Научная статья
УДК 004.056
https://doi.org/10.31854/1813-324X-2026-12-3-139-150
EDN:CMCIHU

Метод адаптивного выбора режима информационного обмена в системе связи для оптимизации управления группировкой робототехнических комплексов при кибервоздействиях

Алексей Владимирович Рабин[1] ✉, rabin.av@sut.ru
Валерий Алексеевич Липатников[2], lipatnikovanl@mail.ru
Илья Андреевич Андреев[2], andreev.ilia.1984@mail.ru

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Военная академия связи им. Маршала Советского Союза С.М. Буденного, Санкт-Петербург, 194064, Российская Федерация

Аннотация

Актуальность. *Актуальность исследования обусловлена развитием концепции Internet of Robotic Things, в рамках которой робототехнические устройства рассматриваются как сетевые интеллектуальные объекты, взаимодействующие с облачными, периферийными, сенсорными и управляющими компонентами.* ***Цель работы.*** *Целью работы является разработка метода адаптивного выбора режима информационного обмена в системе связи группировки робототехнических комплексов, обеспечивающего повышение устойчивости управления при кибервоздействиях и деградации каналов связи.* ***Решение.*** *В статье предложен метод адаптивного выбора режима информационного обмена в системе связи для оптимизации управления группировкой робототехнических комплексов при кибервоздействиях и деградации каналов связи.* ***Научная новизна.*** *Научная новизна работы заключается в разработке метода адаптивного выбора режима информационного обмена, основанного на совместной оценке критериев доступности, целостности, своевременности доставки сообщений и операционной связности.* ***Вычислительный эксперимент****, выполненный для группировки из 20 робототехнических комплексов, показал, что при комбинированном кибервоздействии предложенный метод обеспечивает доступность доставки сообщений 0,804, целостность сообщений 0,988, снижает количество принятых ложных сообщений до 1932 и уменьшает среднее число переключений режима до 6,3 за один прогон.* ***Практическая значимость.*** *Практическая значимость результатов заключается в возможности применения разработанного метода при проектировании и совершенствовании систем связи управления группировками робототехнических комплексов, функционирующих в условиях кибервоздействий и деградации каналов связи.*

Ключевые слова: *робототехнический комплекс, группировка робототехнических комплексов, система связи управления, информационный обмен, кибервоздействие, доступность, целостность данных, задержка передачи, адаптивный выбор режима, multi-robot systems, Internet of Robotic Things*

Ссылка для цитирования: Рабин А.В., Липатников В.А., Андреев И.А. Метод адаптивного выбора режима информационного обмена в системе связи для оптимизации управления группировкой робототехнических комплексов при кибервоздействиях// Труды учебных заведений связи. 2026. Т. 12. № 3. С. 139–150. DOI:10.31854/1813-324X-2026-12-3-139-150. EDN:CMCIHU

Original research
https://doi.org/10.31854/1813-324X-2026-12-3-139-150
EDN:CMCIHU

Adaptive Selection Method for the Information Exchange Mode in a Communication System for Optimizing Control of a Robotic Complex Group under Cyber Impacts

Aleksey V. Rabin[1] ✉, rabin.av@sut.ru
Valery A. Lipatnikov [2], lipatnikovanl@mail.ru
Ilya A. Andreev[2], andreev.ilia.1984@mail.ru

[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Telecommunications Military Academy,
St. Petersburg, 194064, Russian Federation

