ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ В УСЛОВИЯХ ИХ БОЕВОГО ПРИМЕНЕНИЯ

Стародубцев Ю.И.[1], Худайназаров Ю.К.[2], Ермолаев В.Е.[3]

DOI:10.21681/3034-4050-2025-1-3-19

Ключевые слова: *концепция боевого применения, оперативно-тактические модели, информационно-управляющая система, защищаемые информационные ресурсы, информационная модель, конфликтующие системы, информационно-измерительный квант.*

Цель работы: *состоит в исследовании проблемы обеспечения информационной безопасности системы управления робототехническими комплексами (РТК).*

Метод исследования: *системный подход применен для анализа состава, функций, роли и места информационно-управляющей системы в системе управления современных и перспективных РТК.*

Результаты исследования: *приведены результаты анализа основных свойств и требований к системам управления РТК ВН как системам управления военного назначения. Выявлены основные проблемы повышения эффективности систем управления РТК ВН.*

Представлены специфические угрозы информационной безопасности РТК ВН и недостатки в теории и практике обеспечения информационной безопасности системы управления РТК ВН, определены основные симптомы проблемы. Известные в настоящее время теоретические модели не отражают существенные особенности формирования и защиты информационных ресурсов системы управления РТК ВН, что не позволяет обеспечить адекватность системы защиты. Методом аналитического моделирования сформирована проблема информационной безопасности управления РТК военного назначения (ВН). Информационная модель взаимодействия в конфликтных условиях может быть основой для разработки модели формирования и защиты информационных ресурсов системы управления РТК ВН, а концепция информационно-измерительного кванта может использоваться для устранения дефицита информационных ресурсов и повышения доверия к интеллектуальным информационно-управляющим системам.

Научная новизна: *заключается в формализации информационного взаимодействия между объектами и субъектами системы управления РТК ВН в базисе теоретической информатики с учетом конфликтности условий функционирования РТК ВН.*

Введение

Низкая эффективность РТК различного назначения в ходе специальной военной операции обусловлена недостаточной проработкой оперативно-тактических моделей их боевого применения, недостатками используемых технологий управления и связи, недостатками методов и технологий обеспечения информационной безопасности системы управления РТК, а также недостатками системы подготовки операторов РТК.

Скорость изменения обстановки и соответственно возрастающий объем управляющей информации таковы, что человек-оператор в режиме дистанционного управления не способен выполнять задачи своевременно. Поэтому требуется повышение степени автономности РТК за счет интеллектуализации информационно-управляющей системы и повышение степени доверия к интеллектуальным системам управления РТК в условиях их боевого применения.

В этой связи системы управления РТК военного назначения (РТК ВН) являются новой ветвью развития систем управления оружием, отличающейся высокой степенью автономности и динамичности объектов управления. В перспективе системы управления данного

[1]Стародубцев Юрий Иванович, доктор военных наук, профессор, профессор кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия. Email: starodub@mail.ru

[2]Худайназаров Юрий Кахрамонович, кандидат технических наук, докторант кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия. E-mail: yu-78@ya.ru

[3]Ермолаев Владимир Евгеньевич, адъюнкт кафедры Безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт Петербург, Россия. E-mail: VErmol@ya.ru

вида, расширяясь, должны поглотить системы управления войсками и системы управления оружием, так как робототехнические войска станут основным родом войск.

Следует отметить, что определение РТК в действующих нормативных документах требует расширенного понимания роботизированного средства, в котором модуль движения может отсутствовать, а степень автономности может быть регулируемой. Тогда телекоммуникационное оборудование и средства автоматизации управления, выполняющие автономно большую часть своих функций (возможно, с дистанционным контролем оператором), являются робототехническими комплексами. Следовательно, инфотелекоммуникационная сеть представляет собой группу РТК (робототехническую систему), специализирующихся на процессах передачи и обработки информации (информационных потоков), т. е. являются роботизированной системой связи и управления.

Исследование вопросов обеспечения информационной безопасности систем управления РТК является одним из ключевых направлений решения проблемы повышения эффективности РТК военного назначения. Поэтому требуется исследование новых подходов, методов и технологий защиты и контроля защищенности информационно-управляющих систем РТК.

Известные в настоящее время результаты анализа опыта боевого применения РТК в основном отражают методы и средства защиты военных объектов от РТК ударного типа. Вопросы защиты РТК от информационно-технических воздействий в ходе их боевого применения исследованы недостаточно.

Одной из актуальных задач обеспечения информационной безопасности системы управления РТК ВН является формирование единой критериальной базы оценки защищенности от технической разведки и информационно-технических воздействий противника. Известные в настоящее время методики оценки защищенности объектов от технической разведки и информационно-технических воздействий [1] не имеют общей теоретической основы, что не позволяет адекватно выполнять свертку частных показателей защищенности и оценивать эффективность защитных функций для группы РТК. К тому же методы и технологии контроля безопасности связи [2] не позволяют обрабатывать в режиме реального времени большие объемы информации, циркулирующей в контурах управления РТК, на предмет возможной утечки защищаемых сведений или имитонавязывания.

В данном направлении требуется разработка модели угроз информационной безопасности СУ РТК и модели информационного конфликта между системой управления РТК и системой разведки и информационно-технических воздействий противника. Для обоснования требований по информационной безопасности, а также исследования методов и технологий защиты информационных ресурсов систем управления РТК ВН требуется разработка достаточно адекватной модели информационного конфликта между информационно-управляющей системой РТК (или группы РТК) и системой технической разведки и ИТВ противника, отражающей взаимосвязь свойств защищаемых информационных ресурсов с показателями эффективности системы управления РТК и эффективности ИТВ на систему управления РТК.

В настоящее время в нормативных документах и научных публикациях нет единства понимания сущности информационных ресурсов. Требуется разработка общей модели формирования информационных ресурсов на основе аксиологического подхода, которая позволит обосновать динамические критерии защищенности (уровни доверия) информационных ресурсов с учетом характеристик их пользователей, времени использования (обработки) и количества.

Решение поставленной задачи

Опыт специальной военной операции на Украине показал, что роботизированные комплексы сухопутных войск способны решать широкий спектр задач, основными из которых являются:

- ведение разведки и наблюдения;
- обеспечение связи для управления подразделениями;
- огневое поражение объектов противника;
- эвакуация раненых из «красной зоны»;
- обнаружение, обследование и обезвреживание мин, фугасов и самодельных взрывных устройств;
- вскрытие позиций снайперов, огневых средств, засад и систем наблюдения противника;
- обследование зданий, сооружений и отдельных объектов;
- доставка материально-технических средств к месту назначения.

Тактика боевых действий в ходе специальной военной операции существенно изменяется благодаря новым методам и способам применения ударных и разведывательных беспилотных летательных аппаратов (БПЛА). Для достижения эффекта «огневого вала» применяется следующий способ. Службой БПЛА готовятся ударные

дроны, чтобы они переводились в рабочее состояние максимально просто. Штурмовая пехота, выходя на исходную позицию для атаки раскладывает на грунте взятые с собой ударные дроны (более двух десятков) и включает их. Операторы БПЛА подключаются к дронам с помощью направленных антенн и начинают бить по атакуемым позициям с минимальными интервалами за счет короткого подлетного расстояния, что создает эффект подавления и позволяет атакующей пехоте сближаться с атакуемыми позициями.

Используется также тактика засады из множества дронов, когда их удается занести в тыл противника с помощью диверсионно-разведывательных групп (ДРГ), при этом важен выбор места, чтобы обеспечить возможность подключения операторами БПЛА удаленно.

