УДК: 004.056 DOI: 10.53816/23061456_2022_7–8_70

АНАЛИЗ УЯЗВИМОСТЕЙ ПРИ ГРУППОВОМ ПРИМЕНЕНИИ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

VULNERABILITY ANALYSIS IN THE GROUP APPLICATION OF SPECIAL PURPOSE ROBOTIC SYSTEMS

Г.Е. Русов, С.В. Краморев, Д.С. Телегин, канд. техн. наук С.А. Диченко

G.E. Rusov, S.V. Kramorev, D.S. Telegin, Ph.D. S.A. Dichenko

Краснодарское высшее военное училище им. С.М. Штеменко

Разработка и применение автоматизированных систем различного назначения обеспечило повышение надежности и оперативности получения необходимой информации. Отсутствие при этом необходимости траты времени на обработку данных позволяет перераспределить ресурсы на их анализ и выработку управленческих решений. В то же время эффективное использование удаленных автоматизированных систем специального назначения — робототехнических комплексов, активно применяемых в том числе в Вооруженных Силах Российской Федерации, требует постоянного управления оператором по стойкому защищенному каналу связи. Проведен анализ действий злоумышленника в отношении нарушения целостности, конфиденциальности и достоверности информации, передаваемой по командной радиолинии при применении робототехнических комплексов специального назначения, в том числе групповом.

Ключевые слова: робототехнический комплекс специального назначения, информационная система, командная радиолиния, групповое применение робототехнических комплексов.

The development and application of automated systems for various purposes has improved the reliability and efficiency of obtaining the necessary information. The absence of the need to waste time on data processing allows you to reallocate resources for their analysis and development of management decisions. At the same time, the effective use of remote automated systems for special purposes – robotic complexes that are actively used, including in the Armed Forces of the Russian Federation, requires constant operator control over a stable secure communication channel. The analysis of the actions of the attacker in relation to the violation of the integrity, confidentiality and reliability of information transmitted over the command radio line when using special-purpose robotic systems, including group.

Keywords: special purpose robotic complex, information system, command radio line, group application of robotic complexes.

Введение

XXI век ознаменован кардинальными изменениями во всех сферах деятельности человека. Научно-технический прогресс не обошел стороной и робототехническую область развития науки. За последние 10 лет в робототехнике произошли глобальные изменения, связанные

с массовым производством и испытанием в различных условиях робототехнических комплексов (РТК) специального назначения [1, 2].

Уровень развития производства и обеспечения автоматизации процессов принятия решений в ходе работы РТК как при применении в составе группы, так и в индивидуальном порядке достиг планки, когда практически нет ограничений на мощности, массогабаритные характеристики и возможности вычислительных средств. Тенденцией является многократное увеличение мощности и ресурсов источников питания для обеспечения применения РТК. Уже имеющийся, а также потенциальный уровень оснащения роботизированными средствами и комплексами в ближайшем будущем пророчит ведение современных сетецентрических войн, характерной чертой которых будет широкое групповое применение РТК [3].

Основные направления работ в области развития робототехнических систем и комплексов специального назначения, ведущихся Россией, в целом совпадают с зарубежными направлениями. К ним относятся: дооснащение уже имеющихся образцов специальной техники модульным или навесным оборудованием и создание дистанционно управляемых, автономных и полуавтономных РТК. Характерной чертой обоих направлений является безэкипажное применение разрабатываемых образцов в режиме дистанционного управления.

Концепция развития и регулирования отношений в сфере технологий искусственного интеллекта и робототехники определяет, что к 2030 году доля безэкипажных средств составит 30 % от общего количества боевых машин [3].

В то же время работа в области разработки и внедрения технологий робототехники военного назначения является приоритетным направлением для Вооруженных Сил Российской Федерации. Министерство обороны Российской Федерации широко применяет и осваивает номенклатуру наземных, морских и воздушных РТК военного назначения. В основном областями их применения являются: ведение разведки, прорыв обороны злоумышленника, обеспечение обороны роботизированными огневыми точками, подавление огневого противодействия мобильными РТК, ликвидация нештатных ситуаций с опасными в обращении боеприпасами, обезвреживание взрывоопасных предметов, проведение аварийно-восстановительных работ, эвакуация с поля боя личного состава и техники под огнем, инженерная разведка, минирование и разминирование, обеспечение преодоления заграждений, доставка боеприпасов и материалов в зону огневого воздействия, охрана и оборона.