Annotation

Relevance. *The relevance of this study is further enhanced by the evolution of the Internet of Robotic Things (IoRT) concept, in which robotic devices operate as intelligent networked entities interacting with cloud, edge, sensing, and control components.* ***Purpose.*** *The purpose of this study is to develop an adaptive information exchange mode selection method for communication systems of robotic system groups to improve control resilience under cyberattacks and communication channel degradation.* ***Methods.*** *The paper proposes an adaptive information exchange mode selection method for optimizing the control of robotic system groups under cyberattacks and communication channel degradation.* ***Scientific novelty.*** *The scientific novelty of the proposed approach lies in the development of an adaptive information exchange mode selection method based on the joint assessment of communication availability, message integrity, delivery timeliness, and operational connectivity.* ***A computational experiment*** *involving a group of 20 robotic systems demonstrated that, under combined cyberattacks, the proposed method achieved a message delivery availability of 0.804 and a message integrity of 0.988, reduced the number of accepted false messages to 1,932, and decreased the average number of operating mode switches to 6.3 per simulation run.*
Practical significance. *The practical significance of the proposed method lies in its applicability to the design and enhancement of communication systems for robotic system groups operating under cyberattacks and communication channel degradation.*

Keywords: *robotic complex; robotic complex group; communication control system; information exchange; cyber impact; availability; data integrity; delivery delay; adaptive mode selection; multi-robot systems; Internet of Robotic Things*

For citation: Rabin A.V., Lipatnikov V.A., Andreev I.A. Adaptive Selection Method for the Information Exchange Mode in a Communication System for Optimizing Control of a Robotic Complex Group under Cyber Impacts. Proceedings of Telecommunication Universities. 2026;12(3):139–150. (in Russ.) DOI:10.31854/1813-324X-2026-12-3-139-150. EDN:CMCIHU

Введение

Развитие робототехнических комплексов (РТК) и их объединение в группировки приводит к усложнению систем связи управления, обеспечивающих передачу управляющих команд, телеметрии и служебной информации между пунктом управления, ретрансляционными узлами и отдельными робототехническими средствами. В отличие от одиночных робототехнических платформ, группировка РТК функционирует как распределенная ки-

берфизическая система, в которой результат выполнения задачи зависит от состояния отдельных устройств и от качества информационного обмена между ними. Актуальность задачи усиливается развитием концепции IoRT (*аббр. от англ.* Internet of Robotic Things), где робототехнические устройства рассматриваются как сетевые интеллектуальные объекты, взаимодействующие с облачными, периферийными, сенсорными и управляющими компонентами [1–4]. Такая интеграция расширяет функциональные возможности группировок, но одновременно увеличивает число потенциальных уязвимостей и поверхность кибервоздействий.

Исследования коммуникаций в многороботных системах показывают, что эффективность группового поведения зависит от топологии сети, пропускной способности каналов, задержек, потерь сообщений и своевременности доставки данных [5]. Поэтому система связи управления не может рассматриваться только как среда передачи данных: она непосредственно влияет на согласование действий, устойчивость функционирования и безопасность группировки.

Для робототехнических и киберфизических систем характерны угрозы несанкционированного доступа (НСД), подмены данных, модификации сообщений, сетевых атак, отказа в обслуживании, воздействия на сенсорные данные и нарушения управляющих контуров [6–9]. В контексте группировки РТК такие воздействия имеют не только информационные, но и функциональные последствия, поскольку задержка или искажение управляющей команды может привести к рассогласованию действий и снижению вероятности успешного выполнения групповой задачи.

В качестве базовых свойств информационной безопасности (ИБ) обычно рассматриваются конфиденциальность, целостность и доступность информации [10]. Для системы связи управления группировкой РТК эти свойства приобретают прикладную интерпретацию: доступность связана с доставкой команд и телеметрии, целостность – с отсутствием подмены или модификации сообщений, а конфиденциальность – с предотвращением НСД к управляющей и служебной информации. Дополнительно существенную роль играет своевременность доставки, поскольку корректное сообщение может утратить прикладную ценность при чрезмерной задержке.

Несмотря на значительное число работ по кибербезопасности (КБ) робототехнических систем, устойчивому управлению, обнаружению атак и коммуникациям в многороботных системах (группировках РТК), недостаточно проработанной остается задача выбора режима информационного обмена при изменяющемся профиле нарушения. В существующих работах акцент обычно делается либо на обнаружении конкретного класса атак, либо на устойчивом управлении при заданной модели отказов, либо на оптимизации коммуникаций без явной связи с профилем нарушения КБ [11–20].

