ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ СИСТЕМ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ

Стародубцев Ю.И.[1], Лаута О.С.[2], Худайназаров Ю.К.[3]

DOI:10/24682/3034-4050-2024-2-43-52

Ключевые слова: *информационно-управляющая система, защищаемые информационные ресурсы, угрозы информационной безопасности, комплексный подход.*

Аннотация

Цель: *предложить решение задачи анализа особенностей защиты информационных ресурсов (ИР) системы управления робототехническими комплексами (РТК).*

Метод: *использован системный подход для анализа состава, функций, роли и места информационно-управляющей системы в системе управления современных и перспективных РТК. Методом аналитического моделирования представлены основные противоречия в теории управления РТК военного назначения (ВН).*

Результат: *приведены результаты анализа защищаемых информационных ресурсов в информационно-управляющей системе робототехнического комплекса: информации, носителей информации и информационных процессов. Выявлены основные особенности применяемых протоколов информационного взаимодействия в соответствии с эталонной моделью OSI.*

Представлены результаты анализа угроз информационной безопасности и функциональные составляющие комплексной системы защиты информационных ресурсов системы управления робототехническими комплексами.

Научная новизна: *заключается в формализации объективных противоречий в свойствах процесса управления РТК ВН между непрерывностью и скрытностью, а также между свойствами системы управления РТК: ограниченность ресурсов (вычислительных, сетевых и памяти) для реализации функций безопасности; высокая динамика структурных, информационных и функциональных характеристик защищаемых ресурсов Следствием указанных противоречий является необходимость комплексирования разнородных методов и средств защиты, а также управления в реальном масштабе времени задачами и информационными ресурсами информационно-управляющей системы (ИУС) РТК ВН.*

Известные в настоящее время методы и технологии не позволяют учесть все особенности ИР системы управления РТК как объекта защиты и обеспечить адекватность системы защиты угрозам и состоянию защищаемых ресурсов при их высокой динамичности.

Введение

В современных условиях перехода к массовому применению робототехнических комплексов военного назначения, проблемной областью является отсутствие методологии оптимального управления РТК ВН при выполнении задач вне контролируемой зоны в условиях деструктивных внешних воздействий.

Одной из проблем в данной области является защита информационных ресурсов системы управления РТК ВН.

Под робототехническим комплексом (РТК) понимается[4] комплекс, состоящий из одного или нескольких роботов, их рабочих органов и любых механизмов, оборудования, приборов или датчиков, обеспечивающих выполнение роботом функционального назначения (задания).

Система управления (СУ) РТК представляет собой совокупность управляющей логики и силовых функций, позволяющих контролировать и управлять механической конструкцией робота, а также осуществлять взаимосвязь с внешней средой (оборудованием и пользователями). СУ РТК ВН относится к специальным системам управления оружием, в частности к информационно-техническим системам реального времени, которые используют ресурс специальных (выделенных) направлений и сетей связи.

Оператор — лицо, уполномоченное запускать,

[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. E-mail: starodub@mail.ru

[2]Лаута Олег Сергеевич, доктор технических наук, профессор кафедры Государственного университета морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия. E-mail: laos-82@yandex.ru

[3]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

[4]ГОСТ Р 60.0.0.4 — 2019/ИСО 8373:2012 Роботы и робототехнические устройства. Термины и определения.

контролировать и останавливать выполнение заданной операции роботом или робототехническим комплексом.

Информационные ресурсы РТК ВН включают в себя: оперативные данные, которые хранятся, передаются и обрабатываются в системе управления СУ РТК; данные, которые обеспечивают функционирование элементов СУ РТК (программные коды микроконтроллеров, программные агенты, операционная система, используемые протоколы информационного обмена (форматы сообщений, идентификаторов, алгоритмы обработки данных), структура и параметры используемых сигналов).

Ключевое значение в координации и управлении группой РТК имеет информационно-управляющая система (ИУС). Рассмотрим основные особенности информационно-управляющей системы группы РТК.

Информационно-управляющая система (ИУС) группы РТК представляет собой высокоуровневую систему, которая позволяет координировать и управлять действиями нескольких робототехнических устройств, работающих совместно. Такие системы могут использоваться в различных контекстах, например, в промышленной автоматизации, военной технике, логистике и многих других областях. Основные элементы такой системы следующие.

