиационной системы и классификация угроз безопасности циркулирующей в ней информации // Матер. II всеросс. науч.-техн. конф. "Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения". СПб.: Военно-космическая академия им. А.Ф. Можайского, 2015. 44 с.

7. *Коцыняк М.А., Крибель А.М., Кузнецова В.В., Лаута О.С., Московченко В.М.* Подход к обеспечению защиты каналов управления робототехнических систем // Робототехника и техническая кибернетика. № 4 (17). СПб.: ЦНИИ РТК. 2017. С. 15-21.

Статья поступила в редакцию интернет-журнала 10 сентября 2017 г.

A.V. Vinokurov

ENSURING TECHNOSPHERIC SAFETY OF COMPLEXES WITH UNMANNED AERIAL VEHICLES

Information security complexes with unmanned aerial vehicles (UAVC) in the overall formulation of the problem can be achieved only by mutually linked solution of its three components, one of which is to protect the environment from threats from UAVC. The article is devoted to the solution of the scientific problem of the technospheric security of UAVC, which is considered in cooperation with the general theory of information security, and the UAV as a subject of threats and as an object to which the destructive effects of the offender are directed. This article outlines a comprehensive solution to the challenges of providing technospheric safety of UAVC through the development of models, methods and ways to detect UAV, suppression of radio and physical neutralization of UAV. The indicator of the probability of destructive impacts from the offender is proposed to use as a mathematical apparatus of the estimation of efficiency of application of protection measures. Variation in the choice of protection mechanisms, for example, according to the minimum cost criterion, will allow solve the problem of ensuring technospheric safety at a given level in accordance with the importance of the protected object.

Key words: unmanned aerial vehicle, technospheric safety, subject and object of threats, terrorism.

References

1. Poltavskii A.V., Zhumabaeva A.S., Bikeev R.R. *Mnogofunktsionalnye kompleksy bespilotnykh letatelnykh apparatov: razvitie v sisteme vooruzheniia* [Multifunctional complexes of unmanned aerial vehicles: development in the weapons system]. *Nadezhnost i kachestvo slozhnykh sistem*, 2016, no. 1 (13), pp. 39-45.

2. Skotnikov A.P., Iakubov V.I., Shikhovtsev S.V. Rol i mesto bespilotnykh kompleksov v sisteme vooruzheniia Rossiiskoi armii [The role and place of unmanned systems in the Russian army armament system]. *Voennaia mysl*, no. 4, 2007, pp. 62-68.

3. Maliuk A.A. *Informatsionnaia bezopasnost: kontseptualnye i metodologicheskie osnovy zashchity informatsii: ucheb. pos. dlia vuzov* [Information security: conceptual and methodological foundations of information security: textbook for high schools]. Moscow, Goriachaia liniia – Telekom Publ., 2004. 280 p.

4. Efremov S.V. *Upravlenie tekhnosfernoi bezopasnostiu: kratkii kurs* [Management of technospheric safety: a short course]. Saint Petersburg, 2013. 46 p. http://www.bzhd.spbstu.ru/docs/Upr.teh.bez.pdf.

5. Vinokurov A.V. *Razrabotka i sovershenstvovanie metodov zashchity informatsionnogo obespecheniia kompleksov s bespilotnymi letatelnymi apparatami kak zadacha protivodeistviia informatsionnomu terrorizmu* [Development and improvement of methods of protection of information support of complexes with unmanned aerial vehicles as a task of counteraction to information terrorism]. *Mater. Iuzhnogo foruma informatsionnoi bezopasnosti Infoforum-Krym* [Materials of the southern information security forum Infoforum-Crimea], 2017, https://infoforum.ru/ conference/sevastopol-17.

6. Vinokurov A.V. *Analiz uiazvimostei bespilotnoi aviatsionnoi sistemy i klassifikatsiia ugroz bezopasnosti tsirkuliruiushchei v nei informatsii* [Analysis of the vulnerabilities of the unmanned aviation system and classification of security threats of the information circulating in it]. *Mater. II vseross. nauch.-tekhn. konf. "Teoreticheskie i prikladnye problemy razvitiia i sovershenstvovaniia avtomatizirovannykh sistem upravleniia voennogo naznacheniia"* [Proceed. of the materials of the II all-Russian scientific and technical conference "Theoretical and applied problems of development and improvement of automated control systems for military purposes"]. Saint Petersburg, A.F. Mozhaysky Military-Space Academy Publ., 2015. 44 p.

7. Kotsyniak M.A., Kribel A.M., Kuznetsova V.V., Lauta O.S., Moskovchenko V.M. Podkhod k obespecheniiu zashchity kanalov upravleniia robototekhnicheskikh sistem [Approach to securing control channels of robotic systems]. *Robototekhnika i tekhnicheskaia kibernetika*, no. 4 (17), Saint Petersburg, Russian State Scientific Center for Robotics and Technical Cybernetics Publ.. 2017, pp. 15-21.