Проблема подавления средствами РЭБ своих дронов решается организацией «коридоров», через которые свои дроны могут пролетать к позициям противника. Часто такие коридоры образуются не по плану, а хаотично. Передовые подразделения используют средства РЭБ не скоординированно, по собственному усмотрению и без уведомления подразделений БПЛА. Поэтому значительное время у подразделений БПЛА затрачивается на составление «карты полей РЭБ». В связи с этим актуальна задача повышения эффективности взаимодействия подразделений БПЛА, РЭБ и связи по вопросам мониторинга радиоэлектронной обстановки и управления использованием радиочастотного спектра. Максимальное количество одновременной работающих расчетов БПЛА доходит до 6 ударных и одного наблюдательного (ретранслирующего) дронов. Рота БПЛА обычно действует в составе до 8 расчетов в полосе 2–3 км. Возникает необходимость согласования используемых радиочастот каналов управления и видеоканалов.

Затрудняет выполнение задач подразделений БПЛА необходимость работы в режиме без автоматической стабилизации в условиях ветра (изменения гидрометеорологической обстановки по воздушным эшелонам) и незнакомой местности. Поэтому с оператором БПЛА работает техник, который следит за работой системы управления и при необходимости управляет направленной антенной приемопередатчика.

Связанная с предыдущей вторая задача заключается в информационном обеспечении подразделений БПЛА и управлении доступом к базам данных по радиоэлектронной и гидрометеорологической обстановке, а также по оптимальным маршрутам для БПЛА (дневным и ночным секторам или коридорам, свободным от воздействия радиопомех и скрытым от разведки противника). Фактически, это задача формирования информационных ресурсов системы управления РТК ВН.

При сопровождении штурмов с помощью БПЛА используется способ «карусели» для непрерывного наблюдения за штурмом. При недостаточном количестве БПЛА из-за разряда батареи может потребоваться привлечение БПЛА соседних подразделений. В этом случае информация передается через офицера штаба, а не напрямую к штурмующим подразделениям. Кроме того, использование квадрокоптеров ближнего радиуса действия артиллерийскими подразделениями затруднено тем, что они находятся далеко от линии фронта, поэтому зачастую артиллерийские расчеты получают информацию от «чужих» подразделений, находящихся на переднем крае для корректировки «своего» огня. Это приводит к задержке и искажениям в передаче информации.

Система радиоэлектронной разведки (РЭР) противника способна определять местонахождение пульта оператора БПЛА по типовым и индивидуальным демаскирующим признакам (ДМП) даже в условиях сложной электромагнитной обстановки. Наиболее информативными являются ДМП расположения (локализации источников радиоизлучений) и системные признаки деятельности (периодичность, систематичность радиосигналов). Место вылета и погрузки, маршруты движения транспортных БПЛА (агродронов) отслеживаются противником с помощью средств РЭР и видовой разведки. Более скрытым является применение наземных робототехнических средств (беспилотных электротележек).

При использовании тактики «кочующего миномета» расчеты ударных БПЛА относительно безопасно успевают запустить 4–8 дронов с одной позиции. Учитывая длительное время подлета дрона, противник имеет возможность обнаружить местонахождение расчета БПЛА и начать огонь на поражение. Чтобы затруднить разведке противника обнаружения расчета БПЛА, при возвращении на стартовую позицию маршрут прокладывается через лесной участок.

Использование в системой управления дронами SIM-карт для каналов управления и видеоканалов по сетям 4G и 5G позволяет обеспечить проникновение и сохранение устойчивости управления в зданиях и защитных сооружениях.

Могут использоваться волоконно-оптические линии управления дронами, а также радиоканалы с псевдослучайной перестройкой радиочастот каналов управления. Ожидается появление дронов, которые устойчивы к

воздействию радиопомех и используют функции автозахвата цели с помощью машинного зрения.

Таким образом, опыт боевого применения РТК показывает, что существенно увеличивается дальность их применения и функциональность. В то же время преимущественно используется режим дистанционного управления РТК. Это не позволяет в условиях противоборства управлять боевым роботом одному оператору, так как требуется обеспечение разведки, охранения и связи. Основными недостатками режима дистанционного управления, обусловленными необходимостью постоянного информационного обмена с оператором, являются: высокие требования к каналу связи, ограниченный радиус действия канала связи, демаскировка объекта и пункта управления, возможность применения средств радиоэлектронного и огневого противодействия. В связи с этим требуется совершенствование способов и систем управления РТК для их более эффективного группового применения.

Одним из недостатков в практике является отсутствие информационных ресурсов (баз данных) для информационно-управляющих систем РТК ВН:

- по радиоэлектронной обстановке и оптимальным маршрутам движения;
- по гидрометеорологической обстановке;
- по составу и удалению до РТК ближайших соседних подразделений;
- по разведке объектов противника;
- по доступным каналам связи для управления и передачи данных с целевой нагрузкой.

Системы управления РТК ВН (СУ РТК ВН) образуют новую развивающуюся ветвь специальных систем управления боевыми средствами.

Система управления военного назначения (СУВН) — это совокупность функционально взаимосвязанных органов и пунктов управления, систем связи и автоматизации и специальных систем. В общем случае СУВН включает в себя оперативную и техническую подсистемы.

Техническая подсистема обеспечивает обмен информацией между элементами внутри системы управления и между взаимодействующими системами управления. В нее в ходят система связи, система автоматизации, ряд специальных систем.

По характеру управляемых объектов СУВН подразделяются на:

1. Системы управления войсками;
2. Системы управления боевыми средствами (оружием);
3. Специальные системы управления (специального назначения).

Системы управления боевыми средствами — это системы технологического типа, объектами управления в которых являются оружие и другая боевая техника.

К специальным системами управления оружием (информационно-техническим системам реального времени) относятся системы предупреждения о ракетном нападении, контроля космического пространства, разведывательно-ударные комплексы. Они могут быть организационного или технологического типа.

Развитие СУВН идет в направлении построения комплексных систем управления (организационно-технологического типа). К таким системам относится СУ РТК ВН, особенностью которой является соответствие заданным требованиям.

Требования — условия, положения, предписания, отражающие какое-либо соотношение характеристик свойств системы и их граничных значений, определяемых, как правило, суперсистемой. В настоящее время требования к СУ РТК ВН не сформированы, поэтому рассмотрим основные аспекты, характеризующие особенности СУВН.

Основными свойствами СУВН являются:

- структурно-топологические (структура, число элементов и их взаимосвязи, пространственный размах);
- характеристики функционирования (процесса управления: адекватность, оптимальность, оперативность, непрерывность, скрытность; функционирования системы управления: боевая готовность, устойчивость, мобильность, производительность, безопасность, наблюдаемость, управляемость);
- экономические характеристики (затраты на производство, строительство, эксплуатацию, ресурсопотребление).

Основными способами построения СУВН являются централизованный, децентрализованный, смешанный.

К СУВН предъявляются требования по следующим свойствам:

1. Боевая готовность (способность системы и ее элементов переходить из одного состояния в другое за время, не превышающее допустимое);
2. Устойчивость (способность обеспечивать управление с требуемой эффективностью при воздействии неблагоприятных факторов);
3. Мобильность (способность в установленные строки развертываться, свертываться и пере-

мещать свои элементы, а также изменять свою структуру в соответствии с обстановкой);

4. Производительность (способность преобразовывать требуемые объемы информации в установленные сроки);

5. Безопасность (способность противостоять всем видам разведки, вводу ложной информации и несанкционированному доступу к информации);

6. Качество используемых моделей, методик и алгоритмов управления (способность обеспечить необходимую адекватность управления на основе использования применяемых для выработки управляющих воздействий моделей, методик, алгоритмов);

7. Управляемость (способность изменять свое состояние в необходимых пределах и сохранять требуемые значения показателей существенных свойств при переходе из одного состояния в другое);

8. Ресурсопотребление (характеризует численность привлекаемых к управлению должностных лиц, номенклатуру и количество необходимых технических, программных и других средств).

Новое дополнительное требование к СУ РТК ВН предлагается включить в существующий перечень интероперабельность — способность двух и более информационных систем к обмену информацией и к использованию информации, полученной в результате обмена[4]. Это свойство играет ключевую роль при создании, развитии и объединении информационных систем различных типов и назначения.