1. Центральный управляющий узел (центральный контроллер), выполняет функции: планирования, мониторинга и координации действий всей группы роботов; управления общими задачами и распределения задач между роботами; обработки данных, поступающих от всех роботов, с целью принятия решений.
2. Индивидуальные контроллеры роботов выполняют функции: локального управления и контроля каждого робота; реализации задач, полученных от центрального управляющего узла; обратной связи с центральным узлом, включая отчеты о выполнении задач и состояние робота.
3. Средства связи включают в себя: беспроводные или проводные каналы связи для обмена данными между центральным узлом и индивидуальными роботами; средства синхронизации и координации действий между роботами.
4. Сенсорные системы включают в себя: датчики и сенсоры, установленные на роботах для сбора информации о внешней среде и собственном состоянии (например, камеры, лидары, GPS, датчики положения и движения); средства обработки и передачи сенсорных данных для принятия решений и выполнения задач.
5. Аналитические модули могут включать в себя: модули для обработки данных и анализа информации (например, модуль машинного зрения, модуль распознавания образов, алгоритмы машинного обучения); средства оптимизации маршрутов, прогнозирование ситуаций и принятие решений на основе анализа данных [1].
6. Интерфейсы пользователя включают в себя: консоли управления для операторов, где можно задавать задачи, мониторить состояние системы, получать отчеты и управлять отдельными роботами; графические интерфейсы, панели управления и системы визуализации.
7. Подсистемы обеспечения безопасности могут включать: механизмы для предотвращения коллизий между роботами и с окружающей средой; средства аутентификации и защиты от несанкционированного доступа.
8. Энергетическая подсистема: источники питания для роботов и централизованных систем; механизмы управления энергопотреблением и резервирования энергии для надежной работы всей системы.

Основные функции ИУС включают:

1. Сбор информации. ИУС собирает данные от различных сенсоров и устройств, установленных на роботах, а также от внешних источников, таких как камеры наблюдения, GPS и т. д.
2. Анализ данных. ИУС обрабатывает и анализирует собранные данные для принятия решений. Этот анализ может включать обнаружение препятствий, определение оптимальных маршрутов движения и т.д.
3. Планирование задач. ИУС распределяет задачи между роботами на основе алгоритмов, которые могут учитывать текущие состояния роботов, их расположение, и другие релевантные данные.
4. Обмен информацией. ИУС обеспечивает быстрое и надежное взаимодействие между всеми членами группы роботов, что позволяет координировать их действия и предотвращать конфликты.
5. Безопасность и защита. ИУС включает меры по защите информации и предотвращению несанкционированного доступа. В области информационной безопасности это особенно важно для предотвращения кибератак и обеспечения целостности данных.
6. Мониторинг и контроль. ИУС непрерывно отслеживает состояние и выполнение задач каждым роботом, а также может вмешиваться в случае возникновения проблем.

Таким образом, информационно-управляющая система является центральной частью системы управления робототехнических комплексов, обеспечивая синхронизацию, координацию и выполнение задач в соответствии с заданными параметрами и условиями.

В соответствии с моделью OSI (Open Systems Interconnection) ИУС группы РТК, можно рассмотреть на каждом из семи уровней. Для обеспечения

информационного взаимодействия робототехнических комплексов на каждом уровне в рамках модели OSI выполняются функции с использованием соответствующих протоколов информационного обмена (табл. 1).

