ФОРМАЛИЗАЦИЯ ЗАДАЧИ ПОСТРОЕНИЯ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА, ФУНКЦИОНИРУЮЩЕГО В УСЛОВИЯХ АНТАГОНИСТИЧЕСКОЙ КИБЕРЭЛЕКТРОМАГНИТНОЙ ДЕЯТЕЛЬНОСТИ

Головской В.А.¹, Чернуха Ю.В.², Семенюк Д.Б.³

Аннотация. В статье представлены результаты анализа условий функционирования робототехнических комплексов специального назначения. Рассмотрены тенденции развития средств радиоэлектронной разведки и подавления, а также особенности реализации информационно-технических воздействий применительно к задаче обеспечения информационной безопасности ресурсов указанных робототехнических комплексов. Применительно к рассматриваемой задаче скорректировано определение сложного информационного конфликта. Сформулированы основные угрозы информационной безопасности ресурсов робототехнических комплексов, а также возможные сценарии реализации угроз. Показано, что радиоэлектронная разведка радиоканалов системы передачи данных робототехнических комплексов является необходимым этапом для осуществления кибернетической разведки ресурсов данных комплексов и осуществления дальнейших таргетированных кибернетических атак. Сделан вывод о целесообразности выбора оптимальной структуры системы передачи данных робототехнических комплексов в целях повышения скрытности её функционирования и, соответственно, снижения эффективности кибернетической разведки ресурсов робототехнических комплексов. С учетом определенных условий функционирования робототехнических комплексов специального назначения, сформированного перечня защищаемых ресурсов и условий среды функционирования, формализована задача выбора оптимальной структуры указанной системы передачи данных в целях обеспечения информационной безопасности ресурсов рассматриваемых робототехнических комплексов. Полученные результаты позволяют формулировать требования к системе передачи данных робототехнических комплексов, моделировать ее функционирование, и могут быть полезны для дальнейших исследований.

Ключевые слова: сетевая среда, информационное взаимодействие, сложный информационный конфликт, информационно-техническое воздействие, радиоэлектронная разведка, радиоэлектронная борьба, робототехнический комплекс специального назначения.

DOI: 10.21681/2311-3456-2019-6-113-122

Введение

В условиях создания технологически развитыми государствами сетецентрической системы управления войсками увеличивается сложность, непредсказуемость и динамика среды, в которой придется действовать вооруженным силам [1], вследствие чего изменяется их роль и место в перспективной вооруженной борьбе. При этом все большее внимание уделяется требованиям непрерывности информационно-аналитического обеспечения противоборствующих сторон и снижения влияния человеческого фактора при выполнении специальных задач. Применение робототехнических комплексов специального назначения (РТК) является од-

ним из возможных способов обеспечения указанных требований [2].

Как указывалось в [3], РТК могут быть полезны как при ведении боевых действий, так и при выполнении различных специальных операций на территориях различной принадлежности на значительном удалении от пункта управления. Под РТК в дальнейшем понимается система, состоящая из [3]:

- робота или группы роботов, выполняющих специальные задачи в интересах ВС РФ;
- пункта управления, контроля и обработки информации (пункт управления);

1 Головской Василий Андреевич, кандидат технических наук, доцент, доцент кафедры, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: golovskoy_va@mail.ru

2 Чернуха Юрий Владимирович, кандидат технических наук, доцент, начальник кафедры, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: chernuhauv@yandex.ru

3 Семенюк Дмитрий Борисович, сотрудник Восьмого управления Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: flot72@mail.ru

- системы передачи данных (СПД) РТК;
- средств транспортировки, запуска и др.

Будем полагать, что система передачи данных РТК обеспечивает:

- функционирование информационных, командных и телеметрических радиоканалов для связи роботов с пунктом управления, а также радиоканалов для связи между роботами в группе;
- ретрансляцию сигналов как для нужд группы, так и для коалиционных систем и средств, т.е. объединенных в условную «коалицию» согласованными целями функционирования;
- использование своих элементов в качестве датчиков (источников информации, для других систем в том числе).

В указанных условиях будут предъявляться повышенные требования к обеспечению информационной безопасности (ИБ) ресурсов РТК [1, 3, 4]. Концепция сетевидной системы управления предполагает, что ИБ должна обеспечиваться сетевидной средой, под которой понимается совокупность человеческих и технических ресурсов, а также технологий, обеспечивающих их эффективное взаимодействие [1]. Однако в реальных условиях сетевидная систе-

в киберпространстве и радиоэлектронной борьбы. По этой причине вопросы обеспечения ИБ ресурсов РТК актуальны и будут оставаться таковыми при наличии организованного противоборства.

Цель работы – определение факторов, оказывающих существенное влияние на функционирование СПД РТК в условиях антагонистической киберэлектромагнитной деятельности, и формализация задачи выбора структуры СПД РТК, обеспечивающей информационную безопасность ресурсов рассматриваемых РТК.

В целях формализации задачи обеспечения ИБ ресурсов РТК определим перечень защищаемых ресурсов РТК R , угрозы ИБ U и наиболее возможные сценарии S деструктивного воздействия на данные ресурсы.

Анализ защищаемых ресурсов РТК

При анализе проблем обеспечения безопасности функционирования СПД РТК будем различать ИБ ресурсов РТК и безопасность функционирования самой СПД РТК [5].

