АНАЛИЗ УЯЗВИМОСТЕЙ КОМПЛЕКСОВ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ И КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ЦИРКУЛИРУЮЩЕЙ В НИХ ИНФОРМАЦИИ

Винокуров Александр Владимирович,
г. Краснодар, Россия, VAV73@rambler.ru

Аннотация. Рассматриваются угрозы информационной безопасности комплексов с беспилотными летательными аппаратами (КБЛА). На основе анализа функциональных возможностей БЛА и циркулирующих в них потоков информация определены объекты защиты и уязвимости КБЛА. Результаты исследования предлагается использовать для развития методологии системных исследований в области защиты информации, циркулирующей в КБЛА. Практическая направленность заключается в обоснованном формировании требований технического задания на проектирование и разработку БЛА и построения механизмов защиты циркулирующей в них информации.

Ключевые слова: информационная безопасность; комплекс с беспилотными летательными аппаратами; модель угроз.

Сведения об авторе: Винокуров А.В. к.т.н., доцент, докторант Краснодарского высшего военного училищ имени генерала армии С.М. Штеменко.

В настоящее время КБЛА используются для решения различных задач обеспечения обороноспособности государства, включая:

- воздушную разведку общего и специального назначения;
- радиоэлектронное подавление радиоэлектронных средств противника;
- целеуказание системам оружия и корректировку артиллерийского огня.

В условиях возможного осуществления информационного воздействия, результатом которого будет модификация его свойств как информационной системы, КБЛА могут являться объектом информационного противоборства [1]. Функционируя в условиях радиоэлектронной борьбы КБЛА потенциально подвержены угрозам, в том числе, направленным на нанесение ущерба его информационным ресурсам [2, 3]. Например, 4 декабря 2012 г. мировые СМИ, ссылаясь на информацию иранских источников, сообщили, что средства РЭБ Ирана посадили на востоке страны американский беспилотный аппарат RQ-170 Sentinel. В данном случае иранскими специалистами была использована уязвимость в системе управления БЛА, заключающаяся в обмене информацией с наземными пунктами управления и передачи данных внешней системы позиционирования БЛА в пространстве по открытым радиоканалам. Летом 2009 года американские войска обнаружили на ноутбуках иракских повстанцев программное обеспечение, позволяющее перехватывать специальную информацию с БЛА, которая передавалось в командные пункты по незашифрованным каналам связи. Приведенные примеры, а также анализ функциональных возможностей перспективных систем РЭБ США [2] позволяют сделать вывод о необходимости совершенствования системы защиты информации, циркулирующей в КБЛА. Данные обстоятельства обусловливают актуальность научной проблемы синтеза оптимальной по критерию информационной безопасности КБЛА специального назначения при ограничениях на ресурсы, выделяемые на цели защиты циркулирующей в ней информации.

Несмотря на достаточное количество публикаций по данному направлению они в основном ограничены тактико-техническими характеристиками и способами применения БЛА [4] или общими вопросами защиты информации и основными задачами разработки средств криптографической защиты информации (СКЗИ) [5].

Целью статьи является формальное обоснование степени защищенности КБЛА специального назначения, путем выявления ее уязвимостей для построения модели угроз безопасности информации, циркулирующей в них.

Модель угроз безопасности информации – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. Основной задачей модели является

научное обеспечение процесса разработки методов и средств защиты КБЛА за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта их технической реализации. Практическая значимость модели угроз заключается в ее направленности для детализации целей оценки угроз, которая включает:

– идентификацию уязвимых мест КБЛА;
– анализ вероятности угроз, направленных на использование таких уязвимых мест;
– оценку последствия успешного выполнения угрозы;
– оценку стоимости каждого вторжения;
– анализ стоимости возможных мер противодействия;
– выбор удовлетворительных механизмов защиты.

Исходя из анализа информационных потоков, циркулирующих в КБЛА, наибольший интерес представляет следующие информационные массивы:

– ключевая информация;
– команды управления БЛА и аппаратуры;
– данные позиционирования БЛА в пространстве;
– специальная информация (данные разведки, интеллектуальной СПР, команды управления в рамках боевой информационной системы);
– телеметрическая информация.