Особенности РТК как объекта защиты информации

РТК является сложной эргодической системой, подверженной деструктивному информационному воздействию (ДИВ) злоумышленника [4–6]. В связи с этим при рассмотрении РТК как объекта защиты от ДИВ необходимо принимать во внимание следующие особенности:

– наличие сложных взаимосвязей между разнородными информационными потоками, существующими внутри РТК;

– ДИВ на телеметрическую информацию может привести к формированию ложных команд управления РТК и нарушению их функциональной устойчивости;

– ДИВ на инерциально-навигационную систему может привести к нарушению функционирования блока управления, отвечающего за взаимодействие оператора и управляемого комплекса;

– наличие разнородных по структуре, формату и избыточности видов информации предполагает применение криптографических средств защиты информации и специальных протоколов передачи данных;

– массогабаритные и энергетические ограничения РТК определяют дополнительные требования к средствам обнаружения ДИВ и защиты систем РТК и информации, функционирующей в них.

Угроза осуществления атак на РТК может возникнуть в результате образования канала реализации угрозы между источником угрозы и РТК. Поскольку РТК используют каналы беспроводной связи с пунктом управления (ПУ), реализация угрозы может осуществляться путем эксплуатации атакующим существующих каналов беспроводной связи с РТК.

В идеальном варианте защите должны подлежать все каналы беспроводной связи РТК с ПУ. Однако с учетом требований минимальной

ресурсоемкости систем защиты РТК, во многих случаях рассматривается защита только наиболее критичных каналов взаимодействия РТК с ПУ, к которым можно отнести:

– канал управления, поскольку основные угрозы РТК, такие как перехват управления или вывод из строя, наиболее просто осуществлять в случае успешной эксплуатации атакующим канала управления РТК;

– канал телеметрии, поскольку успешная подмена атакующим телеметрической информации также может привести к реализации перечисленных выше угроз РТК.

Стоит отметить, что в настоящее время существует достаточно большое количество методов защиты информации для стандартных протоколов беспроводной связи и их реализаций. Однако их использование напрямую для защиты каналов связи РТК и ПУ невозможно или нецелесообразно по следующим причинам.

1. Методы, протоколы и реализации криптографических алгоритмов зависят от организации самого радиоканала и структуры разворачиваемой беспроводной сети. Прямое копирование любого набора методов и протоколов информационной безопасности для использования в каналах связи РТК невозможно в силу расхождения принципов организации радиоканалов, количества объектов связи и структуры их связности.

2. Многие методы, например, организация доверенного центра аутентификации объектов, центра генерации и распределения ключей, обладают значительной избыточностью в применении.

3. Применение многих методов обеспечения безопасности приводит к значительному повышению нагрузки на каналы связи и снижает пропускную способность каналов. В системе управления РТК любая излишняя нагрузка на каналы связи может привести к снижению скорости передачи командной информации и повлиять на управляемость и динамику полета самого РТК.

4. Одним из основных принципов стандартов групповой связи являются удобство, простота и прозрачность настроек для оператора РТК. Данный принцип распространяется и на методы обеспечения безопасности, что приводит к тому, что производители вынуждены пользоваться настройками по умолчанию, которые позволяют подключаться к системам связи, но снижают показатели безопасности передачи данных.

5. Некорректная реализация криптографических алгоритмов и особенно систем управления криптографическими ключами, а также их разработка без учета особенностей последующего применения приводит к наличию уязвимостей в таких реализациях.

Стоит отметить, что специфика применения РТК требует применения специально адаптированных для РТК схем генерации, распределения и использования ключевой информации, значительно отличающихся от обычных протоколов защиты беспроводной связи [7].

Групповое применение РТК

Наиболее приоритетным форматом использования РТК является групповое применение. Наиболее существенными преимуществами реализации группового применения РТК являются высокий радиус охватываемой территории для достижения широкомасштабных целей и более высокая вероятность выполнения задач за счет перераспределения целей и подзадач между роботами (рис. 1).

Групповое применение РТК характеризуется следующими особенностями:

– непредсказуемая динамика изменений внешней обстановки;

– ограниченность передачи состояния внешней среды оператору;

– сложность обеспечения коммуникации группировки в пространстве.

Вышеперечисленные особенности являются глубинным источником угроз, а также объектом ДИВ злоумышленника.