Выделим из состава ресурсов (R) три группы (рис.1): аппаратные (R_{HW}), программные (R_{SW}) и информационные ресурсы (R_{Inf}), т.е. $R = \{R_{HW}, R_{SW}, R_{Inf}\}$. В качестве ресурсов РТК, под-

Рис. 1. Структура подлежащих защите ресурсов РТК

ма не является замкнутой средой, и концепции^{4, 5} киберэлектромагнитной деятельности акцентируют внимание на едином планировании и интеграции операций

4 Joint Doctrine Note 1/18: Cyber and electromagnetic activities, February 2018, UK Ministry of Defence [Электронный ресурс]. – Режим доступа: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf (дата обращения: 10.02.2019)

5 Field Manual 3-12 «Cyberspace and Electronic Warfare Operations». Department of the Army. Washington, DC, April 2017 [Электронный ресурс]. – Режим доступа: https://www.cyberwar.nl/d/fm3_12.pdf (дата обращения: 10.02.2019)

лежащих защите, определим средства и данные, необходимые для выполнения РТК целевой задачи, обеспечения эффективного информационного взаимодействия РТК с пунктом управления и другими РТК, а также коалиционными системами.

К защищаемым аппаратным ресурсам R_{HW}^Z отнесем средства информационно-управляющей системы (накопления и обработки информации), навигационное оборудование, средства обеспечения ИБ, датчики, радиочастотные модули и системы электропитания, т.е. $R_{HW}^Z \subseteq R_{HW}$.

В группу защищаемых информационных ресурсов R_{SW}^Z включим целевые данные и данные, хранящиеся

в СПД РТК, циркулирующие в системах обмена данными СПД РТК, а также данные системы обеспечения ИБ, т.е. $R_{SW}^Z \subseteq R_{SW}$.

Программные же ресурсы все будут отнесены к защищаемым, т.е. $R_{Inf}^Z = R_{Inf}$.

Таким образом множество защищаемых ресурсов РТК может быть описано как

$$R^Z = \{R_{HW}^Z, R_{SW}^Z, R_{Inf}^Z\} \subseteq R. \quad (1)$$

Как определено в [6], безопасность СПД РТК характеризует ее способность противостоять определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав СПД РТК ресурсы, каналы связи и протоколы, которые могут привести к ухудшению качества выполнения задач.

Под информационной безопасностью СПД РТК будем понимать допустимую, приемлемую в рассматриваемых условиях, вероятностную характеристику, определяющую возможный ущерб, который может быть нанесен СПД в результате несанкционированного доступа к её защищаемым информационным ресурсам, нарушения их целостности и доступности, а также нарушения целостности и доступности её защищаемого программного обеспечения. Опишем условия осуществления несанкционированного доступа

$$\{\bar{C}(R_{Inf}^Z) \cup \bar{D}(R_{Inf}^Z) \cup \bar{K}(R_{Inf}^Z) \cup \bar{C}(R_{SW}^Z) \cup \bar{D}(R_{SW}^Z)\} \neq \emptyset, \quad (2)$$

где $\bar{C}(R_x^Z)$, $\bar{D}(R_x^Z)$ и $\bar{K}(R_x^Z)$ – множество вари-

антов воздействий, нарушающих целостность, доступность и конфиденциальность защищаемых ресурсов группы x соответственно.

Наличие возможности воздействия на защищаемые ресурсы СПД РТК, способного прямо или косвенно нанести ущерб ИБ, является угрозой безопасности СПД РТК. Полное множество угроз безопасности СПД РТК достаточно трудно формализуемо, однако анализ показывает [7-13], что основными угрозами ИБ ресурсов РТК являются реализуемые в отношении радиоканалов СПД:

- радиоэлектронная разведка (РЭР);
- радиоэлектронное подавление (РЭП).

Указанные угрозы могут быть реализованы вооруженными силами иностранных государств и их коалиций, а также террористическими организациями [3]. Рассмотрим особенности и тенденции развития средств РЭП и РЭР, организационно входящих в состав систем радиоэлектронной борьбы (РЭБ).

Анализ тенденций развития систем РЭБ

Анализ тенденций развития теории и практики РЭБ

позволяет увидеть следующие закономерности [1, 2, 8, 10, 11, 14-17]:

- использование в качестве носителя средств РЭБ летательных аппаратов, причем в настоящее время имеет место тенденция к увеличению среди них доли беспилотных летательных аппаратов;
- совершенствование системы мониторинга сигналов в различных физических полях;
- расширение номенклатуры типов формируемых комплексами РЭБ помех (около 300 на настоящее время);
- интеграция воздушных, наземных, морских и космических средств РЭБ в единую систему;
- увеличение возможностей влияния на условия распространения и отражения электромагнитных волн;
- развитие технологий «когнитивного подавления»;
- интеграция РЭБ с ведением космических, кибернетических и навигационных операций, борьбы с системами управления в «Киберэлектромагнитную деятельность»;
- расширение диапазона используемых способов информационно-технических воздействий (ИТВ).