Проблемы повышения эффективности боевого применения РТК

Эффективное использование автономных РТК сухопутных войск возможно лишь при их групповом применении и распределении решаемых задач между роботами в группе. Разработка одиночных автономных роботов имеет смысл только для решения специальных задач. Отсутствие согласованной концепции автономных РТК ВН является одной из ключевых проблем повышения эффективности их боевого применения.

Направлениями совершенствования РТК ВН являются:

- комплексный подход к развитию РТК ВН и их элементов;
- увеличение количества и расширение функционала РТК ВН;
- групповое применение РТК ВН;
- повышение уровня автономности РТК ВН в составе группы;
- повышение эффективности функционирования РТК ВН в различных физических средах;
- обеспечение интероперабельности СУ РТК ВН.

Повышение автономности РТК связано с решением следующих проблем:

- отсутствие разработанной тактики применения РТК СВ;
- отсутствие отечественных сенсоров для технического зрения;
- отсутствие высокоточных бортовых средств навигации;
- недостаток надежных алгоритмов обнаружения, распознавания автономного применения целевой нагрузки;
- проблема скрытой и устойчивой связи;
- проблема формирования информационных ресурсов для системы управления РТК;
- проблема интеллектуализации информационно-управляющих систем РТК при ресурсных ограничениях.

Задача обоснования облика автономных РТК ВН тесно связана с планируемой тактикой применения и должна решаться в комплексе. Известные в настоящее время исследования форм, методов и способов решения боевых и обеспечивающих задач с использованием робототехнических комплексов (РТК) на поле боя в основном направлены на их одиночное применение. Исследования в области группового применения РТК носят преимущественно обобщенный характер. Важное значение для исследований новых форм, методов и способов вооруженной борьбы с применением традиционных сил и средств совместно с РТК имеет моделирование боевых действий.

На систематизацию опыта использования групп РТК, выработку единых подходов к формированию сценариев боевого применения групп РТК нацелены работы Пшихопова В.Х. В работе [3] сформирована терминологическая база, используемая для разработки сценариев применения групп РТК на поле боя, обобщенная структура сценария на примере модели применения РТК. В частности, определены термины «групповое управление» и «групповое применение», «сценарий», «боевой эпизод», «информационный боевой эпизод», «обеспечивающий эпизод»,

[4]ГОСТ Р 71063-2023 Информационные технологии. Робототехнические комплексы. Интероперабельность. Общие положения.

«ударный эпизод», «модель сценария», «реализация модели сценария». Групповое управление направлено на реализацию отдельных действий РТК ВН и их групп: перемещение, взаимодействие, целераспределение и т. д.

Групповое применение реализует функции более высокого уровня, связанные с боевым применением РТК ВН: планирование выполнения боевых и обеспечивающих задач, контроль выполнения задач и др.

На основе особенностей группового применения вырабатываются требования к управлению группой РТК ВН и к системе группового применения.

Многие особенности группового применения РТК ВН мало изучены и не могут быть формализованы. Авторы [3] используют сценарный подход для формализации роли и места РТК на поле боя в различных видах вооруженных конфликтов. Сценарий содержит последовательность боевых эпизодов, фаз, этапов, соответствующих реализаций сценария с учетом закономерностей военных действий в части решаемой задачи и замыслом разработчика. Определены требования к типовым сценариям в форме уровней зрелости сценариев. Последовательная детализация и уточнение моделей типовых сценариев применения РТК ВН позволяет перейти к имитационному моделированию. Промежуточным этапом перед имитационным моделированием является разработка модели сценария. При этом модель сценария формируется на этапе планирования реализации сценария исходя из конкретных условий обстановки с учетом качественного и количественного состава своих войск и войск противника, их пространственного расположения, условий среды и других факторов. Жизненный цикл сценария боевого применения РТК ВН включает: разработку сценария; формализацию сценария; моделирование действий группы РТК с помощью имитационной модели; полевую апробацию сценария; отработку сценариев при решении группами РТК ВН боевых и обеспечивающих задач.

Модель оценки целесообразности боевого применения РТК ВН на примере БПЛА предложена в работе [4]. В качестве показателя целесообразности боевого применения БПЛА использован показатель «эффективность/стоимость» (приведенная стоимость выполнения боевой задачи). Автором отмечено, что современные тенденции применения БПЛА идут по пути уменьшения их массогабаритных параметров, удешевления конструкции и повышения маневренности, объединения их в группы, что позволяет выполнить боевую задачу даже при увеличении количества потерянных БПЛА.

По результатам анализа отечественного и зарубежного опыта разработки и применения РТК ВН основными тенденциями развития являются: поэтапное наращивание интеллектуальных возможностей систем дистанционного управления с постепенным исключением функций управления и контроля со стороны операторов, повышение подвижности и продолжительности автономной работы РТК, достижение массовости применения РТК в составе перспективных систем вооружения. Повышение автономности и эффективности взаимодействия РТК в группе требует совершенствования интеллектуальных информационно-управляющих систем.

При организации управления группами разнотипных РТК количество требующих решения теоретических задач и технологических проблем возрастает. Необходимо формирование единого замысла применения групп однотипных и разнотипных РТК. Фрагментарность и противоречивость нормативных документов в области стандартизации и унификации РТК обусловлена во многом отсутствием единой терминологии. Однозначно не определены общие подходы к организации управления и типовые состав и структура робототехнических средств и комплексов. Это существенно затрудняет объединение усилий научно-исследовательских организаций, предприятий и организаций военно-промышленного комплекса для формирования единого замысла создания и применения перспективных РТК. В соответствии с нормативными документами робототехническое средство (РТС) независимо от типа, назначения и особенностей исполнения включает в себя модуль движения и модуль целевой нагрузки. Для управления РТС необходимо одновременно решать две существенно различные, но взаимосвязанные задачи: управление движением и управление целевой нагрузкой. РТС, включающие в себя модули управления движением, модули управления нагрузкой и средства управления составляют РТК. В общем случае РТК может включать в себя одно или несколько РТС. В настоящее время задачи, решаемые модулями движения и модулями целевой нагрузки, становятся сравнимыми по своей сложности. Отсутствие универсальной методологии организации управления целевой нагрузкой групп однородных или разнородных РТС существенно ограничивает возможности практического применения специализированных РТК. Приоритетными становятся исследования в области интеграции методов, моделей и алгоритмов управления движением и целевой нагрузкой РТС в составе разнородной группы [5].

Независимо от применяемого режима управления РТК ВН в составе группы остается проблема обеспечения устойчивой связи между РТК в группе, а также между РТК и пультом дистанционного управления (или высокопроизводительной вычислительной облачной системой). Поэтому одной из проблем повышения эффективности РТК ВН является обеспечение скрытности и помехоустойчивости каналов связи в системе управления РТК ВН. Анализ состояния сетей передачи данных наземных РТК ВН показал, что существующее методическое обеспечение обоснования требований к разведзащищенности и помехоустойчивости разрабатываемых сетей передачи данных (СПД) РТК ВН требует совершенствования. В частности, для обоснования требований к СПД РТК ВН по радиоэлектронной защите требуется разработка на этапе эскизного проектирования создаваемого образца РТК частной модели радиоэлектронной борьбы и электромагнитной обстановки (РЭБ и ЭМО). Модель РЭБ и ЭМО включает в себя модель преднамеренных радиопомех и модель непреднамеренных радиопомех, в которых указываются тактико-технические характеристики радиоэлектронных средств создаваемого образца РТК и типовые условия его применения, виды потенциальных источников радиопомех, параметры радиопомех на входе радиоприемников в типовых условиях применения РТК [6].

В работе [7] рассматривается проблема формирования защищенных механизмов межмашинного обмена данными между агентами при их коммуникации за пределами территории контролируемой зоны. Формулируется задача на разработку концепции безопасного управления интеллектуальными роботами и коалициями роботов, создание соответствующих алгоритмов и протоколов защищенного взаимодействия в рамках создания единого подхода к управлению робототехническими комплексами. Децентрализованный способ управления и коммуникации между роботами в группе за пределами контролируемой зоны делают мультиагентную систему уязвимой к угрозам несанкционированного перехвата сообщений, нарушения целостности передаваемых сообщений, отказ в обслуживании, перехват запросов с их модификацией и последующим воспроизведением. Существующие методы и сре-дства защиты требуют адаптации применительно к группам мобильных роботов.