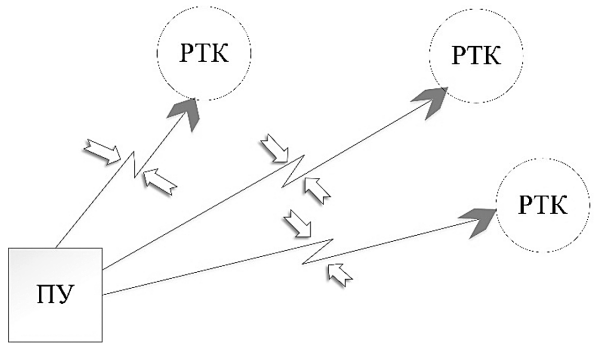

Рис. 1. Линия связи ПУ и РТК при групповом применении

Радиолиния как объект защиты информации

Радиолинии являются одним из наиболее уязвимых звеньев систем управления, поскольку они обнаруживаются по излучению и их работе может быть оказано радиопротиводействие, то есть противодействие радиотехническими методами.

Радиопротиводействие (РПД) — это временное нарушение нормального функционирования радиоэлектронных систем управления под воздействием умышленно создаваемых помех.

Развитие методов и средств РПД породило контррадиопротиводействие, в задачу которого входит разработка методов и средств, снижающих эффективность РПД, обеспечивающих получение информации с помощью радиоэлектронных средств в условиях радиопротиводействия и затрудняющих злоумышленнику организацию и применение средств РПД.

Помехи, направленные на подавление командной радиолинии РТК

Различные радиоэлектронные средства, которые используются в качестве механизмов управления специального назначения, подавить помехами невозможно. Исходя из этого, злоумышленником могут использоваться виды помеховых сигналов, направленные конкретно на определенные типы каналов радиоэлектронных средств управления. Более того, в современных конфликтах для подавления средств одного и того же класса, но использующих разные виды сигналов и способы их обработки, применяют отличающиеся друг от друга виды помех [7, 8].

Существует множество вариантов классификации помех для радиолинии. По происхождению помехи делят на организованные (искусственные, преднамеренные) и неорганизованные (естественные, преднамеренные).

Организованные помехи появляются вследствие применения соответствующей аппаратуры. Целью таких помех является подавление радиоэлектронных средств, за счет которых осуществляется управление РТК. Неорганизованные помехи являются следствием отражения электромагнитных волн от предметов окружающей среды, различных природных образований, явлений, радиоизлучений промышленных установок. Также к неорганизованным помехам относятся помехи создаваемые собственными шумами приемных устройств и взаимные помехи радиосредств, работающих на схожих радиочастотах.

По виду средств создания помех различают активные и пассивные помехи. Активные помехи появляются при применении передатчика помех и излучаются в установленную область пространства. В частности, в сторону ПУ. Пассивные помехи появляются посредством отражения зондирующих сигналов, которые подавляются непосредственно самим устройством управления РТК от искусственно создаваемых отражателей, таких как облака дипольных отражателей.

По характеру воздействия помехи разделяют на маскирующие, имитирующие и подавляющие. Целью применения маскирующих помех является ухудшение характеристик системы управления. Пассивные помехи создают для системы управления дестабилизирующий фон, который в значительной мере затрудняет или же полностью исключает возможность распознавания и обнаружения объектов управления. Излучение сигналов, направленных на опознавание субъектом управления объекта управления, при отражении становится затруднительным, создаваемый фон не позволяет измерить параметры несущих сигналов. Использование маскирующих помех может привести к полному отключению системы опознавания РТК.

Имитирующие помехи предназначены для воссоздания на входе подавляемого устройства управления РТК сигнала, схожего с требуемым, но несущего ложную информацию об объекте управления. Имитирующие помехи могут привести к потере части полезной информации, снижению пропускной способности устройства управления, введению в заблуждение оператора, появлению ложной ошибки в системе. Возможность использования имитирующих помех появляется за счет ограниченности возможностей устройств приема в системах управления РТК — узкий динамический диапазон входных сигналов. Исходя из этого, можно установить конкретное значение мощности помехового сигнала на входе устройства управления, при котором каналы приема теряют возможность выполнять свои функции по излучению информативных сигналов [7].

По тактическому использованию помехи разделяют на помехи самоприкрытия и поме-

хи, создаваемые для групповой защиты. Помехи самоприкрытия используются в том случае, если атакующая или атакуемая цель сама несет в себе источник помех. Тогда реализуется индивидуальная защита объекта от воздействия помех злоумышленника. Помехи, создаваемые для групповой защиты, реализуются при помощи использования отдельного устройства, которое является источником помех для защиты группы РТК.