1. Физический уровень (Physical Layer): обеспечивается функция физического соединения между устройствами. Параметры физического уровня включают электрические и механические характеристики интерфейсов и среды передачи. Реализация в составе ИУС группы РТК предполагает использование разнообразных физических сред, таких как радиочастоты (Wi-Fi, Zigbee), оптоволокно или другие беспроводные технологии для соединения роботов друг с другом.
2. Канальный уровень (Data Link Layer): обеспечивается функция надёжной передачи данных через физические соединения. Обнаружение и исправление ошибок на уровне кадра. Реализация в составе ИУС группы РТК предполагает использование протоколов MAC (Media Access Control) для управления доступом к общей среде передачи. Применяются технологий, такие как Bluetooth или Zigbee, которые включают функции ARQ (Automatic Repeat reQuest) для коррекции ошибок.
3. Сетевой уровень (Network Layer): реализуется функция определения маршрутов данных между устройствами. Управление логическими адресами и маршрутизацией пакетов. В составе ИУС группы РТК может обеспечиваться использованием протоколов маршрутизации, таких как OLSR (Optimized Link State Routing) или RPL (Routing Protocol for Low-power and Lossy Networks), чтобы обеспечить эффективную маршрутизацию данных между роботами в динамическом окружающем пространстве.
4. Транспортный уровень (Transport Layer): реализуется функция надёжной передачи данных между хостами. Установление, поддержание и завершение соединений, контроль перегрузок и восстановление данных при ошибках. В составе ИУС группой РТК может обеспечиваться применением UDP (User Datagram Protocol) для приложений, требующих минимальной задержки, или TCP (Transmission Control Protocol) для приложений, где требуется надёжность.
5. Сеансовый уровень (Session Layer): реализуется функция управления сеансами связи, установления, координации и завершения сеансов между взаимодействующими устройствами. В составе ИУС группой РТК данная функция может обеспечиваться с использованием протоколов для установления и управления сессиями данных, например, с помощью WebSocket для сессионных взаимодействий между группами роботов.
6. Представительный уровень (Presentation Layer): реализуется интерпретация данных между различными формами данных, кодирование, дешифрование и сжатие данных. В составе ИУС группы РТК функция может обеспечиваться с помощью кодирования сообщений данных с использованием стандартов, таких как JSON или XML, для унифицированного формата обмена данными между различными подсистемами РТК.
7. Прикладной уровень (Application Layer): реализуется поддержка специфических сетевых приложений, таких как удалённое управление, коммуникация и совместная работа. В составе ИУС группы РТК может обеспечиваться с использованием протоколов приложения, таких как MQTT (Message Queuing Telemetry Transport) для обмена телеметрической информацией между роботами, или RESTful API для взаимодействия с внешними системами.

Таблица 1.

Эталонная модель информационного взаимодействия элементов РТК

Уровень по OSI	***Выполняемые функции***	***Технологии, стандарты и протоколы***
Прикладной уровень	Поддержка специфических сетевых приложений, таких как удалённое управление, коммуникация и совместная работа	MQTT (Message Queuing Telemetry Transport), RESTful API
Представительный уровень	Интерпретация данных между различными формами данных, кодирование, дешифрование и сжатие данных	JSON или XML
Сеансовый уровень	Управление сеансами связи, установления, координации и завершения сеансов между взаимодействующими устройствами	WebSocket
Транспортный уровень	Надёжная передача данных между хостами. Установление, поддержание и завершение соединений, контроль перегрузок и восстановление данных при ошибках	UDP (User Datagram Protocol) или TCP (Transmission Control Protocol)

Уровень по OSI	*Выполняемые функции*	*Технологии, стандарты и протоколы*
Сетевой уровень	Определение маршрутов данных между устройствами, управление логическими адресами и маршрутизацией пакетов	OLSR (Optimized Link State Routing) или RPL (Routing Protocol for Low-power and Lossy Networks)
Канальный уровень	Надёжная передача данных через физические соединения. Обнаружение и исправление ошибок на уровне кадра	MAC (Media Access Control), технологий, такие как Bluetooth или Zigbee, которые включают функции ARQ (Automatic Repeat reQuest) для коррекции ошибок
Физический уровень	Физическое соединение между устройствами. Параметры физического уровня включают электрические и механические характеристики интерфейсов и среды передачи	Wi-Fi, Zigbee

Рассматривая взаимодействие РТК в составе группы, важно учитывать, что успешная работа на каждом из уровней OSI зависит от корректного функционирования и координации между этими уровнями. Современные подходы в кибернетике и робототехнике часто интегрируют решения, обеспечивающие надёжную и эффективную коммуникацию на каждом уровне модели OSI.

Первым этапом построения системы защиты является определение защищаемых информационных ресурсов ИУС группы РТК. Они могут быть классифицированы следующим образом:

1. Данные сенсоров и датчиков: данные позиционирования (GPS, LIDAR, камеры, инерциальные измерительные единицы (IMU)); данные окружающей среды (от сенсоров температуры, давления, освещения, влажности и других); тактические и стратегические данные (от сенсоров, которые обеспечивают понимание текущей ситуации в рабочей зоне).
2. Коммуникационные каналы: каналы прямой связи (беспроводные сети (Wi-Fi, LTE, радиосвязь), проводные сети (Ethernet и другие)); ретрансляторы и хабы (беспилотные летательные аппараты (БЛА), действующие как ретрансляторы сигналов);
3. Средства обработки данных и вычислительные ресурсы: серверы и облачные вычисления (обеспечение высокопроизводительных вычислений, анализа данных, машинного обучения); локальные вычислительные мощности (встроенные процессоры, ПЛИС и микроконтроллеры, выполняющие локальные вычисления на уровне каждого РТК);
1. Командные и управляющие системы: программное обеспечение для управления (алгоритмы и программы для сценарного управления, маршрутизации, координации действий); интерфейсы управления (системы ЧМИ (человеко-машинного интерфейса) для операторов);
2. Подсистема технического контроля: информационные базы данных о состоянии РТК (оперативная информация о текущем состоянии, результатах диагностики и техническом обслуживании).
3. Подсистема информационной безопасности: средства и функции шифрования и аутентификации (защита передаваемых и обрабатываемых данных от несанкционированного доступа); системы обнаружения вторжений (анализ сетевого трафика и активности для выявления аномалий и потенциальных угроз); другие подсистемы, реализующие политику безопасности и процедуры (набор правил и процедур для защиты информационных ресурсов).

Для формализации свойств указанных защищаемых ресурсов целесообразно их систематизировать в соответствии с тремя обобщенными категориями свойств информационно-управляющей системы:

- информационная (оперативная и служебная информация, математические модели, информационно-алгоритмическое обеспечение);
- структурная (вычислительные и сетевые (коммуникационные) ресурсы, память);
- функциональная (цель, задачи, процессы, действия).

Каждая из этих категорий информационных ресурсов имеет свою составляющую в общей эффективности и безопасности системы управления группой РТК, определяя выполнимость задач в разнообразных оперативных ситуациях и условиях.

Рассмотрим основные угрозы безопасности информационным ресурсам СУ группой РТК. Для СУ группой РТК существуют различные угрозы безопасности информационным ресурсам. Важно учитывать как внешние, так и внутренние угрозы:

1. Кибератаки (специальные программные воздействия): Malware, Ransomware (программное обеспечение, которое может скомпрометировать данные или нарушить функционирование робототехнических комплексов); фишинг (попытки обманом получить конфиденциальную информацию, такую как учетные данные или ключи доступа); DDoS (распределенные атаки отказа в обслуживании) (перегрузка сетевой инфраструктуры системы управления, приводящая к исчерпанию ресурсов);
2. Компрометация сетевой безопасности: снифинг трафика (сбор данных, передаваемых по сети, который может позволить злоумышленникам получить доступ к конфиденциальной информации); Man-in-the-Middle (атака «человек посередине») (перехват и изменение трафика между компонентами системы); беспроводные угрозы (использование незащищенных беспроводных соединений, что может позволить противнику получить доступ к управлению роботами);
3. Компрометация устройств и сенсоров: физический доступ (незаконное проникновение и физическая манипуляция устройствами или сенсорами); внедрение фальшивых сенсоров (введение ложных данных через сенсоры для дезориентации системы управления);
4. Уязвимости программного обеспечения: ошибки в коде (уязвимости из-за ошибок в программном обеспечении, которое управляет роботами); уязвимости программного обеспечения (использование устаревшего программного обеспечения с известными уязвимостями); недостаточная аутентификация и авторизация (неадекватные меры контроля доступа могут позволить неавторизованным пользователям получить доступ к системе управления);
5. Человеческий фактор: внутренние угрозы (обслуживающий персонал или операторы системы, которые могут преднамеренно или случайно скомпрометировать безопасность); неправильная конфигурация (ошибки в настройке системы, которые могут оставить уязвимости);
6. Социальная инженерия: (использование методов психологического влияния на обслуживающий персонал или на операторов РТК для получения доступа к конфиденциальной информации или системам).

Для защиты информационных ресурсов СУ группой РТК необходимо комплексно использовать методы и средства по следующим направлениям защиты:

1. Обеспечение сетевой безопасности (использование шифрования для защиты данных при передаче, установка межсетевых экранов и систем обнаружения вторжений (IDS));
2. Обеспечение программно-алгоритмической безопасности (кибербезопасности): регулярное обновление программного обеспечения, применение антивирусного ПО и брандмауэров, а также регулярные проверки на наличие уязвимостей (Penetration Testing);
3. Обеспечение защиты от несанкционированного физического доступа (ограничение доступа к устройствам, защита сенсоров от несанкционированного воздействия);
4. Обучение персонала: обучение операторов методам распознавания фишинговых атак, способам управления безопасностью данных и мероприятиям при нарушении безопасности;
5. Контроль и управление доступом (использование многофакторной аутентификации (MFA) и роли доступа (RBAC) для ограничения доступов к системам управления) [2];
6. Мониторинг и логирование: постоянный мониторинг систем и анализ логов для своевременного обнаружения аномалий и инцидентов безопасности [3].