В рассматриваемой постановке выбор режима информационного обмена является элементом замкнутого цикла управления системой связи группировки РТК при кибервоздействиях. Такой цикл включает сбор сведений о состоянии каналов и сообщениях, расчет критериев доступности, целостности, своевременности и операционной связности, определение профиля нарушения, выбор требуемого режима обмена, проверку устойчивости принятого решения и последующее применение выбранного режима на следующем интервале наблюдения. В отличие от статической организации обмена, данный цикл позволяет связывать наблюдаемое ухудшение состояния связи с конкретным управляющим воздействием: усилением контроля целостности, резервированием передачи, децентрализацией взаимодействия или ограничением объема трафика. Поэтому задача выбора режима информационного обмена рассматривается не как вспомогательная настройка сети, а как самостоятельный процесс управления устойчивостью системы связи группировки РТК.

Целью работы является разработка метода, который по значениям критериев состояния связи выбирает режим информационного обмена и ограничивает число необоснованных переключений. Для достижения цели решаются задачи формализации модели системы связи, определения критериев оценки обмена, разработки правила адаптивного выбора режима по профилю нарушения и экспериментального сравнения предлагаемого метода с базовыми схемами.

2. Анализ существующих работ и постановка задачи

Исследования по тематике статьи можно разделить на несколько групп: коммуникации в группировке РТК, технологии IoRT, ИБ робототехнических и киберфизических систем, устойчивое распределенное управление, а также методы обнаружения вторжений. Их сопоставление приведено в таблице 1.

В многороботных системах обмен данными поддерживает координацию, передачу состояний и выполнение распределенных алгоритмов. В [5] подчеркивается, что для таких систем характерны динамическая топология, ограничения радиоресурса, интерференция и неполнота информации. Эти факторы делают актуальной не только маршрутизацию сообщений, но и адаптацию режима обмена к текущему состоянию сети.

ТАБЛИЦА 1. Сопоставление направлений исследований с задачей статьи

TABLE 1. Comparison of Research Areas with the Objective of the Article

Направление	Основное содержание работ	Ограничение для рассматриваемой задачи
Коммуникации в группировках РТК [5]	– топология – пропускная способность – задержки – обмен состояниями – распределенные алгоритмы	Недостаточно рассматривается выбор режима обмена по профилю кибервоздействия
IoRT [1–4]	– архитектуры – протоколы – облачные и периферийные вычисления – безопасность IoRT	Преимущественно анализируются технологии и общие проблемы безопасности
КБ роботов и CPS [6–9]	– уязвимости – деревья атак – оценка безопасности – защита роботизированных CPS	Акцент на оценке уязвимостей и атак, а не на оперативном переключении режима обмена
Устойчивое управление многоробот-ными системами [11, 18–20]	– resilient coordination – задержки – отказоустойчивость – успешность миссий	Информационный обмен часто является условием работы алгоритма, а не объектом управления
Атаки на многороботные и многоагентные системы [12–17]	– deception – DoS – false data injection – adversarial perception – communication jamming	Обычно рассматриваются отдельные классы воздействий или отдельные контуры управления.
IDS для IoT [21, 22]	– классификация нормального и аномального поведения – ML/DL-подходы	IDS-слой не определяет режим организации информационного обмена

Работы по IoRT [1–4] показывают, что робототехнические устройства все чаще функционируют как сетевые интеллектуальные объекты. При этом возрастают требования к безопасности обмена, защите данных и устойчивости к сетевым воздействиям. Однако большинство таких работ носит обзорный или архитектурный характер и не решает задачу выбора режима информационного обмена в динамике.