Таким образом, в предметной области военных и технических наук проявляются следующие недостатки теории и практики управления РТК ВН:

- отсутствие обоснованного перечня типовых боевых задач, для решения которых могут применяться РТК и их группы;
- отсутствие обоснованных этапов (вариантов) применения РТК с учетом возможностей и действий традиционных сил и средств, а также возможного изменения обстановки;
- отсутствие систематизированных форм и способов боевого применения РТК ВН и их групп.

Низкая скрытность управления и разведзащищенность системы управления группой РТК обусловлены:

- отсутствием исследований, направленных на скрытие управляющих сигналов между группировками различных роботов в условиях невозможности устранения демаскирующих признаков роботов-разведчиков;
- отсутствием универсальных подходов к комплексному обеспечению безопасности мультиагентных робототехнических систем с сетецентрическим управлением;
- существующие модели верификации агентов не могут быть применены в мобильных робототехнических группах с сетецентрическим управлением;
- возможность контроля ограничена, особенно при решении трудно формализуемых задач (не известен универсальный научно-методический аппарат выявления скрытых информационных атак на исследуемые системы).

Авторами [7] исследованы подходы к решению задач маскирования управляющих сигналов агентов с помощью цифровых водяных знаков, встраиваемых в границы изображений.

Формирование критериальной базы оценки информационной безопасности систем управ-ления РТК является важной научной задачей, для решения которой требуется разработка модели конфликта между системой управления и системой разведки и информационно-технических воздействий противни-ка. Применительно к системе управления одиночным РТК с беспилотными летательны-ми аппаратами (БПЛА) данная задача решается в работе [8]. Авторами рассмотрены частные показатели, характеризующие информационно-управляющую систему (ИУС) робототехнических комплексов с БПЛА, как систему подвижной пакетной радиосвязи специального назначения в усло-

виях информационно-технических воздействий (ИТВ). Предложена система основных тактико-технических показателей характеризующих безопасность функционирования ИУС РТК с БПЛА: скрытность, устойчивость, киберустойчивость. При этом ИУС РТК включает в себя систему информационного обмена и систему обработки и хранения информации.

В работе [9] представлена модель оценки показателей защищенности группы РТК с БЛА от радиотехнической разведки по параметрам командно-телеметрического радиоканала. Сделан вывод о существенном снижении дистанции разведки при увеличении диапазона перестройки частот командно-телеметрического канала более 5 МГц (дальность обнаружения около 10 км для диапазона 3,3–3,4 ГГц при мощности передатчика 0,5 Вт и усилении антенны 1,5 дБ).

Таким образом, большая дальность обнаружения радиоизлучения БПЛА не позволяет обеспечить скрытность управления и внезапность действий войск с применением РТК. В связи с этим требуется разработка оперативно-тактических моделей применения РТК с БПЛА при комбинированных (смешанных) режимах управления на различных этапах выполнения операции. Возможно, варианты с предварительным развертыванием обеспечивающей информационной инфраструктуры позволят существенно повысить разведзащищенность группы РТК. Также требуется повышение автономности РТК и интеллектуальности ИУС для реализации супервизорного режима управления группой РТК при ограниченных коммуникациях в условиях разведки и ИТВ противника.

Методы обеспечения информационной безопасности системы управления РТК ВН

Особенностью РТК ВН являются конфликтные условия их применения на территории, которая находится за пределами контролируемой зоны, или в экстремальных условиях. Группы РТК в этом случае должны быть защищены от обнаружения, перехвата и ввода ложной информации, а также от блокирования информации в СУ РТК. Кроме того, необходимо учитывать такие интеллектуальные способы воздействия противника на СУ РТК, как перехват управления, подмена РТК или базового пункта управления, а также внедрение РТК-диверсанта, саботирующего выполняемые задачи группой РТК. Научный подход предполагает систематизацию защищаемых информационных ресурсов, построение модели угроз безопасности информации, формирование требований к системе защиты. Основные особенности условий функционирования РТК военного и специального назначения заключаются в высокой степени неопределенности и динамичности ситуаций, в которых решаются задачи с применением РТК ВН (СН). Проблема защиты информационных ресурсов РТК ВН заключается в необходимости обеспечить оптимальные условия управления войсками при выполнении задач с применением РТК в условиях неопределенности и высокой динамичности внешних воздействующих факторов, а также структурно-функциональной динамичности группы РТК ВН.

Вопросы обеспечения защиты информационных ресурсов в системах управления РТК рассматриваются многими авторами, однако полученные результаты исследований не позволяют реализовать системный подход для решения этой проблемы.

Наиболее системно вопросы информационной безопасности групповых мобильных РТК рассмотрены в работах Викснина И.И., Зикратова И.А., Зикратовой Т.В., Винокурова А.В., Бардаева Э.А.

Особенностями условий функционирования групп мобильных РТК являются:

- высокая динамика внешних воздействующих факторов;
- высокая степень неопределенности исходных данных для управления, обусловленная неполнотой и противоречивостью знаний агентов о состоянии внешней среды и других агентов группы (недостаточные информационные ресурсы системы управления);
- широкая вариативность путей решения задач группы, структуры группы, распределения ролей в группе;
- сложность обеспечения надежной коммуникации, распределенность группы в пространстве.

Специфические уязвимости мобильных групп РТК обусловливают необходимость адаптации известного научно-методического аппарата и средств обеспечения информационной безопасности к условиям функционирования РТК. В качестве основных угроз, связанных с особенностями РТК, рассмотрены:

- атаки на каналы связи;
- затруднение идентификации и аутентификации роботов в системе;
- физическое внедрение «инородных» роботов, которые могут перехватывать управление другими роботами и создавать условия для их перепрограммирования злоумышленником. В результате численного моделирования атак на информационные ресурсы системы

управления группы однотипных РТК, реализующей муравьиный алгоритм самоорганизации, авторами [10] подтверждены выводы по результатам аналогичных исследований о необходимости введения механизмов информационной безопасности для идентификации и аутентификации членов группы (роя), а также для обнаружения вторжений роботов-диверсантов.

Для реализации функций информационной безопасности РТК с роевым интеллектом предложено:

- включение в состав роя роботов-полицейских, выявляющих аномалии, вторжения, обеспечивающих идентификацию и аутентификацию агентов (в том числе за пределами роя), контроль разграничения доступа и противодействие роботам-диверсантам;
- обеспечение идентификации и аутентификации агентов и их сенсорных систем;
- обеспечение защиты от компрометации криптоключей по побочным каналам и при возможном физическом захвате их за пределами контролируемой зоны;
- обеспечение возможности обнаружения факта проведения атаки при действиях типа «ложный путь» по выявлению циклических маршрутов у отдельных групп роботов.

Основными особенностями структуры и поведения группы РТК, которые определяют ее потенциальные уязвимости, являются:

- недостаточная определенность текущего состояния, местоположения каждого устройства;
- относительно низкая интенсивность обмена информацией с координирующим центром;
- изначально заложенная автономность действий устройств;
- возможность действий устройств за пределами контролируемой зоны;
- несовершенство (отсутствие) механизмов идентификации и аутентификации устройств, приводящее к значительным задержкам при обнаружении вторжений в группу;
- ограниченные возможности по обнаружению аномального поведения элементов РТК.

Потенциальными угрозами для группы РТК являются:

- сбор информации (наблюдение и перехват передаваемых сообщений);
- несанкционированный доступ (подбор паролей доступа, обход алгоритмов аутентификации);
- отказ в обслуживании.

Последствиями указанных угроз могут быть:

- нарушение взаимодействия между РТК в группе;
- подмена РТК в группе или перехват управления агентами;
- дезорганизация группы агентов в РТК.