Основные научно-теоретические проблемы разработки методологии защиты информационных ресурсов связаны с построением сетецентрической системы управления РТК ВН, позволяющей оперативно реагировать на изменения обстановки и перераспределять задачи и ресурсы.

Отличительными особенностями сетецентрического подхода, по сравнению с традиционным, являются:

- возможность согласованного испольвания географически распределенных сил и средств;

самосинхронизация сил, участвующих в операции (боевых действиях);

- высокая динамичность, активность и результативность всех процессов управления и самих боевых действий;
- изменение формы военных действий, которая от последовательных боев и операций с соответствующими промежутками (паузами) между ними, приобретает форму непрерывных высокоскоростных действий (операций, акций) с решительными целями;
- наличие сети связи между системами и средствами управления войсками и оружием, что дает возможность на обширном географическом пространстве проводить совместные действия, а также динамически наилучшим образом распределять ответственность и объем задач между различными подразделениями применительно к текущей обстановке.

Основная суть сетецентричекого подхода в возможности оперативного обмена информацией и многоуровневой самоорганизации для гарантированного выполнения поставленных задач в заданные сроки.

Новый облик ВС РФ предусматривает многоуровневую систему управления боевыми действиями в регионе конфликта. Поэтому для формирования структуры и требований к элементам сетецентрической системы управления необходимо определение принципа разграничения полномочий между различными иерархическими уровнями.

Основными недостатками в практике создания сетецентрических систем управления являются следующие [5].

1. Сетецентрические системы управления предполагают сбор и интеграцию различных средств и систем разведки, работающих на различных физических принципах в различных диапазонах длин волн в единую интегрированную базу данных. В то же время в научно-методическом плане не существует проверенных на практике и эффективных методов и способов идентификации целей, объединения и отождествления разнородных данных, обеспечивающих высокую вероятность обнаружения и идентификации целей.
2. Методы многомерной многофакторной оптимизации разработаны для крайне ограниченных и простых условий и функций и, как правило, не пригодны для сложных нелинейных функций с ярко выраженными корреляционными связями между основными параметрами этих функций. Поэтому требуется разработка методов синтеза сложных сетецентрических систем управления.
3. Проблема опознавания «свой-чужой» не имеет надежных методов и технических средств для распознавания своих сил и средств на поле боя. Требуется постановка комплекса поисковых и прикладных исследований для определения путей решения данной проблемы.

Построение защищенной сетецентрической СУ РТК позволит значительно повысить устойчивость управления группой РТК в конфликтных условиях. Обеспечение защиты информационных ресурсов СУ группой РТК основывается на анализе и формализации процессов информационного обмена в группе РТК, моделировании угроз информационной безопасности и определении комплекса защитных мер. Необходимо учесть особенности различных сценариев применения РТК военного назначения (ВН) [4], применяемых в составе группы.

К СУ РТК ВН предъявляются требования по следующим свойствам [5]:

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 перемещать 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).

При выполнении требований к сетецентрической системе управления [6], [7] возникает объективное противоречие между свойствами безопасности и производительности. Наглядным является графическое представление указанного противоречия при обеспечении выполнения требований к СУ РТК ВН (рис. 1).

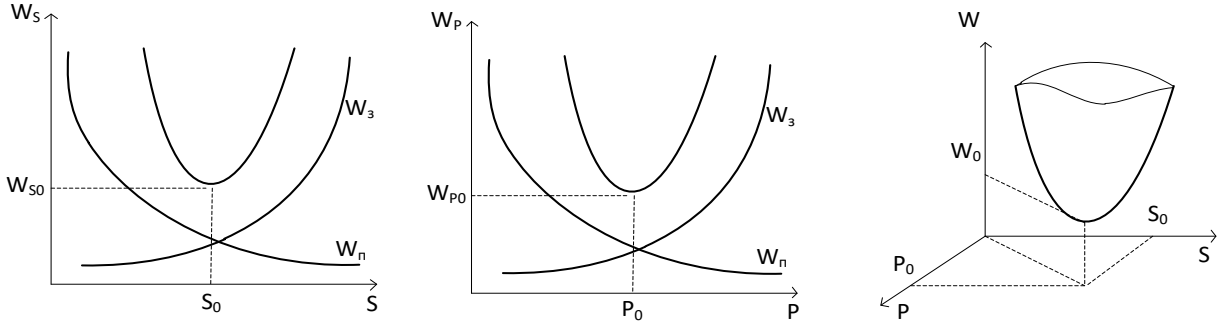

Рис. 1. Условия оптимальности управления РТК ВН

Проблема защиты ИР СУ РТК обусловлена объективными противоречиями при обеспечении выполнения требований к системе управления военного назначения: обеспечение безопасности ИУС РТК при заданных требованиях по производительности ИУС.