В работах по КБ роботов и CPS [6–9] систематизируются уязвимости данных, программного обеспечения, сетевого взаимодействия и аппаратных компонентов. Отдельные исследования предлагают автоматизированную оценку безопасности, деревья атак и моделирование атак. Эти подходы важны для анализа угроз, но не определяют, какой режим обмена следует использовать при конкретном сочетании потерь, задержек и нарушений целостности.

Наиболее близкими являются исследования устойчивого управления и состязательных сред [11–20]. Например, deception-атаки связываются с нарушением целостности, а DoS-атаки – с нарушением доступности [12]. Отдельно рассматриваются атаки на коммуникационные связи [13], прерывистая связь [14], semantic attacks [15], adversarial perception [16], отказоустойчивая локализация [17], задержки связи [19] и обмен критической информацией [20]. Эти работы обосновывают набор нарушений, учитываемых в настоящей статье: снижение доступности, нарушение целостности, рост задержек и ухудшение операционной связности.

Отдельное значение для рассматриваемой задачи имеют методы обнаружения вторжений и аномалий в сетях Интернета вещей. В работах [21, 22] анализируются современные подходы к построению систем обнаружения вторжений на основе методов машинного и глубокого обучения, предназначенные для выявления нормального и аномального поведения сетевых узлов. Такие методы могут использоваться как источник информации о признаках кибервоздействия, однако сами по себе они, как правило, не определяют режим организации информационного обмена. В настоящей работе результаты обнаружения или оценки аномальности рассматриваются не как конечное управляющее решение, а как возможная входная информация для формирования профиля нарушения и последующего выбора режима обмена.

В отечественных работах также рассматриваются смежные задачи динамического обнаружения киберугроз, обработки результатов сетевого контроля и поддержки принятия решений при управлении сетями связи. В [23] предложен метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей, ориентированный на анализ поведения узлов и выявление аномалий. В [24] рассматривается обработка результатов сетевого контроля при поддержке принятия решений администратора безопасности информации. В [25] исследуется метод поддержки принятия решения при управлении сетью связи на основе нейросетевых технологий. Указанные работы подтверждают актуальность интеллектуальной обработки сетевых состояний и поддержки принятия решений, однако в них не решается задача выбора режима информационного обмена в системе связи управления группировкой РТК по совокупности критериев доступности, целостности, своевременности и операционной связности.

Дополнительно вопросы навигации, кооперативного обследования, защиты робототехнических и беспилотных групп, а также сетевого обнаружения вторжений рассматриваются в современных обзорах и исследованиях [26–32]. Эти источники подтверждают актуальность учета ограничений

связи, киберугроз и устойчивости обмена при проектировании групповых робототехнических систем.

Таким образом, существующие исследования раскрывают отдельные аспекты проблемы, но недостаточно рассматривают выбор режима информационного обмена в системе связи управления группировкой РТК при изменяющемся профиле нарушения. Под профилем нарушения далее понимается совокупность признаков, характеризующих доступность доставки сообщений, целостность принимаемых данных, своевременность доставки и операционную связность группировки.

Постановка задачи заключается в разработке и экспериментальной оценке метода, который на каждом интервале наблюдения оценивает состояние информационного обмена и выбирает один из режимов: штатный, защищенный, резервированный, децентрализованный или ограниченный. Выбор должен учитывать профиль нарушения и ограничивать число необоснованных переключений режима.

3. Модель и метод адаптивного выбора режима информационного обмена

3.1. Модель системы связи управления

Систему связи управления группировкой РТК представим динамическим графом:

$$G(t) = \langle V, E(t) \rangle,$$

где V – множество узлов; $E(t)$ – множество каналов связи, доступных на момент времени t.

Множество узлов включает пункт управления v_c, множество ретрансляционных узлов V_r и множество робототехнических комплексов V_b:

$$V = \{v_c\} \cup V_r \cup V_b.$$

$$e_{ij}(t) p_{ij}^{loss}(t) d_{ij}(t) s_{ij}(t).$$

Каждый канал характеризуется вероятностью потери сообщения, задержкой передачи и состоянием доступности. В рассматриваемых сценариях DoS-подобное воздействие приводит к росту потерь и отказам каналов, задерживающее воздействие увеличивает время доставки, а нарушение целостности связано с появлением ложных или модифицированных сообщений.