В работе [10] решается задача исследования скрытых деструктивных информационных воздействий, которая не решена применительно к беспилотным летательным аппаратам (БПЛА). Проведенный анализ показал уязвимость канала управления группой БПЛА для актуальных угроз безопасности информации. Большинство известных научных работ и полученных результатов исследований в данной предметной области неприменимы для групп БПЛА и рассчитаны на централизованную стратегию группового управления.

Авторами разработана теоретико-множественная модель управления роем БПЛА, эксперименты с которой позволяют выявлять и анализировать уязвимости в информационном взаимодействии элементов группы БПЛА, в том числе к скрытым информационным воздействиям. При этом авторы разделяют информационные взаимодействия (ИВ) в системе управления роем БПЛА на внутренние и внешние.

Во внутреннем ИВ участвуют следующие элементы: сенсоры и датчики, процессорное устройство, моторы и другие устройства, обеспечивающие выполнение функциональных задач агента (робота или БПЛА). При этом передается информация о местоположении, параметрах движения, препятствиях, техническом состоянии агента, команды для регулировки положения в пространстве.

Во внешнем ИВ участвуют агенты (БПЛА) как неделимые объекты. Информация, передаваемая между агентами, включает информацию о местоположении других агентов, местоположении препятствий в среде, техническом состоянии агентов.

Наиболее уязвимыми являются устройства регулирования положения в пространстве и дополнительные устройства, так как они являются последними элементами информационной цепи и получают наиболее искаженную информацию. Авторами проведен эксперимент, который показал, что элементы системы управления БПЛА в процессе внутреннего ИВ не имеют возможности идентифицировать нарушение целостности информации и оценить его как скрытое деструктивное информационное воздействие.

Вопросы защиты системы управления РТК от несанкционированного доступа явля-

ются одной из наименее исследованных областей групповой робототехники. Для обеспечения устойчивого управления группой РТК необходимо использовать функции идентификации и аутентификации членов группы, а также системы обнаружения несанкционированного доступа к управлению отдельными РТК. Преимущества технологии блокчейн позволяют обеспечить надежную идентификацию участников группы и предотвратить несанкционированный доступ к системе управления РТК. Также блокчейн-технология может решить проблему масштабируемости при распределенном коллективном принятии решений и упростить подготовку новых участников группы для присоединения к уже функционирующей группе РТК. Основным недостатком, обусловливающим проблему применения технологии блокчейн, является: латентность (большая задержка между отправкой информации о транзакции и моментом ее подтверждения в среднем 10 минут). Чем дольше группа работает, тем больше становится цепочка, для хранения которой требуется значительный ресурс памяти РТК. Пропускная способность блокчейн-систем ограничена несколькими транзакциями в секунду, а для относительно большой группы РТК этого недостаточно [11].

Таким образом, применяемые в настоящее время подходы к защите информационных ресурсов распределенных в пространстве объектов на основе анализа уязвимостей, угроз, контроля статистических параметров для выявления аномалий, контроля целостности информационных объектов не позволяют управлять процессом защиты в режиме реального времени. Требуется разработка новых методов и технологий для сокращения цикла контроля и гарантированного выполнения функций безопасности в распределенных динамических системах в режиме времени, близком к реальному.

Информационная модель взаимодействия конфликтующих систем

В ИУС РТК информационные ресурсы представлены преимущественно в электрическом виде.

В работе [12] авторами предложена классификация информационных ресурсов по признакам действий, совершаемых над информационными ресурсами:

- форма представления;
- метод формирования;
- метод проведения поиска;
- метод обработки;
- метод хранения;
- варианты распространения.

Авторами рассматриваются следующие методы формирования информационных ресурсов:

1. Исследование и формализация зависимостей, характеризующих реальные объекты, процессы или явления (применительно к природным объектам);
2. Измерение характеристик и их обработки с заданной целью (применительно к искусственным объектам);
3. Обработка массивов разнородных первичных ранее полученных данных с другими целями (выявление новых зависимостей).

В качестве специфических свойств информационных ресурсов выделяются:

- нерасходуемость;
- трансформируемость;
- полиморфичность;
- распространяемость;
- комплексируемость;
- концентрируемость.

Для реализации системного подхода требуется формализовать свойства защищаемых информационных ресурсов в соответствии с тремя обобщенными категориями свойств информационно-управляющей системы:

- структурные (сигналы, машинные носители, вычислительные и сетевые (коммуникационные) ресурсы, память);
- информационные (оперативная и служебная информация, математические модели, информационно-алгоритмическое обеспечение);
- функциональные (цель, задачи, процессы, действия).

Концептуально проблема реализации комплексного подхода к защите ИР СУ РТК имеет два основных аспекта, обусловленных объективными противоречиями при реализации требований к процессу управления и к системе управления:

а) обеспечение разведзащищенности ИУС РТК при заданных требованиях по производительности и управляемости;
б) обеспечение имитозащищенности ИУС РТК при заданных ограничениях по ресурсопотреблению.

Процесс принятия решения — ключевой процесс в общей структуре управления, который представляет собой процесс преобразования информации состояния в количественные (качественные) составляющие информации управления (командную информацию) для достижения заданной цели.

Процесс управления в СУВН имеет три

уровня общности:

1. Цикл управления;
2. Цикл выработки решения;
3. Цикл выработки вариантов и выбора способа решения.

Решения могут быть трех типов:

1. Информационные;
2. Организационные;
3. Оперативные.

Модель процесса принятия решения должна учитывать неопределенности вследствие отсутствия необходимой информации о возмущающих воздействиях (в том числе противника); практической невозможности выявления полного набора предпочтений лиц, принимающих решение; несовпадение предпочтений членов группы при групповом принятии решения. Неопределенности учитываются методами теории игр или нечетких множеств.

Информированность субъекта, принимающего решение, играет ключевую роль в решении и характеризуется тремя уровнями: а) детерминированный (при наличии полной и достоверной информации о возмущающих факторах); б) случай неопределенности (отсутствие информации о воздействующих факторах, кроме множества возможных состояний среды или стратегий противника); в) случай риска (имеется частичная информация о воздействующих факторах в виде некоторого распределения вероятности состояний среды или стратегий противника).

В условиях преднамеренного информационно-технического воздействия на РТК необходимо рассматривать взаимоотношения системы ИТВ и ИУС РТК в форме информационного конфликта. С позиций концепции информационного противоборства сущность информационного конфликта заключается в создании средствами ИТВ угроз нарушения безопасности информации в ИУС РТК и реагировании их на угрозы. Для противодействия ИТВ в СУ РТК организуется целенаправленная деятельность с применением аппаратно-программных средств защиты информации. Исход информационного конфликта в условиях ограниченных транспортно-вычислительных и интеллектуальных ресурсов системы ИТВ и ИУС РТК существенно зависит от качества управления ими. В процессе управления для обоснования стратегий, форм, методов и способов целенаправленного поведения при информационном конфликте необходимо выявить закономерности поведения систем ИТВ и ИУС РТК.

Основные трудности построения и управления подсистемой защиты обусловлены наличием в системе ИТВ интеллектуальной компоненты, позволяющей адаптировать и корректировать цели, формы, методы и способы воздействия.

Основной целевой функцией управления безопасностью сети связи в условиях информационного конфликта является минимизация времени обнаружения деструктивного фактора и достижение требуемого качества управления ресурсами, выделяемыми для его нейтрализации в течение времени информационного конфликта.

Для реализации целевой функции управления безопасностью сети связи требуется разработка модели, формализующей закономерные взаимосвязи процессов воздействия ИТВ и управления сетью связи по критерию минимизации времени обнаружения и обработки инцидентов, а также обоснования требований к циклу управления ресурсами для защиты от ИТВ. Модель должна включать в себя модель системы (процесса) защиты (как объекта контроля), модель ИТВ, модель системы (процесса) контроля [13].

Рассмотрим основные свойства информации и информационного взаимодействия, существенные для разработки модели информационного взаимодействия конфликтующих систем с позиций теоретической информатики [14].