Пусть P — производительность ИУС РТК;

S — безопасность ИУС РТК;

$W_п(S)$ — потери при нарушении безопасности ИУС РТК;

$W_з(S)$ — затраты на обеспечение безопасности ИУС РТК.

Тогда условие оптимальности для безопасности ИУС РТК:

$$W_{S0}=min\ (W_п(S)+W_з(S)) \text{ при } P=const \quad (1)$$

Пусть $W_п(P)$ — потери, обусловленные недостаточной производительностью ИУС РТК;

$W_з(P)$ — затраты на обеспечение производительности ИУС РТК;

Тогда условие оптимальности для обеспечения производительности ИУС РТК:

$$W_{P0}=min\,(W_п(P)+W_з(P)) \text{ при } S=const \quad (2)$$

При функционировании ИУС должны выполняться оба условия оптимальности (безопасности и производительности) ИУС РТК:

$$W_{02}=min\,(W_{S0}+W_{P0}) \quad (3)$$

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

- обеспечение скрытности управления РТК при заданных требованиях непрерывности управления;
- обеспечение имитозащищенности ИУС РТК при заданных ограничениях по производительности ИУС.

Интероперабельность может быть своевременным дополнением существующего перечня требований к СУВН.

Интероперабельность[5] — способность двух и более информационных систем к обмену информацией и к использованию информации, полученной в результате обмена. Это свойство играет ключевую роль при создании, развитии и объединении информационных систем различных типов и назначения.

Другим актуальным требованием к системе управления военного назначения при возрастании степени ее интеллектуальности является «доверие» к искусственному интеллекту (ИИ).

Для РТК ВН особенностью применения обусловлено требование доверия к ИИ (объяснимость работы ИИ и процесса достижения им результатов).

Доверие[6] к системе искусственного интеллекта — уверенность потребителя, и при необходимости, организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, и иных заинтересованных сторон в том, что система способна выполнять возложенные на нее задачи с требуемым качеством.

[5]ГОСТ Р 59796 — 2021 Информационные технологии. Интероперабельность. Термины и определения.

[6]ГОСТ Р 59276 — 2020 Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения.

Доверенная система искусственного интеллекта — система искусственного интеллекта, в отношении которой потребитель и, при необходимости, организации, ответственные за регулирование вопросов создания и применения систем искусственного интеллекта, проявляют доверие.

Требуется поиск новых подходов для обеспечения скрытности и непрерывности управления, разработка новых методов и технологий для защиты ИР СУ РТК, позволяющие при ограниченных вычислительных, транспортных возможностях и памяти контролировать параметры целостности (имитозащищенность) разнородных информационных ресурсов в режиме реального времени.

Для разрешения указанных противоречий в теории и практике управления РТК ВН требуется проведение междисциплинарных исследований, разработка соответствующей методологии на основе новых подходов к моделированию современных информационно-телекоммуникационных систем в условиях информационного конфликта[8], исследование теоретических основ интеллектуализации ИУС РТК на основе современных методов и технологий управления сложными организационно-техническими системами в режиме реального времени [9], исследование методов и технологий формализации свойств и моделирования сложных систем [10], разработка новых методов и технологий управления сетевой безопасностью в информационно-телекоммуникационных сетях [11], а также мониторинга состояния информационно-телекоммуникационных сетей [12].