Для маршрута $P_c, k(t)$ от пункта управления или ретрансляционного узла к k-му РТК вероятность доставки и задержка определяются выражениями:

$$P_{deliv}, k(t) = \prod_{e_{ij} \in P_c, k(t)} \left(1 - p_{ij}^{loss(t)}\right),$$

$$D_{k(t)} = \sum_{e_{ij} \in P_c, k(t)} d_{ij(t)}.$$

Эти величины используются при расчете критериев доступности и своевременности передачи управляющих сообщений.

3.2. Критерии оценки состояния обмена

Состояние информационного обмена описывается вектором критериев:

$$K(t) = \langle K_A(t), K_I(t), K_T(t), K_G(t) \rangle.$$

Критерий доступности определяется как доля доставленных управляющих сообщений:

$$K_A(t) = \frac{N_{deliv}(t)}{N_{sent}(t)}.$$

Критерий целостности учитывает ложные или модифицированные сообщения, ошибочно принятые системой:

$$K_I(t) = 1 - \frac{N_{false}(t)}{N_{recv}(t)}.$$

Критерий своевременности рассчитывается по средней задержке доставки управляющих сообщений:

$$K_{T(t)} = 1, \text{если } \bar{D}(t) \le D_{ok};\ 1 - \frac{\bar{D}(t) - D_{ok}}{D_{crit} - D_{ok}},$$

если $D_{ok} < \bar{D}(t) < D_{crit}$; 0, если $\bar{D}(t) \ge D_{crit}$.

Критерий операционной связности определяется как доля РТК, для которых существует пригодный маршрут связи:

$$K_G(t) = \frac{N_{conn}(t)}{N}.$$

Маршрут считается пригодным, если вероятность доставки по нему не ниже заданного порога, а задержка не превышает допустимого значения. Такая трактовка отличает операционную связность от простой топологической связности графа.

3.3. Режимы информационного обмена

Вводится множество режимов информационного обмена (их назначение приведено в таблице 2):

$$Q = \{q_0, q_1, q_2, q_3, q_4\}.$$

ТАБЛИЦА 2. Режимы информационного обмена

TABLE 2. Information Exchange Modes

Режим	Название	Назначение	Ограничение
q_0	штатный	минимальная задержка и служебная нагрузка в нормальных условиях	низкая устойчивость к кибервоздействиям
q_1	защищенный	усиленная проверка целостности и подлинности сообщений	рост задержки и служебного трафика
q_2	резервированный	дублирование сообщений или использование резервных маршрутов	рост сетевой нагрузки

q_3	децентрализованный	снижение зависимости от пункта управления	усложнение координации
q_4	ограниченный	передача преимущественно критически важных сообщений	уменьшение полноты обмена

3.4. Правило выбора режима

На каждом интервале наблюдения формируется профиль нарушения $R(t)$, включающий признаки снижения доступности, целостности, своевременности и операционной связности.

Требуемый режим $q^*(t)$ определяется правилом приоритетов:

$$q*(t) = q_1, \text{если } K_{I(t)} < K_I^{\min},$$
$$q_3, \text{если } K_{G(t)} < K_G^{\min},$$
$$q_4, \text{если } K_{A(t)} < K_A^{crit} \text{ и } K_{T(t)} < K_T^{crit},$$
$$q_2, \text{если } K_{A(t)} < K_A^{\min},$$
$$q_4, \text{если } K_{T(t)} < K_T^{\min},$$
$$q_0 \text{ иначе.}$$

Приоритет нарушения целостности обусловлен тем, что принятие ложной или модифицированной управляющей команды может привести к некорректным действиям РТК. Снижение операционной связности требует частичной децентрализации, снижение доступности – резервирования, а рост задержек и перегрузка – ограничения объема передаваемого трафика.