Ценность информации — материальная или обобщенная полезность информационного объекта.

Обобщенная ценность информации — ассиметричная характеристика, которая определяется приемником, потребителем показателями экономии затрат, материалов, энергии, времени и других ресурсов.

Информативность сообщения или качество информации является асимметричной характеристикой, ее оценивает потребитель информации при решении своих задач, она определяется новизной поступившей информации для субъекта и ее адекватностью, достоверностью, характеризующей свойства источника информации, который косвенно оценивает информационные потребности в виде ожидаемых показателей информативности: полнота, объективность, своевременность полученных данных [14].

Информационная связь между объектами и субъектами — опосредованная зависимость между образами (моделями явлений), представляющими знания субъекта об этих явлениях.

Особенность взаимодействия информационных систем заключается в том, что при передаче субъектом информации он сам ее не теряет, за исключением материального носителя.

Другой особенностью информационной связи является гибкость составляющих ин-

формацию метазнаков — понятий, легко допускающих изменение и пополнение новыми смыслами в языковой системе, т. е. они способны быть заменителями заменителей при кодировании-декодировании, абстрагировании-конкретизации, обобщении-ограничении, идеализации проблемных ситуаций.

Модель взаимодействия информационных систем можно представить в виде трех уровней:

1. Сенсорный (физический);
2. Синтаксический (знаковый, символьный, понятийный);
3. Семантический (модельный, виртуальный).

Информационная связь между субъектами взаимодействия осуществляется передачей по каналу связи сообщений — знаковых структур.

Модель информационного обмена в СУ РТК включает в себя (рис.1):

- языковые субъекты: C1, C2;
- языки понимания (внутренние): L_1, L_2;
- языки общения (внешние): L_{12}, L_{21};
- языковая среда: первого субъекта — L_1, L_{12}; второго субъекта — L_2, L_{21};
- процессоры языковой среды: A,B,E,G,F_{m12};
- составные каналы связи: $\{(A,B,E,G)_1, F_{m12}, (A,B,E,G)_2\}_{1,2,...N}$;

N, M — количество простых каналов связи в составных прямом (от C1 к C2) и обратном (от C2 к C1) каналах связи;

И — имя понятия, знак;

Д — прямое семантическое значение знака;

К — косвенное семантическое значение знака;

А — ссылочное семантическое значение знака;

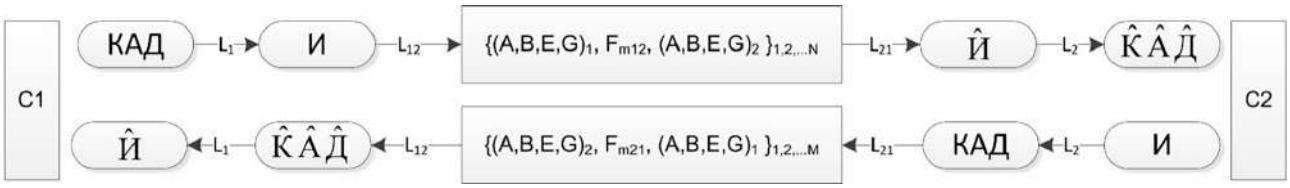

Рис.1 Обобщенная модель информационного обмена в системе управления РТК

Первый субъект (C1) синтезирует семантику КАД и передает ее второму субъекту (C2) по каналу связи с материальным процессором F_{m12}.

Второй субъект (C2) получает точную информацию И или искаженную И^, пытается исправить ошибки, распознать и декодировать семантику сообщения, встраивает в смысловые структуры К^А^Д^, в свою понятийную сеть.

Идеальная передача семантики сообщения К^А^Д^ произойдет при отсутствии ошибок кодирования КАД→И, декодирования И^→К^А^Д^, отсутствии синтаксических помех в канале связи И^=И, взаимно однозначном соответствии языков понимания $L_1 = L_2$ и общения $L_{12} = L_{21}$.

В общем случае взаимодействия информационных объектов (систем) связь не является симметричной. Информационный обмен дополнительно включает обратную связь с другим (или тем же) материальным процессором языковой среды (F_{m12} и F_{m21}).

Дефицит информационных ресурсов при выполнении регламентов в системе управления, возникающий в случае изменения обстановки и приводящий к потере управления, требует в теоретическом плане разработать модель синтеза информационных ресурсов в СУ РТК ВН.

СУ РТК ВН должна обеспечивать функционирование РТК ВН, при этом рациональным образом определять и устранять априорную неопределенность относительно внешних и внутренних деструктивных воздействий путем устранения дефицита информационных ресурсов и разрушения процесса функционирования ИИУС на основе формирования условия существования процесса функционирования РТК ВН.

Внутренние конфликты использования информационных ресурсов устраняются обеспечением интероперабельности взаимодействующих языковых субъектов [15] на трех уровнях в соответствии с эталонной моделью интероперабельности:

- организационном (согласование целей и задач взаимодействующих информационных систем, отличающихся внутренней структурой и процессами);
- семантическом (согласование смыслов сообщений и протоколов, алгоритмов информационных процессов);
- техническом (согласование форматов дан-

ных, сообщений и интерфейсов взаимодействующих подсистем).

Внешние информационные конфликты могут быть формализованы с помощью модели опосредованного информационного взаимодействия конфликтующих языковых субъектов, которые реализуют свои концепции управления относительно одного и того же объекта управления, которым является информационно-управляющая система РТК.

В то же время ИУС РТК сама является языковым субъектом, посредством которого происходит информационное взаимодействие системы управления РТК и системы управления технической разведкой и ИТВ противника.

Взаимодействующие языковые субъекты в конфликтных условиях (рис. 2):

C1 — интеллектуальная информационно-управляющая система РТК ВН (ИИУС);

C2 — система управления и контроля информационной безопасности РТК ВН (СУ и КИБ);

C3 — система технической разведки и информационно-технических воздействий противника на РТК ВН (СТР и ИТВ);

V и W — количество простых каналов в составных прямом и обратном каналах связи между СУ РТК ВН и СУ ТСР и ИТВ противника.

В известных публикациях недостаточно раскрыты процессы на первом уровне (сенсорном) информационного взаимодействия.

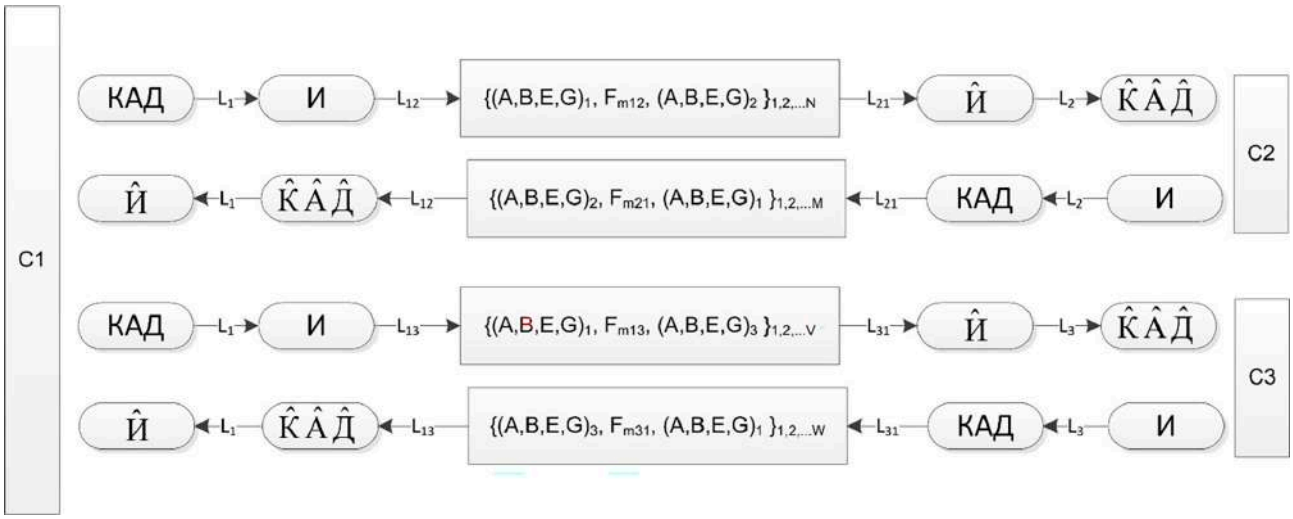

Рис.2. Модель опосредованного информационного взаимодействия конфликтующих языковых субъектов