Уязвимость (ИС) – свойство ИС, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Анализ структуры и функциональной модели КБЛА позволил выявить следующие уязвимости:

– необходимость постоянного обмена информацией с наземными пунктами управления;
– использование внешней системы позиционирования БЛА в пространстве;
– открытые потоки телеметрической информации;
– отсутствие или ограниченное использование СКЗИ;
– высокая вероятность компрометации ключевой информации и СКЗИ;
– необходимость информационного взаимодействия с пилотируемыми летательными аппаратами (ПЛА).

Угрозы КБЛА рассмотрим через ущерб информации, циркулирующей в ее подсистемах, при этом под угрозой безопасности информации будем понимать совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Эффективная защита от потенциальных атак невозможна без их детальной классификации, облегчающей их выявление и задачу противодействия им.

Классификационным признаком предлагается рассмотреть степень риска, имеющая большое практическое значение, так как позволяет ранжировать уровень угроз по следующим классам:

– высокий – угрозы, успешная реализация которых позволяет атакующему немедленно получить доступ к управлению БЛА, перехватить и использовать специальную информацию БЛА;
– средний – угрозы, успешная реализация которых потенциально может дать атакующему доступ к БЛА или специальной информации БЛА;
– низкий – угрозы, при успешной реализации которых противник может получить сведения, облегчающие ему задачу перехвата управления БЛА или раскрытия содержания специальной информации.

На основе анализа угроз и уязвимостей КБЛА предлагается рассматривать применяемую для оценки рисков модель «с полным перекрытием», представляющую собой триаду «угрозы – уязвимости – объекты защиты». Угрозы, уязвимости и информационные ресурсы КБЛА, как объекты защиты, представлены на рисунке 1.

Оценка угроз по степени риска является не полной и целесообразно учитывать вероятностный характер возможности реализации угроз для нанесения ущерба информационным ресурсам КБЛА. Предлагается рассмотрение стратегий нарушителя для достижения поставленной цели:

– первого типа направлены на установление (раскрытие) языка информационного обмена Борт-Земля. Цель – получить специальную информацию КБЛА;
– второго типа направлены на навязывание ложной информации. В данном случае предполагается навязывание ложных команд управления с наземных пунктов управления, а также перехват и целенаправленное искажение навигационных данных (спуфинг-атака). Цель – перехват управления БЛА, навязывание ложной целевой информации;
– третьего типа направлены на срыв или ухудшение качества информационных взаимодействий путем создания агрессивной среды осуществления информационных взаимодействий, что достигается,

например, при постановке помех средствами радиоэлектронного подавления и др. Цель – затруднить или нарушить управление БЛА, искажение специальной информации;

– четвертого типа направлены на нарушение целостных характеристик объектов, в которых находится защищаемая информация. Данные стратегии обычно используются, когда отсутствуют возможности по реализации вышестоящих типов стратегий. Цель – нанесение ущерба системе путем воздействия на обеспечивающую ее инфраструктуру.