Для уменьшения числа необоснованных переключений используется гистерезис. Переключение выполняется только в том случае, если требуемый режим сохраняется не менее H последовательных интервалов наблюдения:

$$q(t) = q^*(t),$$
$$\text{если } q*(t) = q^*(t-1) = \cdots = q^*(t-H+1),$$
$$\text{иначе } q(t) = q(t-1).$$

$$H = 5$$

В вычислительном эксперименте параметр гистерезиса H принят равным 5 шагам. Обобщенный алгоритм метода приведен в таблице 3.

Структура имитационной модели представлена на рисунке 1, обобщенный алгоритм адаптивного выбора режима информационного обмена – на рисунке 2.

ТАБЛИЦА 3. Основные этапы метода адаптивного выбора режима

TABLE 3. Main Stages of the Adaptive Mode Selection Method

Этап	Действие
1	Сбор данных о доставке сообщений, задержках, ложных сообщениях и состоянии каналов
2	Расчет критериев K_A, K_I, K_T, K_G
3	Формирование профиля нарушения $R(t)$
4	Определение требуемого режима $q^*(t)$ по правилу приоритетов
5	Проверка условия гистерезиса
6	Выбор $q(t)$ и применение режима на следующем интервале наблюдения

Представленный алгоритм вводит в цикл управления системой связи несколько дополнительных процессов по сравнению со статической схемой обмена. К ним относятся расчет векторной оценки состояния информационного обмена, формирование профиля нарушения, приоритетный выбор режима по характеру нарушения и проверка гистерезиса перед переключением. За счет этого смена режима выполняется не при единичном отклонении одного показателя, а при устойчивом подтверждении соответствующего состояния системы связи. Такой подход снижает вероятность частых переключений режима при кратковременных флуктуациях задержек, потерь сообщений или оценок целостности.

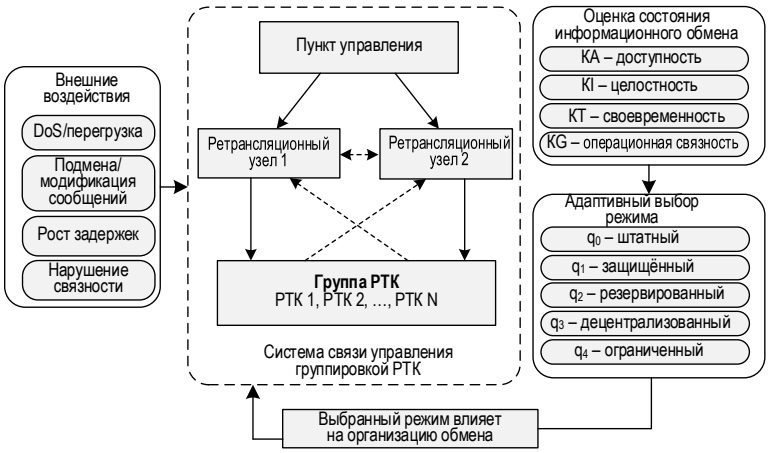


Рис. 1. Структура имитационной модели системы связи управления группировкой РТК

Fig. 1. Structure of the Simulation Model of the Communication System for Robotic Group Control