Для целей настоящей статьи под способом ИТВ будем понимать последовательность действий, необходимых для формирования совокупности факторов, нацеленных на нарушение конфиденциальности, целостности и/или доступности обрабатываемой РТК информации и/или алгоритмов ее обработки и достаточных для реализации с использованием электромагнитных полей и/или электрических токов некоторых условий функционирования РТК, при выполнении которых он переходит в состояния потери работоспособности, сниженной эффективности функционирования, управляемости и/или доступности для углубленного анализа источником таких воздействий [17].

В целях определения угроз ИБ рассмотрим условия функционирования РТК при выполнении ими специальных задач.

Условия функционирования РТК

Перспективные условия ведения боевых действий предполагают выполнение РТК операций в любых условиях обстановки, под которыми понимается совокупность факторов F внешней среды (в том числе киберпространства), определяемой:

- рельефом и растительным покровом местности;
- степенью урбанизации местности;
- динамично изменяющейся радиообстановкой (в том числе по причине РЭБ);
- метеорологическими явлениями, активными воздействиями противника, например, в форме организации аэрозольных облаков и т.д.;
- влиянием операций, проводимых в киберпространстве, на физическую и информационные области внешней среды.

Учет степени урбанизации объясняется тем, что боевые действия в городских условиях становятся все более обыденным явлением [18].

Таким образом РТК функционирует в сложных условиях динамично изменяющихся параметров внеш-

ней среды и антагонистического информационного конфликта, определяемых киберэлектромагнитной деятельностью противника в том числе. Однако эксперты отмечают [7], что, кроме традиционно рассматриваемого антагонистического информационного конфликта, имеет место обострение коалиционного конфликта. Под коалиционным конфликтом понимается проблема электромагнитной совместимости (ЭМС) технических средств (ТС) с коалиционными системами и средствами. Под ЭМС ТС⁶ при этом понимается способность ТС функционировать с заданным качеством в заданной электромагнитной обстановке (радиообстановке) и не создавать недопустимых электромагнитных помех другим ТС.

Анализ проблемы межсистемной ЭМС показывает [19, 20], что с учетом предъявляемых к РТК требований к способности выполнения ими задач в любых условиях обстановки, необходимо рассматривать еще один вид информационного конфликта – радиоэлектронный конфликт (т.е. нарушение ЭМС) с системами, не относящимися ни к коалиционным, ни к антагонистическим системам. Предлагается называть такой конфликт индифферентным, а технические средства и системы, участвующие в таком конфликте с системами РТК, – индифферентными. Такими индифферентными средствами и системами могут быть [20-22]:

- радиорелейные и радиолокационные станции (ближней и дальней радиолокации);

- ТС сотовых систем подвижной связи и систем профессиональной подвижной связи;
- ТС земных станций спутниковой связи;
- ТС радиовещательных станций;
- ТС систем широкополосного беспроводного доступа и др.

Скорректируем понятие сложного информационного конфликта с учетом рассмотренных аспектов функционирования РТК в городской среде. Предлагается под сложным информационным конфликтом понимать одновременное наличие антагонистического (C_{ant}), коалиционного (C_{coal}) и индифферентного (C_{ind}) конфликтов:

$$C_{comp} = \{C_{ant}, C_{coal}, C_{ind}\}, \quad (3)$$

где $C_{ant} \neq \emptyset$, $C_{coal} \neq \emptyset$, $C_{ind} \neq \emptyset$, т.е. каждый

тип характеризуется непустым множеством вариантов конфликтных воздействий.

При функционировании РТК в условиях сложного информационного конфликта будут предъявляться повышенные требования к таким характеристикам СПД РТК [12, 13], как помехоустойчивость, помехозащищенность, электромагнитная совместимость и др.

Рис. 2. Схема информационного взаимодействия

6 ГОСТ Р 50397-2011. Совместимость технических средств электромагнитная. Термины и определения. – Введ. 2012-09-01. – М.: Стандартинформ, 2013.

С позиций системного анализа можно выделить объекты и типы информационного взаимодействия (ИВ) между этими объектами, определяющие структуру СПД РТК, функционирующей в условиях сложного информационного конфликта. С учетом рассмотренных условий функционирования РТК выделим следующие объекты ИВ:

- СПД РТК;
- антагонистические системы (РЭБ противника);
- коалиционные системы (разведки, навигации, передачи данных, управления и др.);
- индифферентные системы;
- среда функционирования.

Между СПД РТК и приведенными объектами возможны следующие типы ИВ [23], при этом направленность ИВ показана стрелкой:

- СПД РТК $\leftrightarrow$ среда: индифферентное;
- СПД РТК $\leftrightarrow$ коалиционные системы: коалиционное;
- СПД РТК $\leftrightarrow$ антагонистические системы: конфликтное;
- индифферентные системы $\rightarrow$ СПД РТК: индифферентное;
- антагонистические системы $\rightarrow$ коалиционные системы: конфликтное;
- антагонистические системы $\rightarrow$ среда: конфликтное;
- среда $\rightarrow$ антагонистические системы: индифферентное;
- среда $\rightarrow$ коалиционные системы: индифферентное.

Информационные процессы, которые будут возникать при ИВ рассматриваемых объектов с СПД РТК, обуславливают её структурные характеристики. В целях исследования рассмотрим процессы ИВ, влияющие на функциональную эффективность СПД РТК (рис.2). При построении схемы информационного взаимодействия нами рассматривается только направленность ИВ без анализа конфликтных противостояний более низких иерархических уровней. При этом объекты ИВ образуют надсистему, обладающую самостоятельными свойствами,

не присущими ни одной из систем, но влияющими на поведение системы [24].