По перекрытию частотного диапазона помехи разделяют на заградительные и прицельные.

Заградительные помехи отличаются наличием широкого спектра частот, который во много раз превышает полосу пропускания подавляемого приемника. За счет заградительных помех можно воздействовать сразу на несколько средств управления РТК, работающих на схожих частотах и дислоцирующихся в одном районе. Для применения таких помех необходимо лишь приблизительно знать диапазоны рабочих частот, подавляемых РТК. Поэтому разведку, управляющую передатчиками помех, можно считать относительно простой. Недостатком заградительных помех является малая эффективность использования энергии передатчика помех.

Прицельные помехи имеют относительно узкий спектр частот, который соизмерим с полосой пропускания подавляемого средства управления. Средняя частота спектра помехового сигнала должна примерно совпадать с несущей частотой подавляемого устройства. При этом, прицельные помехи используют мощность передатчика более эффективно, но необходимо точно знать несущую частоту подавляемого объекта, что усложняет задачу разведки.

По виду излучения помехи разделяют на непрерывные и импульсные. Непрерывные помехи представляют собой высокочастотные непрерывные моделируемые колебания. Импульсные — направленные периодические излучения, используемые в определенные моменты времени.

Анализ угроз и уязвимостей линии управления РТК

Основными механизмами реализации атак на РТК как на информационную систему являются:

– атаки на каналы связи;

– затруднение идентификации и аутентификации комплексов в системе;

– физическое внедрение «инородных» роботов в систему управления комплексами оператором.

Для понимания, какие необходимо использовать методы и способы противоборства с атаками злоумышленника на информационные системы РТК, классифицируем его действия на отдельные стратегии и возможные сценарии, по которым, вероятно, может развиваться воздействие:

– Стратегия № 1 — нарушение конфиденциальности информации в системе РТК. Возможна компрометация ключевой информации, перехват и дешифрование информации, дешифрование ключа вследствие криптоанализа;

– Стратегия № 2 — нарушение имитостойкости. Возможно вскрытие алгоритма ключа шифрования. За счеты этого — навязывание ложных команд управления РТК и дестабилизация навигационной системы;

– Стратегия № 3 — нарушение достоверности и доступности. Данная стратегия достигается за счет радиоэлектронного подавления команд управления РТК, что влечет за собой нарушение правил вхождения в связь оператора и робота;

– Стратегия № 4 — нарушение сохранности элементов и подсистем РТК. Возможные действия злоумышленника: внедрение закладных устройств, модификация программного обеспечения, уничтожение или подмена наиболее важных компонентов РТК, воздействие на обеспечивающие компоненты: электропитание, линии связи и т.д.

Исходя из вышеперечисленного, можно выделить следующие угрозы командной радиолинии РТК при их групповом применении:

– раскрытие содержания телеметрической информации;

– раскрытие протоколов взаимодействия;

– раскрытие содержания командной информации;

– искажение навигационного поля;

– подавление командной линии;

– раскрытие ключевой информации;

– навязывание ложной командной информации;

– навязывание ложного навигационного поля;

– нарушение функционирования критически важных систем.

Таблица

Оценка степени ущерба угроз безопасности информации

Тип угрозы	Оценка степени потенциального ущерба
Раскрытие содержания телеметрической информации	Малая
Раскрытие протоколов взаимодействия	Малая
Раскрытие содержания командной информации	Средняя
Искажение навигационного поля	Средняя
Подавление командной линии	Средняя
Раскрытие ключевой информации	Высокая
Навязывание ложной командной информации	Высокая
Навязывание ложного навигационного поля	Высокая
Нарушение функционирования критически важных систем	Высокая

Реализация угроз злоумышленником возможна на всех логических уровнях обработки информации РТК. Для максимально полезного применения механизмов и способов защиты необходимо оценивать уровень угроз на РТК как на информационную систему.

В таблице представлены результаты оценки уровня угроз безопасности информации по критичности возможного ущерба.

Исходя из вышеописанных угроз и анализа уязвимостей командной радиолинии при групповом применении РТК, можно классифицировать действия злоумышленника и определить направления защиты информации:

– действия злоумышленника группируются по объекту воздействия — радиоканалы и информация, циркулирующая в них; критически важные элементы системы РТК.

– наибольший ущерб наносят ДИВ, направленные на навязывание ложной информации.