Выводы

Управление группами РТК (или роями роботов) является одной из наиболее сложных проблем в робототехнике и искусственном интеллекте. Основные аспекты данной проблемы следующие:

1. Самоорганизация и координация РТК в группе предполагают решение двух задач на оперативном и тактическом уровнях управления, связанных с особенностями сценариев применения РТК в составе группы: целеполагание (обеспечение синхронных и согласованных действий роботов с минимальными задержками и энергетическими затратами для решения групповой задачи) и целераспределение (эффективное распределение частных задач между роботами, чтобы максимизировать продуктивность и минимизировать дублирование усилий).
2. Коммуникация (применение технологий, обеспечивающих своевременность и достоверность связи между роботами в условиях, где могут быть помехи или ограничения по частоте, применение протоколов связи, которые могут масштабироваться для больших групп роботов);
3. Децентрализованное управление (создание алгоритмов, где каждый робот может принимать решения на основе ограниченной локальной информации; сокращение этапов и эпизодов функционирования группы РТК с необходимостью центрального управляющего узла, который может стать уязвимым из-за одного точечного отказа);
4. Работа в неизвестной и изменяющейся среде (разработка алгоритмов обеспечивающих способность группы робототехнических комплексов адаптироваться к непредсказуемым изменениям в окружающей среде, а также для исследования и картографирования неизвестных территорий);
5. Энергоэффективность (разработка стратегий для минимизации энергозатрат в процессе выполнения задач, создание систем для автономного подзаряда или распределения энергии среди роботов или оптимального распределения задач);
6. Обнаружение и разрешение внутренних конфликтов (создание алгоритмов, которые позволяют роботам избегать столкновений друг с другом и с окружающими объектами, эффективное разрешение конфликтов между роботами при доступе к ограниченным ресурсам);
7. Информационная безопасность и устойчивость к сбоям (защита группы роботов от информационно-технических воздействий, обеспечение устойчивости группы (роя или стаи) при выходе из строя одного или нескольких роботов).

Исследование этих проблемных аспектов требуют междисциплинарного подхода, включающего методы из области искусственного интеллекта, теории управления, коммуникаций.

Литература

1. Юмашева Е.С., Ныркова А.П. Применение алгоритмов машинного обучения для обнаружения аномального поведения в сетях критической информационной инфраструктуры // В сборнике: Региональная информатика и информационная безопасность. Сборник трудов Санкт-Петербургской международной конференции. Санкт-Петербург, 2023. С. 247–251.

2. Ныpков А.П., Соколов С.С., Алимов О.М., Черный С.Г., Доровской В.А. Оптимальная идентификация объектов в задачах распознавания необитаемыми подводными аппаратами // Проблемы информационной безопасности. Компьютерные системы. 2020. № 2. С. 58–64.
3. Мартынов В.Л., Ныpков А.П., Шиманская М.С., Кречетова Э.В., Шиманская Г.С. Гидроакустические коммуникации в вопросах противодействия подводным роботам // Информатизация и связь. 2024. № 2. С. 51–55.
4. 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
5. Боговик А.В., Игнатов В.В. Теория управления в системах военного управления: Учебн. – СПб.: ВАС, 2008. – 460 с.
6. Чижевский Я.А. Реализация концепции сетецентрических боевых действий в вооруженных силах США // Военная мысль. 2019. № 3, С. 116–137.
7. Попов А.А, Филатов В.И. Модели информационно-управляющей системы обеспечения взаимодействия разновидовых пунктов управления // Стратегическая стабильность. 2020. № 4, С. 19-23.
8. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.
9. Макаренко С.И. Интероперабельность человеко-машинных интерфейсов. Монография. – СПб.: Наукоемкие технологии, 2023. – 185 с.
10. Можаева И.А., Струков А.В., Поленин В.И., Сущенков Д.А. Моделирование байесовских сетей доверия с применением ОЛВМ // В сборнике: Актуальные проблемы защиты и безопасности. Сборник трудов Санкт-Петербургской Всероссийской научно-практической конференции РАРАН. Санкт-Петербург, 2019. С. 430–442.
11. Милославская Н.Г. Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. Дис. …доктора технических наук: 05.13.19. –М.: Федеральный исследовательский центр «Информатика и управление» Российской академии наук, 2020. – 461 с.
12. Будко Н.П., Васильев Н.В., Обзор графо-аналитических подходов к мониторингу информационно-телекоммуникационных сетей и их применение для выявления аномальных состояний // Системы управления, связи и безопасности. 2021. №6. С. 53-75.

FEATURES OF PROTECTION OF INFORMATION RESOURCES OF CONTROL SYSTEMS OF ROBOTIC COMPLEXES

Starodubtsev Yu.I.[1], Lauta O.S.[2], Khudainazarov Yu.K.[3]

Keywords: *information management system, protected information resources, threats to information security, integrated approach.*

Abstract

Objective: *in the article to propose a solution to the problem of analyzing the features of the protection of information resources (IR) of the control system of robotic complexes (RTS).*

Method: *on the basis of a system approach, to analyze the composition, functions, role and place of the information and control system in the control system of modern and future RTCs. The method of analytical modeling presents the main contradictions in the theory of control of military RTCs (HG).*

Result: *the results of the analysis of protected information resources in the information management system of the robotic complex are presented: information, data carriers and information processes. The main features of the applied protocols of information interaction in accordance with the OSI reference model are revealed.*

The results of the analysis of information security threats and the functional components of the integrated system for the protection of information resources of the control system of robotic complexes are presented.