Наличие большого числа ИВ конфликтного типа выводит на первый план такую характеристику СПД РТК, как конфликтная устойчивость. Для уточнения требований к СПД РТК необходимо подробнее рассмотреть угрозы ИБ ресурсов РТК, а также сценарии реализации угроз.

Угрозы ИБ ресурсов РТК

Основными объектами воздействия для угроз ИБ являются подлежащие защите ресурсы РТК (рис. 1). С учетом возможных угроз спроектирована модель угроз ИБ для ресурсов РТК [3]. В настоящей работе предприняты попытки развить составную часть указанной модели – модель нарушителя информационной безопасности ресурсов РТК (табл. 1). Необходимо для дальнейшего анализа отметить, что рассматриваемые в модели подразделения РЭБ могут как входить в подразделения РЭБ, так и быть самостоятельными.

Разработанная модель позволяет выделить схожие составляющие элементы, что позволяет применять классические подходы к обеспечению ИБ и построению СПД РТК, а также разрабатывать новые.

В настоящее время с учетом приведенных угроз предлагается рассматривать следующие основные сценарии ($S = \{s_l\}, l = \overline{1, N_l}$) активного воздействия

противника на радиоканалы СПД РТК [3, 17, 21]:

- 1) осуществление РЭР радиоканалов РТК и дальнейшее их РЭП;
- 2) проведение радиоразведки и вскрытие семантической составляющей информации, передаваемой по радиоканалу;
- 3) осуществление РЭР радиоканалов РТК и дальнейшее внедрение ложных команд в каналы управления РТК;
- 4) осуществление радиотехнической разведки радиоканалов РТК и дальнейшее осуществление ИТВ.

Таблица 1

Модель нарушителя

Характеристика нарушителя	Нарушитель		
	Подразделения РЭБ иностранных государств	Подразделения РЭР иностранных государств	Террористические организации
Возможности технических средств	Специализированные высокопроизводительные средства РЭБ	Специализированные высокопроизводительные средства РЭР / использование данных других систем	Неспециализированные средства

Характеристика нарушителя	Нарушитель		
	Условно неограниченные	Условно неограниченные	Ограниченные
Финансовые ресурсы			
Используемые технологии	Создание вредоносных программ / разработка новых алгоритмов подавления / разработка новых технологий ИТВ	Разработка новых методов РЭР / поиск новых уязвимостей криптографических методов защиты информации	Готовые вредоносные программы, известные уязвимости
Возможность получения информации о построении системы защиты	Могут получать достаточно полную информацию	Могут получать достаточно полную информацию	Могут предпринимать усилия для получения представления о построении системы защиты
Преследуемые цели	РЭП радиоканалов СПД РТК / РЭП бортовых ЭВМ РТК / ИТВ	Получение данных для РЭП / создание условий для ИТВ / вскрытие семантической составляющей	РЭП радиоканалов СПД РТК / вскрытие семантической составляющей
Характер действий	Скрытый / открытый	Скрытый	Скрытый или открытый демонстративный
Глубина проникновения	До достижения поставленной цели или появления серьезного препятствия	До достижения поставленной цели	До достижения поставленной цели или появления препятствия

При реализации ИТВ возможны следующие его цели (последствия):

- функционирование СПД с характеристиками, обуславливающими возникновение коалиционного и/или «индифферентного» конфликта (проблема ЭМС);
- осуществление непреднамеренных излучений для снижения энергопотенциала РТК;
- передача целевой или другой подлежащей защите информации противоборствующей стороне конфликта;
- передача ложных данных (телеметрических, навигационных и других датчиков), сигналов управления и др.

Указанные ИТВ относятся к таргетированным кибернетическим атакам, и угрозы их реализации становятся все более актуальными [25].

Рассмотренные выше сценарии позволяют выделить общую составляющую активных действий противника в отношении защищаемых ресурсов РТК – радиоэлектронная разведка. Кроме того, осуществление ИТВ в отношении ресурсов РТК невозможно без предварительного проведения кибернетической разведки СПД РТК. Кибернетическая разведка может быть реализована только при наличии результатов успешной РЭР. Таким образом успешная РЭР является необходимым

условием осуществления кибернетической разведки.

Рассмотренные выше сценарии воздействия противника на радиоканалы РТК, при их реализации, позволяют противнику нарушить конфиденциальность, целостность и доступность обрабатываемой СПД РТК информации [12] или снизить энергетический потенциал РТК, что в свою очередь, будет способствовать снижению эффективности применения РТК.

С учетом введенного понятия сложного информационного конфликта (3) и рассмотренных выше сценариев можно сделать вывод, что имеет место функциональная зависимость защищенности информации, обрабатываемой и циркулирующей в радиоканалах СПД РТК, от такого её свойства, как скрытность, т.е.

$$W_{зи} = f(W_{ск}), \quad (4)$$

где $W_{зи}$, $W_{ск}$ – показатели защищенности информации и скрытности функционирования СПД РТК соответственно, f – неубывающая функция своего аргумента.

Данное выражение позволяет сделать вывод о том, что состояние защищенности ресурсов РТК достижимо только при обеспечении высокой скрытности функционирования СПД РТК. В описанных условиях сложного информационного конфликта обеспечение требуемых

показателей (4) представляется проблемой.