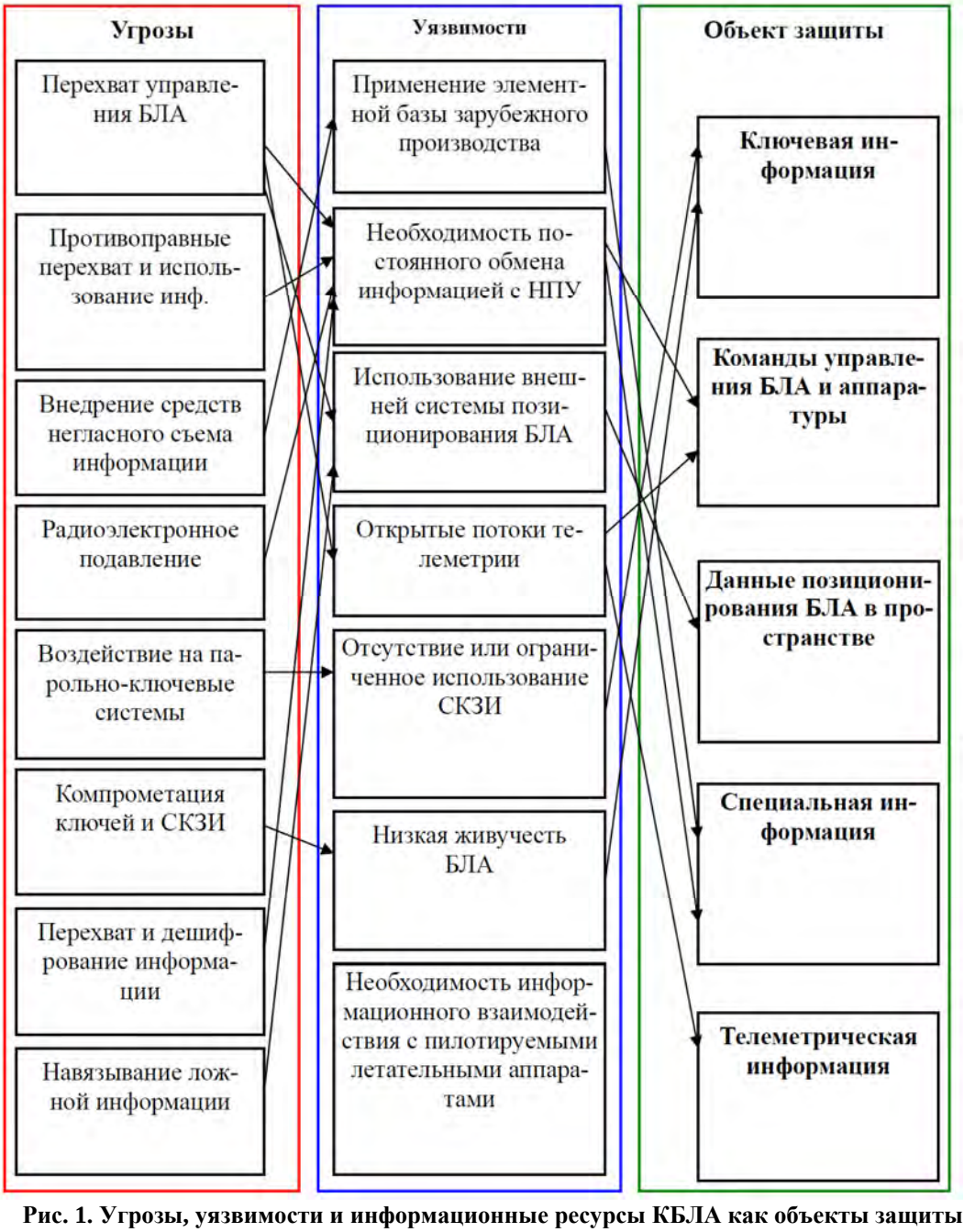

Рис. 1. Угрозы, уязвимости и информационные ресурсы КБЛА как объекты защиты

Стратегии нарушителя предполагают комплекс мер воздействия на ресурсы КБЛА и в первую очередь представляют угрозу безопасности защищаемой информации. В зависимости от типа стратегии предлагаются следующие критерии оптимальности мер противодействия, представленные в таблице 1.

Таблица 1

Реляционное представление стратегий противника и критериев оптимальности мер противодействия

Уровень	Тип стратегии	Сценарий выбора реализуемой стратегии нарушителем	Критерии оптимальности мер противодействия
Стратегия 1 типа	Нарушение конфиденциальности	Раскрытие шифров. Нарушение правил шифрования. Компрометация ключей до запуска БЛА или на НПУ. Перехват и статистическая обработка криптограмм. Вскрытие шифра в результате криптоанализа. Дешифрование специальной информации	Максимизация ожидаемого безопасного времени работы СКЗИ до взлома подсистемы защиты (T_o). Минимизация вероятности раскрытия ключа шифра (P_k). Минимизация вероятности дешифрования специальной информации (P_D).
Стратегия 2 типа	Нарушение имитостойкости	Перехват и модификация команд управления БЛА. Навязывание ложных команд управления БЛА. Вскрытие алгоритма и ключа обеспечения имитостойкости. Подавление и навязывание ложных навигационных данных.	Минимизация навязывания ложной информации ($P_{нав}$) Минимизация вероятности трансформации информации ($P_{тр.}$)
Стратегия 3 типа	Нарушение достоверного информационного взаимодействия	Радиоэлектронное подавление команд управления БЛА, телеметрических и навигационных данных. Нарушение правил вхождения в связь.	Минимизация вероятности искажения информационного символа ($P_{ош}$). Минимизация вероятности подавления информации ($P_{под.}$). Минимизация вероятности необнаруженных искажений ($P_{необ.}$) Минимизация времени доведения информации ($T_д$)
Стратегия 4 типа	Нарушение сохранности (работоспособности) подсистем БАС	Внедрение средств негласного съема информации и РПВ. Модификация ПО. Подмена, уничтожение, хищение наиболее важных компонентов КБЛА. Воздействие на элементы инфраструктуры: электропитание, линии связи и т.д.	Минимизация вероятности необнаружения закладочных устройств и несанкционированной модификации ПО ($P_{нм}$). Максимизация вероятности восстановления работоспособности устройств КБЛА ($P_в$)
	Нарушение регистрируемости		Минимизация вероятности незарегистрируемости факта воздействия и ошибок в подсистемах КБЛА ($P_{нр}$)