Квантовая теория информации дает основания предполагать, что процесс измерения параметров материальных объектов с помощью сенсоров представляет собой передачу информации, точнее запрос на передачу информации от измеряемого объекта. На передачу информации затрачивается энергия источника (измеряемого объекта). Поэтому, если запас энергии (потенциал источника) измеряемого объекта минимальный (квант), то повторно измерить его свойство не возможно. Носитель информации исчезает (расходуется) в процессе передачи информации сенсору. В связи с этим можно предположить, что измерение будет успешным, если чувствительность сенсора (приемника), т. е. необходимая для информационной связи энергия, не превосходит энергетического потенциала источника (измеряемого объекта): $E_{изм} \leq E_0$. Т. е. при $E_{изм} = E_0$ повторное измерение не возможно. Результаты измерений характеризуются мерами точности, полноты, адекватности или мерами ошибки, неопределенности, погрешности $\Delta(x^*,x)$ между идеальной x и реальной x^* формами представления объекта. При идеализации реальных значений $(\Delta(x^*,x) = 0)$ достаточно одной формы представления информационного объекта $(x^* = x)$. При отсутствии идеального источника информации и идеального объекта x (для предельно точных измерений, у которых нет эталона сравнения), мера ошибки заменяется мерой вариативности, воспроизводимости информационного объекта x^*, который выступает в качестве собственного эталона в однород-

ном классе информационных ситуаций.

Сложные динамические системы, в том числе организационно-технические и киберфизические, содержат множество случайных взаимосвязей между подсистемами. Известен подход для повышения адекватности и точности измерений, включающий использование информационно-измерительного кванта в качестве меры неопределенности динамического состояния сложной системы [16]. Информационно-измерительный квант — представляет собой минимальное формирование, отражающее суть вероятностных физических процессов. Для построения измерительного кванта используется совместная оценка текущего значения разности и ее нормированного значения, связанной с аддитивной и мультипликативной изменчивостью объекта исследования. Формально-логическое построение информационно-измерительного кванта базируется на вероятностном представлении многофакторного и многоуровневого пространства. Мера информационно-измерительного кванта обладает свойствами самоподобия и дробной размерностью при условии конечного количества реализаций измеряемых параметров сложной системы [16].

Данный подход может использоваться при устранении конфликтов дефицита информационных ресурсов для распознавания ситуаций (выявления аномалий в работе системы), а также для оценки уровня доверия к информационным объектам (аутентификации) при внутренних информационных взаимодействиях.

Заключение

Таким образом, существование проблемы обеспечения информационной безопасности системы управления робототехническими комплексами проявляется через следующие симптомы:

- низкая эффективность боевого применения РТК;
- сложность управления РТК в боевых условиях в зоне огневого и радиоэлектронного поражения противником;
- недостаточная разведзащищенность и устойчивость информационно-управляющих систем РТК;
- недостаток унифицированных специализированных РТК ВН вследствие недостаточной оперативности в прогнозировании потребностей войск и отсутствии серийно выпускаемых типовых образцов;
- отсутствие массовости применения РТК в ходе боевых действий, невозможность получения системного эффекта от группового применения РТК, вследствие недостаточности разработки сценариев и общей тактики их боевого применения;
- совершенствование систем управления РТК и средств противодействия РТК происходит стихийно без явной тенденции к систематизации методов и средств;
- существующие методы оценки защищенности информационно-управляющих систем РТК от разведки и ИТВ противника не имеют общей теоретической основы и не позволяют получить обобщенные оценки для принятия оперативных решений по управлению группами РТК;
- существующие методы и технологии категорирования, защиты и контроля защищенности информации в системах связи и управления не позволяют своевременно контролировать увеличивающиеся многократно объемы информационных ресурсов в соответствии со степенью их важности (ценности);
- отсутствует единое понимание информационных ресурсов РТК, нет общей модели формирования и защиты информационных ресурсов РТК ВН.

Основными направлениями решения обозначенной проблемы являются:

1. Разработка подходов и методов к формированию, идентификации, классификации и категорированию по степени важности защищаемых информационных ресурсов системы управления РТК ВН;
2. Разработка и исследование моделей конфликтных условий функционирования системы управления РТК ВН;
3. Разработка моделей и методов обоснования требований защищенности информационных ресурсов системы управления РТК ВН;
4. Разработка моделей и методов защиты информационных ресурсов системы управления РТК ВН с учетом ее высокой структурной, информационной и функциональной динамики.

В рамках исследований в обозначенных направлениях проведен анализ базиса теоретической информатики и концепции информационно-измерительного кванта применительно к защите информационных ресурсов системы управления РТК ВН.

Литература

1. Костарев С.В., Карганов В.В., Липатников В.А. Технологии защиты информации в условиях кибернетического противоборства: Научн. монография / Под общ. ред. В.А. Липатникова. – СПб.: ВАС, 2020. – 716 с.: ил.
2. Методы радиоконтроля. Теория и практика: Монография / В.А. Липатников, О.В. Царик – СПб.: ГНИИ «НАЦРАЗВИТИЕ», 2018. – 608 с. – (Серия: Система технической защиты информации в Российской Федерации)
3. Пшихопов В. Х., Гонтарь Д. Н., Мартьянов О. В. Концептуальные подходы к формированию сценариев боевого применения групп робототехнических комплексов // Системы управления, связи и безопасности. 2022. № 3. С. 138–182. DOI: 10.24412/2410-9916-2022-3-138-182
4. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. – СПб.: Наукоемкие технологии, 2020. – 204 с.
5. Воробьев А.А., Сергеев В.В. Проблемы формирования облика специализированных робототехнических комплексов // Робототехника и техническая кибернетика. 9 (4). 2021. С.312-320.
6. Горский А.С., Демьянов В.В., Жуков А.О. // Проблемные вопросы создания наземных робототехнических комплексов. Робототехника и техническая кибернетика. 10 (2). 2022. С. 154-160.
7. Проблемы маскирования управляющих сигналов агентов мобильных робототехнических групп, Шумская О.О., Исхакова А.О. // XIII Всероссийское совещание по проблемам управления ВСПУ-2019. Москва 17-20 июня 2019 г.
8. Пшеничный Ф.И., Королев И.Д., Иванов С.В. Оценка показателей информационно-управляющей системы комплексов с беспилотными летательными аппаратами военного назначения в условиях информационно-технических воздействий // Наукоемкие технологии в космических исследованиях Земли. 2022. Т.14. №1. С. 28–35. DOI: 10.36724/2409-5419-2022-14-1-28-35
9. Пшеничный Ф.И., Королев И.Д. Модель оценки разведзащищенности группы беспилотных летательных аппаратов военного назначения от комплексов радио- и радиотехнической разведки // Электронный научный журнал «Инженерный вестник Дона». № 4. 2023. Ivdon.ru/ru/magazine/archive/n4y2023/8349.
10. Марненков Е.Д., Викснин И.И., Жукова Ю.А., Усова М.А. Анализ защищенности информационного взаимодействия группы беспилотных летательных аппаратов / Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, №5. С. 817-825.
11. Иванов Д.Я. Перспективы применения блокчейн-технологии в групповой робототехнике // Робототехника и техническая кибернетика. 2019. № 7(4). С. 300–305.
12. Стародубцев Ю.И. Экономика цифровых информационных услуг: монография / Ю.И. Стародубцев, М.А. Давлятова; под общей редакцией заслуженного деятеля науки РФ профессора Ю.И. Стародубцева. – СПб.:ПОЛИТЕХ-ПРЕСС, 2019. – 452 с.
13. Жидько Е.А., Разиньков С.Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта // Системы управления, связи и безопасности, 2018., №1 С. 122–135.
    УДК: 621.96:681.327.8
14. Зверев Г.Н. Теоретическая информатика и ее основания: В 2т. – Т.1. – М.: Физматлит, 2007. – 592 с. Т. 2. – М.: Физматлит, 2009. – 576 с.
15. Макаренко С.И. Интероперабельность человеко-машинных интерфейсов. Монография. – СПб.: Наукоемкие технологии, 2023. – 185 с.
16. Безбородова О.Е. Построение математической модели контролируемого объекта на основе анализа энтропии распределения информационно-измерительного кванта / О.Е. Безбородова, О.Н. Бодин, В.Г. Полосин, А.Г. Убиенных // Измерение. Мониторинг. Управление. Контроль. – 2019. - №2. – С. 76-84. – DOI: 10.21685/2307-5538-2019-2-9