Применительно к рассматриваемой задаче с позиций теории принятия решений модель проблемной ситуации в общем виде может быть представлена системой

$$D = \langle G, P, U, \Lambda, \Psi, \Theta \rangle, \quad (5)$$

где $G = \{G_1, G_2\}$ – множество исходов, содержащее два подмножества исходов $G_1 \cap G_2 = \emptyset$: G_1 – подмножество, характеризующее штатные режимы функционирования СПД РТК, G_2 – подмножество нештатных режимов функционирования СПД РТК, обусловленных реализацией противником одного или нескольких сценариев $s_l \in S, l = 1, N_l$;

$P = \{p_k\}, k = \overline{1, N_k}$, – модель предпочтений лица,

принимающего решение, во множестве вероятностей на G ;

U – множество стратегий (способов функционирования СПД);

$\Lambda = \{\Lambda_d, \Lambda_s, \Lambda_{ud}\}$ – множество неконтролируемых факторов, влияющих на исход: Λ_d – определённые (априорные данные о параметрах местности, данные о установленных на носителях средствах РЭБ противника и их характеристики, данные о состоянии РТК и др.); Λ_s – стохастические (параметры радиоизлучений коалиционных и индифферентных ТС, параметры распространения радиоволн и др.); Λ_{ud} – неопределённые (стратегии ведения противником киберэлектромагнитной деятельности), $C_{comp} \subseteq \Lambda$;

Ψ – функция, ставящая в соответствие фиксированной стратегии $u \in U$ и значению неопределённого фактора $\lambda \in \Lambda$ некоторый исход $g \in G$;

Θ – вся остальная информация о проблемной ситуации, представленная в формализованном виде (сведения о неопределённом факторе, предпочтения других лиц – участников ситуации и др.).

Задачу синтеза стратегии $u \in U$ СПД РТК, функционирующей в условиях сложного информационного конфликта, по аналогии с [7] можно сформулировать в виде задачи выбора оптимальной эффективной системы X^* на множестве альтернатив Ω_x построения такой системы

$X^* = \max(\Omega_x, P), \quad (6)$

где P – модель предпочтений, участвующая в формировании системы (5). При разработке системы предпочтений P применительно к рассматриваемой задаче (3) для обеспечения конфликтной устойчивости СПД РТК необходимо обеспечивать согласованность частных задач, выполняемых различными подсистемами СПД РТК, с задачей (6).

Построение отношений $p_k, k = \overline{1, N_k}$, может быть осуществлено на основе выбранных показателей $W_k(X, Y)$, зависящих от характеристик Ω_E и характеристик Ω_y конфликтующей системы, и непрерывных на $\Omega_x \times \Omega_y$.

Для обеспечения устойчивости при коалиционном ИВ отношение p_1 можно сформулировать следующим образом [7]:

$$X_2 p_1 X_1 \Leftrightarrow W_{coal}(X_2, Z^*) > W_{coal}(X_1, Z^*), \quad (7)$$

где Z^* – характеристики ТС, соответствующие заданному режиму функционирования РЭС группировки, каждое n -е РЭС которой описывается вектором $Z = \{z_n\} \in \Omega_z, n = \overline{1, N_z}$.

При рассмотрении индифферентного ИВ отношение p_2 по аналогии с можно определить как

$$X_2 p_2 X_1 \Leftrightarrow W_{ind}(X_2, Y^*) > W_{ind}(X_1, Y^*), \quad (8)$$

где Y^* – характеристика радиообстановки в зоне функционирования РТК, определяемая характеристиками и режимами работы находящихся в непосредственной близости индифферентных ТС.

С учетом одно из отношений должно определяться как

$$X_2 p_3 X_1 \Leftrightarrow W_A(X_2, F^*) > W_A(X_1, F^*), \quad (9)$$

где F^* – характеристика информационной сферы в зоне функционирования РТК, определяемая, в том числе, ведением противником РЭР.

Использование отношений – для формирования алгоритма управления синтезируемой адаптивной СПД предполагает предварительную проработку всех вариантов ИВ, а также интеллектуальную корректировку базы режимов работы СПД в процессе функционирования, что полностью согласуется с сформулированными в [21, 22, 26] требованиями к наличию у СПД РТК когнитивных способностей. Указанная корректировка должна осуществляться с интеллектуальными узлами СПД РТК на основе принципов киберфизического управления.

Заключение

В работе рассмотрены состояние и перспективы развития киберэлектромагнитной деятельности, которые, в том числе, определяют условия функционирования робототехнических комплексов специального назначения. Для рассмотренных условий с позиций системного анализа построена схема информационного взаимодействия СПД РТК с другими объектами информационного взаимодействия, которая является новой для рассматриваемой задачи обеспечения конфликтной устойчивости СПД РТК. На основе анализа условий информационного взаимодействия скорректировано понятие сложного информационного конфликта, под которым предлагается понимать одновременное наличие антагонистического, коалиционного и индифферентного конфликтов. Данное расширение понятия сложного

конфликта за счет введения в рассмотрения индифферентного конфликта является новым, позволяет выявить новые закономерности функционирования СПД РТК и предъявлять требования к структуре указанных СПД.