Таким образом, в результате проведенных исследований подтверждена актуальность задачи обеспечения информационной безопасности КБЛА, предложены элементы модели угроз безопасности информации. Рассмотренные стратегии, реализуемые нарушителем, предлагается учитывать при разработке научно-методического аппарата рациональной защиты информации с учетом ограниченных ресурсов КБЛА, выделяемых на их защиту, а предложенные критерии оптимальности мер противодействия применять при оценке эффективности комплексной защиты для проектируемых и функционирующих КБЛА.

Литература

1. Манойло А.В. Государственная информационная политика в особых условиях: монография. М. : Изд. МИФИ. 2003. 306 с.

2. Круглов Е. Перспективы развития американских авиационных средств РЭБ и тактика их применения в современных вооруженных конфликтах // Зарубежное военное обозрение № 2 (803). 2014. М: Красная звезда. С. 57–63.

3. Цветнов В.В., Демин В.П., Куприянов А.И. Радиоэлектронная борьба: радиомаскировка и помехозащита: Учебное пособие. М.: Изд-во МАИ. 1999. 240 с.

4. Казарьян Б.И. Беспилотные аппараты: способы применения в составе боевых систем / Б.И. Казарьян // Военная мысль. 2012. № 3. С. 21–26.

5. Сашников Т.К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и легкого класса в специализированных АСУ / Сборник трудов Всероссийской научно-технической конференции «Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения» [под общ. Ред. В.В. Алейника, К.Е. Легкова, В.Д. Боева и др.; ответст. За вып.: С.В. Чернышев]. СПб.: ВКА имени А.Ф. Можайского. 2013. С. 247–251.

VULNERABILITY ANALYSIS COMPLEXES WITH UNMANNED AERIAL VEHICLES AND CLASSIFICATION OF SECURITY THREATS CIRCULATING INFORMATION IN THEM

Vinokurov Alexander Vladimirovich,
Krasnodar, Russian, VAV73@rambler.ru

Abstract. This article discusses the threats to information security systems with unmanned aerial vehicles (CUAV). Based on the analysis functionality of UAVs and circulating them in the flow of information identified objects of protection and vulnerability CUAV. Results of the study are encouraged to use the system for the development of the methodology of research in the field of information circulating in CUAV. Practical orientation is grounded formation of the requirements specification to design and develop UAV and build protection mechanisms of circulating information in them.

Keywords: information security, complex with unmanned aerial vehicles, threat model.

References

1. Manoilo A.V. State information policy in special conditions: monograph. - M.: Publishing house. MEPI, 2003, 306 p.
2. Round E. Prospects for the development of American aviation electronic warfare tactics and their application in contemporary armed conflicts / Foreign Military Review number 2 (803), 2014 M: Krasnay zvezda, pp. 57-63.
3. Tsvetnov V.V., Demin V.P., Kupriyanov A.I. Electronic warfare: deception and anti-jamming: Textbook. M .: Publishing House of the Moscow Aviation Institute, 1999. - 240 p.
4. Kazaryan B.I. Unmanned vehicles: methods of application as part of combat systems / B.I. Kazaryan // Moscow: Voennay misl, 2012, No. 3, pp. 21-26.
5. Sashnikov T.K. On the issue of information security unmanned aircraft systems with small aircraft and light class in specialized ACS / Proceedings of the All-Russian Scientific and Technical Conference "Theoretical and applied problems of development and improvement of automated control systems for military use" / under total. Ed. V.V. Aleynik, K.E. Legkov, V.D. Boev, etc .; otvetst. For MY .: SV Chernyshev. Spb .: MSA named after A.F. Mozhaisky, 2013, pp. 247-251.

Information about author: Vinokurov A.V., doctoral student, Krasnodar Higher Military School named after Army General S.M. Shtemenko.