Учитывая пространственную среду распространения командной радиолинии РТК, стоит уделить внимание вопросам, которые касаются защиты информации от несанкционированного доступа к ее смысловому содержанию. Основным методом в этом случае является криптографическая защита, строящаяся из различных алгоритмов шифрования. Также, при групповом применении РТК большую значимость имеет процедура аутентификации. Исходя из этого, в системах передачи данных между пунктом управления и роботом целесообразно использовать асимметричные алгоритмы шифрования. Их преимущества:

– позволяют строить надежные алгоритмы аутентификации, что является более надежным при групповом применении РТК;

– используют меньший объем ключевой информации, нежели симметричные, при групповом применении и с использование большого числа роботов одновременно [9, 10].

Вывод

Таким образом, определены угрозы и уязвимости командной радиолинии при групповом применении РТК. Проведен анализ вероятных стратегий злоумышленника по нарушению функционирования РТК и взаимодействия с оператором. Выделены главные направления, требующие особого внимания при обеспечении безопасности информации, циркулирующей при групповом применении РТК, а также безопасного и корректного управления оператора роботом для полного выполнения боевых и обеспечивающих задач.

Литература

1. Макаренко С.И. Робототехнические комплексы военного назначения — современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. № 2. С. 73–132.

2. Самойленко Д.В., Финько О.А. Обеспечение целостности информации в группе беспилотных летательных аппаратов в условиях деструктивных воздействий нарушителя // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2017. № 5–6 (107–108). С. 20–27.

3. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292–376.

4. Диченко С.А. Модель угроз безопасности информации защищенных информационно-аналитических систем специального назначения // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2022. № 1–2(163–164). С. 64–71.

5. Кравченко А.Ю., Стукало Ю.Е. Проблемы и перспективы создания робототехнических комплексов военного назначения // Материалы VIII Всероссийской научно-практической конференции «Перспективные системы и задачи управления». 2013. С. 22–28.

6. Забегалин Е.В. К вопросу об определении термина «информационно-техническое воздействие» // Системы управления, связи и безопасности. 2018. № 2. С. 121–150.

7. Samoylenko D., Eremeev M., Finko O. et al. Protection of information from imitation on the basis of crypt-code structures // Advances in Intelligent Systems and Computing. 2019. Т. 889. P. 317–331.

8. Диченко С.А., Финько О.А. Контроль и восстановление целостности многомерных массивов данных посредством криптокодовых конструкций // Программирование. 2021. № 6. С. 3–15.

9. 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.

10. 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». 2013. С. 247–251.

References

1. Makarenko S.I. Robotic complexes for military purposes — the current state and development prospects // Systems of Control, Communication and Security. 2016. № 2. P. 73–132.

2. Samoylenko D.V., Finko O.A. Providing integrity information group unmanned aerial vehicles under destructive impact pursue // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2017. № 5–6 (107–108). P. 20–27.

3. Makarenko S.I. Information weapons in the technical sphere: terminology, classification, examples // Systems of Control, Communication and Security. 2016. № 3. P. 292–376.

4. Dichenko S.A. A model of information security threats of protected special-purpose information and analytical systems // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2022. № 1–2 (163–164). P. 64–71.

5. Kravchenko A.Yu, Stukalo Yu.E. Problems and prospects of creating robotic military complexes. «Perspective systems and management tasks» // Materials of the eighth all-Russian scientific and practical conference. 2013. P. 22–28.

6. Zabegalin E.V. On the definition of the term «information technology impact» // Systems of Control, Communication and Security. 2018. № 2 P. 121–149.

7. Samoylenko D., Eremeev M., Finko O. et al. Protection of information from imitation on the basis of crypt-code structures // Advances in Intelligent Systems and Computing. 2019. Vol. 889. P. 317–331.

8. Dichenko S.A., Finko O.A. Control and restoration of the integrity of multidimensional data arrays by means of cryptocode constructions // Programming. 2021. № 6. P. 3–15.

9. Makarenko S.I. Counter Unmanned Aerial Vehicles. Part 3. Electronic Warfare against Navigation and Radio Connection Subsystems of Unmanned Aerial Vehicles // Systems of Control, Communication and Security. 2020. № 2. P. 101–175.

10. Sashnikov T.K. On the issue of ensuring information security of unmanned aerial systems with small and light class aircraft in specialized automated control systems // Proceedings of the All-Russian scientific and technical conference «Theoretical and applied problems of development and improvement of automated control systems for military purposes». 2013. P. 247–251.