Для предложенной в работе структуры подлежащих защите ресурсов РТК, сформулированы вероятные сценарии таргетированных атак, общим местом которых является успешная реализация радиоэлектронной разведки ресурсов СПД РТК.

Проведенная формализация задачи построения СПД РТК, функционирующего в условиях сложного информационного конфликта, позволит осуществлять дальнейшие исследования по созданию СПД

робототехнических комплексов специального назначения.

Дальнейшее развитие исследований видится в выработке стратегий поведения СПД РТК в условиях сложного информационного конфликта, разработке требований к оптимальной программной конфигурации РТК, обеспечивающей корректное функционирование всех подсистем РТК в условиях антагонистической киберэлектромангнитной деятельности, а также в выработке и обосновании правил создания множества альтернатив, причем в целях снижения эффективности радиоэлектронной разведки ресурсов СПД РТК предлагается рациональным требовать максимизации Ω_x .

Литература

1. Макаренко С.И., Иванов М.С. Сетевая война – принципы, технологии, примеры и перспективы. Монография. СПб.: Научное издание, 2018. 898 с.
2. Макаренко С.И. Робототехнические комплексы военного назначения – современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. №2. С. 73-132.
3. Мамедов В.С., Головской В.А. Модель угроз безопасности информации, передаваемой по радиоканалам робототехнического комплекса // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. - Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ. 2018. С. 412-417.
4. Кузнецов Ю.В., Винокуров А.В., Бардаев Э.А. Теоретические основы обеспечения информационной безопасности робототехнических комплексов // Военная мысль. 2018. №12. С. 71-78.
5. Буренин А.Н., Легков К.Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения и управления: Монография. М.: ООО «ИД Медиа Паблишер», 2015. 348 с.
6. Буренин А.Н., Легков К.Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // Научное издание в космических исследованиях Земли. 2015. Т. 7. № 3. С. 46–61.
7. Конфликтно-устойчивые радиоэлектронные системы. Методы анализа и синтеза / Под ред. С.В. Ягольникова. М.: Радиотехника, 2015. 312 с.
8. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. СПб.: Научное издание, 2017. 546 с.
9. Горбачев Ю.Е. Зависимость эффективности операций от интеграции РЭБ и электромагнитной деятельности войск // Радиоэлектронная борьба в Вооруженных Силах Российской Федерации–2015. 2015. С. 15-21.
10. Батурин Ю.О., Золотов С.И. Тенденции развития средств радиоэлектронной борьбы стран НАТО в свете реализации основных концепций ведения военных действий // Сборник трудов XXIII Международной научно-технической конференции «Радиолокация, навигация, связь». 2017. Т. 3. С.1181-1188.
11. Михайлов Р.Л. Радиоэлектронная борьба в Вооруженных силах США: военно-теоретический труд. СПб.: Научное издание, 2018. 131 с.
12. Антохин Е.А., Панасенко Н.Н., Чернова А.Д. Основные требования к беспроводным каналам связи наземных робототехнических комплексов военного назначения // Робототехника и техническая кибернетика. 2017. № 4 (17). С. 10-14.
13. Макаренко С.И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. – Режим доступа: <http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf> (дата обращения: 21.01.2019).
14. Stein R., Delaney W. 21-st Century Military Operations in a Complex Electromagnetic Environment. 2015 [Электронный ресурс]. – Режим доступа: <http://www.dtic.mil/dtic/tr/fulltext/u2/1001629.pdf> (дата обращения: 05.03.2018).
15. Перунов Ю.М., Фомичев К.И., Юдин Л.М. Радиоэлектронное подавление информационных каналов систем управления оружием / Под. ред. Ю.М. Перунова. Изд. 2-е, испр. и дополн. М.: Радиотехника, 2008. 416 с.
16. Верб В.С., Меркулов В.И., Миляков Д.А., Чернов В.С. Мобильные комплексы мониторинга окружающего пространства // Электромагнитные волны и электронные системы. 2015. т. 20. №4. С. 33-50.
17. Бойко А.А., Обущенко Е.Ю., Щеглов А.В. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2017. № 2. С.33-45.
18. Брычков А.С., Дорохов В.Л., Никоноров Г.А. О гибридном характере войн и вооруженных конфликтов будущего // Военная мысль. 2019. №2. С.15-28.
19. Электромагнитная совместимость радиоэлектронных средств и радиоконтроль. Методы оценки эффективности. Монография / Под ред. П.А. Сая. – М. Радиотехника, 2015. 400 с.

20. Головской В.А., Мозоль А.А. Проблемные вопросы обеспечения объектовой электромагнитной совместимости радиоэлектронных средств // Технологии электромагнитной совместимости. 2015. № 3(54). С. 3-10.
21. Головской В.А. Выбор методологических основ создания перспективных когнитивных радиосистем специального назначения // Охрана, безопасность, связь. 2018. Т. 2, № 3 (3). С. 23-29.
22. Мозоль А.А., Головской В.А. О коррекции моделей распространения радиоволн для систем когнитивного радио // Антенны и распространение радиоволн: сб. науч. тр. Всероссийской научн.-техн. конф. Санкт-Петербург, 17-19 октября 2018 г. СПб.: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина), 2018. С. 83-87.
23. Алгазинов Э.К., Сирота А.А. Анализ и компьютерное моделирование информационных процессов и систем. М.: Диалог-МИФИ, 2009. 416 с.
24. Модели информационного конфликта средств поиска и обнаружения. Монография / Под ред. Ю.Л. Козирацкого. М.: Радиотехника, 2013. 232 с.
25. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П. Модель таргетированной кибернетической атаки // Сборник трудов XXIII Международной научно-технической конференции «Радиолокация, навигация, связь». 2017. Т.1. С. 90-98.
26. Гудков М.А., Дворников А.С., Сорокин К.Н. Применение когнитивных радиосистем для обеспечения связи с роботизированными платформами военного назначения // Труды II-й Военно-научной конференции «Роботизация Вооруженных Сил Российской Федерации», Москва, 2017. С. 440-444.