THE PROBLEM OF ENSURING INFORMATION SECURITY OF CONTROL SYSTEMS FOR ROBOTIC COMPLEXES IN THE CONDITIONS OF THEIR COMBAT USE

Starodubtsev Yu.I.[1], Khudainazarov Yu.K.[2], Ermolaev V.E.[3]

Keywords: *concept of combat use, operational and tactical models, information management system, protected information resources, information model, conflicting systems, information and measurement quantum.*

Annotation

The article examines *the problem of ensuring information security of the control system of robotic complexes (RC).*

Based on the generalization *of the experience of using RC during a special military operation, the main disadvantages and the trend in the development of military-purpose RC control systems (MPRC) have been identified.*

The results of the analysis *of the main properties and requirements for the control systems of the RC as control systems for military purposes are presented. The main problems of increasing the efficiency of the control systems of the MPRC have been identified.*

The specific threats to the information security of the MPRC and shortcomings in the theory and practice of ensuring the information security of the MPRC management system are presented, the main symptoms of the problem are identified. The currently known theoretical models do not reflect the essential features of the formation and protection of information resources of the MPRC management system, which does not allow ensuring the adequacy of the protection system.

The novelty *lies in the formalization of information interaction between objects and subjects of the MPRC management system in the basis of theoretical computer science. The information model of interaction in conflict conditions can be the basis for developing a model for the formation and protection of information resources of the MPRC management system, and the concept of an information and measurement quantum can be used to eliminate the shortage of information resources and increase confidence in intelligent information management systems.*

References

1. Kostarev S.V., Karganov V.V., Lipatnikov V.A. Tehnologii zashhity informacii v uslovijah kiberneticheskogo protivoborstva: Nauchn. Monografija / Pod obshh. red. V.A. Lipatnikova. – SPb.: VAS, 2020. – 716 s.: il.
2. Metody radiokontrolja. Teorija i praktika: Monografija / V.A. Lipatnikov, O.V. Carik – SPb.: GNII «NACRAZVITIE», 2018. – 608 s. – (Serija: Sistema tehnicheskoj zashhity informacii v Rossijskoj Federacii)
3. Pshihopov V. H., Gontar' D. N., Mart'janov O. V. Konceptual'nye podhody k formirovaniju scenariev boevogo primenenija grupp robototehnicheskih kompleksov // Sistemy upravlenija, svjazi i bezopasnosti. 2022. № 3. S. 138–182. DOI: 10.24412/2410-9916-2022-3-138-182
4. Makarenko S. I. Protivodejstvie bespilotnym letatel'nym apparatam. Monografija. – SPb.: Naukoemkie tehnologii, 2020. – 204 s.
5. Vorob'ev A.A., Sergeev V.V. Problemy formirovanija oblika specializirovannyh robototehnicheskih kompleksov // Robototehnika i tehnicheskaja kibernetika. 9 (4). 2021. S. 312-320.
6. Gorskij A.S., Dem'janov V.V., Zhukov A.O. // Problemnye voprosy sozdanija nazemnyh robototehnicheskih kompleksov. Robototehnika i tehnicheskaja kibernetika. 10 (2). 2022. S. 154-160.
7. Problemy maskirovanija upravljajushhih signalov agentov mobil'nyh robototehnicheskih grupp, Shumskaja O.O., Ishakova A.O. // XIII Vserossijskoe soveshhanie po problemam upravlenija VSPU-2019 Moskva 17-20 ijunja 2019 g.
8. Pshenichnyj F.I., Korolev I.D., Ivanov S.V. Ocenka pokazatelej informacionno-upravljajushhej sistemy kompleksov s bespilotnymi letatel'nymi apparatami voennogo naznachenija v uslovijah informacionno-tehnicheskih vozdejstvij // Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli. 2022. T.14. №1. S. 28–35. DOI: 10.36724/2409-5419-2022-14-1-28-35

[1]Yuri I. Starodubtsev, Dr.Sc., Professor, Professor of the Department of Security of Information and Communication Systems for Special Purposes at the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E mail: starodub@mail.ru

[2]Yuri K. Khudainazarov, Ph.D., Doctoral student of the Department of Security of Information and Communication Systems for Special Purposes of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny, St. Petersburg, Russia. E-mail: yu-78@ya.ru

[3]Vladimir E. Ermolaev, Adjunct of the Department of Security of Special Purpose Information and Communication Systems, Marshal of the Soviet Union Military Academy of Communications, St. Petersburg, Russia. E-mail: VErmol@ya.ru

9. Pshenichnyj F.I., Korolev I.D. Model' ocenki razvedzashhishhennosti gruppy bespilotnyh letatel'nyh apparatov voennogo naznachenija ot kompleksov radio- i radiotehnicheskoj razvedki // Jelektronnyj nauchnyj zhurnal «Inzhenernyj vestnik Dona». №4. 2023. Ivdon.ru/ru/magazine/archive/n4y2023/8349.
10. Marnenkov E.D., Viksnin I.I., Zhukova Ju.A., Usova M.A. Analiz zashhishhennosti informacionnogo vzaimodejstvija gruppy bespilotnyh letatel'nyh apparatov / Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2018. T. 18, №5. S. 817-825.
11. Ivanov D.Ja. Perspektivy primenenija blokchejn-tehnologii v gruppovoj robototehnike // Robototehnika i tehnicheskaja kibernetika. 2019. № 7(4). S. 300–305.
12. Starodubcev Ju.I. Jekonomika cifrovyh informacionnyh uslug: monografija / Ju.I. Starodubcev, M.A. Davljatova; pod obshhej redakciej zasluzhennogo dejatelja nauki RF professora Ju.I. Starodubceva. – SPb.:POLITEH-PRESS, 2019. – 452 s.
13. 1Zhid'ko E.A., Razin'kov S.N. Model' podsistemy bezopasnosti i zashhity informacii sistemy svjazi i upravlenija kriticheski vazhnogo ob#ekta //Sistemy upravlenija, svjazi i bezopasnosti №1, 2018. S. 122–135. UDK: 621.96:681.327.8
14. Zverev G.N. Teoreticheskaja informatika i ee osnovanija: V 2t. – T.1. – M.: Fizmatlit, 2007. – 592 s. T. 2. – M.: Fizmatlit, 2009. – 576 s.
15. Makarenko S.I. Interoperabel'nost' cheloveko-mashinnyh interfejsov. Monografija. – SPb.: Naukoemkie tehnologii, 2023. – 185 s.
16. Bezborodova O.E. Postroenie matematicheskoj modeli kontroliruemogo ob#ekta na osnove analiza jentropii raspredelenija informacionno-izmeritel'nogo kvanta / O.E. Bezborodova, O.N. Bodin, V.G. Polosin, A.G. Ubiennyh // Izmerenie. Monitoring. Upravlenie. Kontrol'. – 2019. – № 2. – S. 76-84. – DOI: 10.21685/2307-5538-2019-2-9