The scientific novelty consists *in the formalization of objective contradictions in the properties of the control process of the RTS HV between continuity and secrecy, as well as between the properties of the RTS control system: limited resources (computational, network and memory) for the implementation of security functions; high dynamics of structural, informational and functional characteristics of the protected resources The consequence of these contradictions is the need to integrate heterogeneous methods and protection tools, as well as real-time management of*

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

[2]Oleg S. Lauta, Dr.Sc. (of tech.), Professor of the Department of the State University of Maritime and Inland Shipping named after Admiral S.O. Makarov, St. Petersburg, Russia.Email: laos-82@yandex.ru

[3]Yuriy K. Khudainazarov, Ph.D., Doctoral Student of the Department of Security of Special Purpose Information and Communication Systems 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

tasks and information resources of the information management system (ICS) of the HV RTS.

Currently known methods and technologies do not allow to take into account all the features of the R&D system of the RTS control system as an object of protection and to ensure the adequacy of the protection system to threats and the state of protected resources with their high dynamics.

References

1. Jumasheva E.S., Nyrkov A.P. Primenenie algoritmov mashinnogo obuchenija dlja obnaruzhenija anomal'nogo povedenija v setjah kriticheskoj informacionnoj infrastruktury // V sbornike: Regional'naja informatika i informacionnaja bezopasnost'. Sbornik trudov Sankt-Peterburgskoj mezhdunarodnoj konferencii. Sankt-Peterburg, 2023. S. 247–251.
2. Nyrkov A.P., Sokolov S.S., Alimov O.M., Chernyj S.G., Dorovskoj V.A. Optimal'naja identifikacija ob#ektov v zadachah raspoznavanija neobitaemymi podvodnymi apparatami // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2020. № 2. S. 58–64.
3. Martynov V.L., Nyrkov A.P., Shimanskaja M.S., Krechetova Je.V., Shimanskaja G.S. Gidroakusticheskie kommunikacii v voprosah protivodejstvija podvodnym robotam // Informatizacija i svjaz'. 2024. № 2. S. 51–55.
4. 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
5. Rahmanov A.A. Setecentricheskie sistemy upravlenija zakonomernye tendencii, problemnye voprosy i puti ih reshenija // Voennaja mysl' .2011. № 3, S. 41–50.
6. Bogovik A.V., Ignatov V.V. Teorija upravlenija v sistemah voennogo upravlenija: Uchebn. – SPb.: VAS, 2008. – 460 s.
7. Makarenko S.I. Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki. Monografija. – SPb.: Naukoemkie tehnologii, 2020. – 337 s.
8. Lepeshkin O.M. Sintez modeli processa upravlenija social'nymi i jekonomicheskimi sistemami na osnove teorii radikalov: avtoreferat dis. …doktora tehnicheskih nauk : 05.13.10 / Lepeshkin Oleg Mhajlovich. – Sankt-Peterburg, 2014. – 33 s.
9. Polenin V.I., I.A. Rjabinin, S.K. Svirin, I.A. Gladkova Primenenie obshhego logiko-verojatnostnogo metoda dlja analiza tehnicheskih, voennyh organizacionno-funkcional'nyh sistem i vooruzhennogo protivoborstva // Pod red. A.S. Mozhaeva / Rossijskaja akademija estestvennyh nauk. – SPb: SPb-regional'noe otdelenie RAEN, 2011. – 416 s., ill.
10. Zatuliveter Ju. S., Fishhenko E. A. Problemy programmiruemosti, bezopasnosti i nadezhnosti raspredelennyh vychislenij i setecentricheskogo upravlenija. Ch. 1. Analiz problematiki // Problemy upravlenija. 2016. vypusk 3, s. 49–57.
11. V.V. Golenkov, N.A. Guljakina Gra92–101micheskie associativnye modeli i sredstva parallel'noj obrabotki informacii v sistemah iskusstvennogo intellekta // Doklady BGUIR №1. 2004 g. s. 92-101.