FORMALIZATION OF THE PROBLEM OF CREATING A DATA TRANSMISSION SYSTEM IN A ROBOTIC SYSTEM OPERATING IN CONDITIONS OF ANTAGONISTIC CYBER-ELECTROMAGNETIC ACTIVITY

Golovskoy V.A.⁷, Chernuha Yu.V.⁸, Semenyuk D.B.⁹

The purpose of the work is to define the factors producing a significant impact on operation of data transmission system in a robotic system (RS) in conditions of antagonistic cyber-electromagnetic activities, as well as to elaborate suggestions for their consideration in order to ensure information security of RS resources. The article presents the results of analysis of special-purpose robotic systems operation conditions. The article describes the development trends for radio-electronic reconnaissance and suppression tools, as well as peculiarities of realization of information and technical influence as applied to the task of information security assurance of such robotic system resources. In connection to the task considered, the definition of a complex information conflict has been corrected. Main information security threats for robotic system resources have been formulated, and potential threat occurrence scenarios have been described. It has been demonstrated that radio-electronic reconnaissance of data transmission system radio channels is the stage required to perform cyber reconnaissance of the robotic system resources and to carry out further targeted cyber-attacks. The conclusion has been made that it is reasonable to select the optimal structure of RS data transmission system to increase the concealment of its operation and, consequently, to reduce the efficiency of cyber reconnaissance of the robotic system resources. Considering specific conditions of the special-purpose robotic systems operation, the defined list of protected resources, and operation environment conditions, the task has been formalized for selection of the optimal structure of the system in order to ensure the information security of such robotic system resources. The obtained results allow formulating requirements for RS data transmission system, simulate its operation, and can be useful for further research.

Keywords: *network-centric environment, information interaction, complex information conflict, information and technical impact, electronic intelligence, electronic warfare, military robotic complex.*

References

-
- 7 Vasily Golovskoy, Ph.D., Associate Professor, Krasnodar Higher Military School, Krasnodar, Russia. E-mail: golovskoy_va@mail.ru
 - 8 Yuriy Chernuha, Ph.D., Associate Professor, Krasnodar Higher Military School, Krasnodar, Russia. E-mail: chernuhauv@yandex.ru
 - 9 Dmitry Semenyuk, General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: flot72@mail.ru

1. Makarenko S.I., Ivanov M.S. Setecentricheskaya vojna – principy, tekhnologii, primery i perspektivy. Monografiya. SPb.: Naukoemkie tekhnologii, 2018. 898 s.
2. Makarenko S.I. Robototekhnicheskie komplekсы voennogo naznacheniya – sovremennoe sostoyaniye i perspektivy razvitiya // Sistemy upravleniya, svyazi i bezopasnosti. 2016. №2. S. 73-132.
3. Mamedov V.S., Golovskoy V.A. Model' ugroz bezopasnosti informacii, peredavaemoj po radiokanalam robototekhnicheskogo kompleksa // Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki. - Rostov-na-Donu: PC «Universitet» SKF MTUSI. 2018. S. 412-417.
4. Kuznetsov YU.V., Vinokurov A.V., Bardaev E.A. Teoreticheskie osnovy obespecheniya informacionnoj bezopasnosti robototekhnicheskikh kompleksov // Voennaya mysl'. 2018. №12. S. 71-78.
5. Burenin A.N., Legkov K.E. Sovremennye infokommunikacionnye sistemy i seti special'nogo naznacheniya. Osnovy postroeniya i upravleniya: Monografiya. M.: OOO «ID Media Publisher», 2015. 348 s.
6. Burenin A.N., Legkov K.E. Voprosy bezopasnosti infokommunikacionnykh sistem i setej special'nogo naznacheniya: osnovnye ugrozy, sposoby i sredstva obespecheniya kompleksnoj bezopasnosti setej // Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2015. T. 7. № 3. S. 46–61.
7. Konfliktno-ustojchivye radioelektronnye sistemy. Metody analiza i sinteza / Pod red. S.V. Yagol'nikova. M.: Radiotekhnika, 2015. 312 s.
8. Makarenko S.I. Informacionnoe protivoborstvo i radioelektronnaya bor'ba v setecentricheskikh voynakh nachala XXI veka. SPb.: Naukoemkie tekhnologii, 2017. 546 s.
9. Gorbachev Yu.E. Zavisimost' ehffektivnosti operacij ot integracii REHB i ehlektromagnitnoj deyatel'nosti vojsk // Radioelektronnaya bor'ba v Vooruzhennykh Silah Rossijskoj Federacii–2015. 2015. S. 15-21.
10. Baturin Yu.O., Zolotov S.I. Tendencii razvitiya sredstv radioelektronnnoj bor'by stran NATO v svete realizacii osnovnykh koncepcij vedeniya voennykh dejstvij // Sbornik trudov XXIII Mezhdunarodnoj nauchno-tekhnicheskoy konferencii «RADIOLOKACIYA, NAVIGACIYA, SVYAZ'». 2017. T. 3. S.1181-1188.
11. Mihajlov R.L. Radioelektronnaya bor'ba v Vooruzhennykh silah SSHa: voenno-teoreticheskij trud. SPb.: Naukoemkie tekhnologii, 2018. 131 s.
12. Antohin E.A., Panasenko N.N., Chernova A.D. Osnovnye trebovaniya k besprovodnym kanalamsvyazi nazemnykh robototekhnicheskikh kompleksov voennogo naznacheniya // Robototekhnika i tekhnicheskaya kibernetika. 2017. № 4 (17). S. 10-14.
13. Makarenko S.I. Opisatel'naya model' seti svyazi special'nogo naznacheniya // Sistemy upravleniya, svyazi i bezopasnosti. 2017. № 2. S. 113-164. – Rezhim dostupa: <http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf> (data obrashcheniya: 21.01.2019).
14. Stein R., Delaney W. 21-st Century Military Operations in a Complex Electromagnetic Environment. 2015 [EHlektronnij resurs]. – Rezhim dostupa: <http://www.dtic.mil/dtic/tr/fulltext/u2/1001629.pdf> (data obrashcheniya: 05.03.2018).
15. Perunov YU.M., Fomichev K.I., Yudin L.M. Radioelektronnnoe podavlenie informacionnykh kanalov sistem upravleniya oruzhiem / Pod red. YU.M. Perunova. Izd. 2-e, ispr. i dopoln. M.: Radiotekhnika, 2008. 416 s.
16. Verba V.S., Merkulov V.I., Milyakov D.A., Chernov V.S. Mobil'nye komplekсы monitoringa okruzhayushchego prostranstva // Elektromagnitnye volny i ehlektronnye sistemy. 2015. t. 20. №4. S. 33-50.
17. Bojko A.A., Obushchenko E.Yu., SHCheglov A.V. Osobennosti sinteza polnogo mnozhestva testovykh sposobov udalennogo informacionno-tekhnicheskogo vozdeystviya na prostranstvenno raspredelennye sistemy informacionno-tekhnicheskikh sredstv // Vestnik VGU. Seriya: Sistemnyj analiz i informacionnye tekhnologii. 2017. № 2. C.33-45.
18. Brychkov A.S., Dorohov V.L., Nikonorov G.A. O gibridnom haraktere vojn i vooruzhennykh konfliktov budushchego // Voennaya mysl'. 2019. №2. S.15-28.
19. Elektromagnitnaya sovместimost' radioelektronnnykh sredstv i radiokontrol'. Metody ocenki ehffektivnosti. Monografiya / Pod red. P.A. Saya. – M. Radiotekhnika, 2015. 400 s.
20. Golovskoy V.A., Mozol' A.A. Problemnye voprosy obespecheniya ob"ektovoj ehlektromagnitnoj sovместimosti radioelektronnnykh sredstv // Tekhnologii ehlektromagnitnoj sovместimosti. 2015. № 3(54). S. 3-10.
21. Golovskoy V.A. Vybor metodologicheskikh osnov sozdaniya perspektivnykh kognitivnykh radiosistem special'nogo naznacheniya // Ohrana, bezopasnost', svyaz'. 2018. T. 2, № 3 (3). S. 23-29.
22. Mozol' A.A., Golovskoy V.A. O korekcii modelej rasprostraneniya radiovoln dlya sistem kognitivnogo radio // Antenny i rasprostraneniye radiovoln: sb. nauch. tr. Vserossijskoj nauchn.-tekhn. konf. Sankt-Peterburg, 17-19 oktyabrya 2018 g. SPb.: Sankt-Peterburgskij gosudarstvennyj ehlektrotekhnicheskij universitet «LEHTI» im. V.I.Ul'yanova (Lenina), 2018. S. 83-87.
23. Algazinov E.K., Sirota A.A. Analiz i komp'yuternoe modelirovaniye informacionnykh processov i sistem. M.: Dialog-MIFI, 2009. 416 s.
24. Modeli informacionnogo konflikta sredstv poiska i obnaruzheniya. Monografiya / Pod red. Yu.L. Kozirackogo. M.: Radiotekhnika, 2013. 232 s.
25. Kocynyak M.A., Ivanov D.A., Lauta O.S., Nechepurenko A.P. Model' targetirovannoj kiberneticheskoy ataki // Sbornik trudov XXIII Mezhdunarodnoj nauchno-tekhnicheskoy konferencii «Radiolokaciya, navigaciya, svyaz'». 2017. T.1. S. 90-98.
26. Gudkov M.A., Dvornikov A.S., Sorokin K.N. Primeneniye kognitivnykh radiosistem dlya obespecheniya svyazi s robotizirovannymi platformami voennogo naznacheniya // Trudy II-j Voенно-nauchnoj konferencii «Robotizaciya Vooruzhennykh Sil Rossijskoj Federacii», Moskva, 2017. S. 440-444.