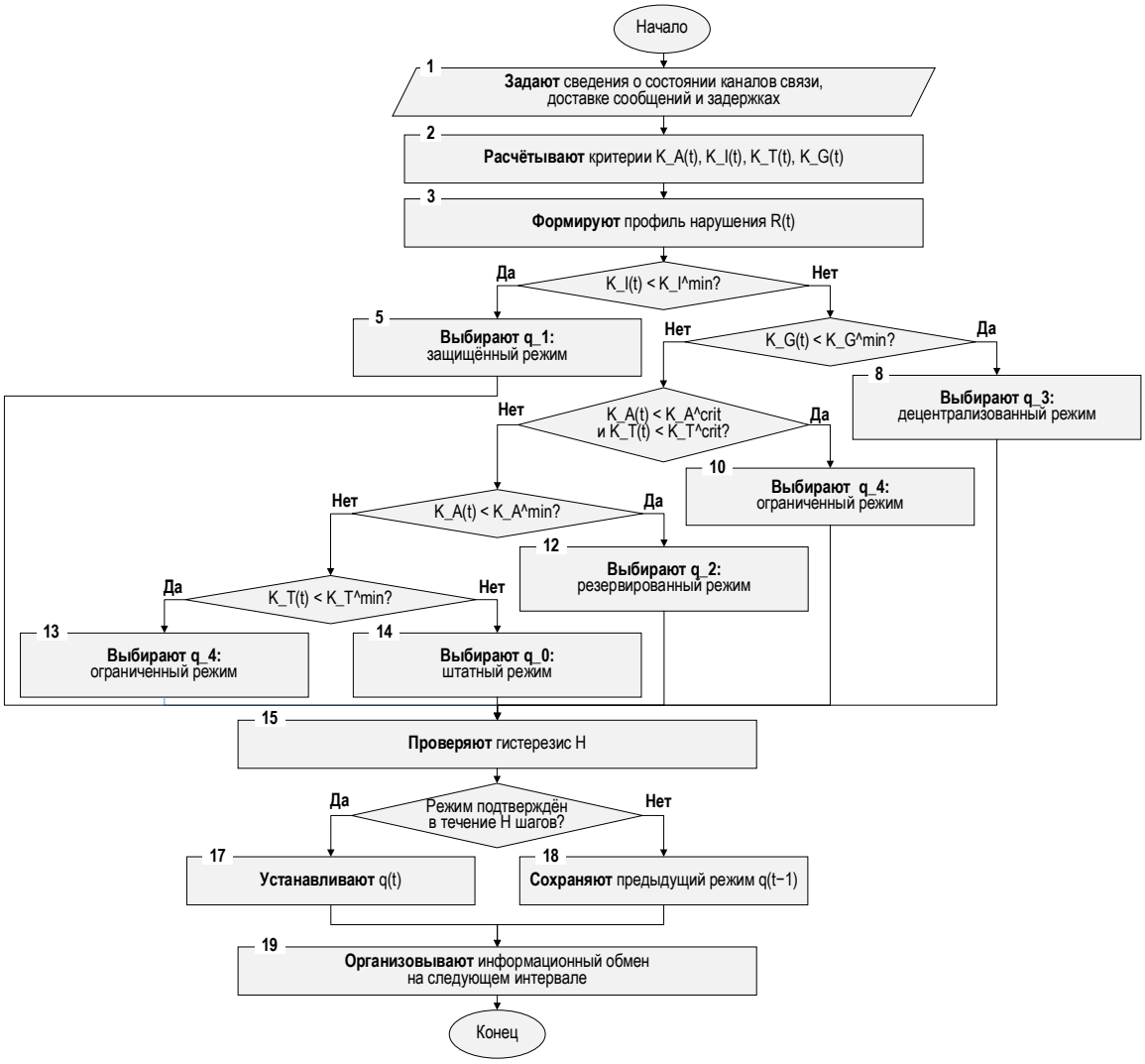


Рис. 2. Алгоритм адаптивного выбора режима информационного обмена

Fig. 2. Algorithm for Adaptive Selection of the Information Exchange Mode

4. Вычислительный эксперимент

4.1. Условия моделирования

Для проверки работоспособности метода проведен вычислительный эксперимент на имитационной модели системы связи управления. Моделирование не включает полную физическую динамику РТК, поскольку объектом исследования является организация информационного обмена. На каждом шаге пункт управления формировал управляющие сообщения для всех РТК; для каждого сообщения определялись возможность доставки, задержка и вероятность потери.

В эксперименте рассматривалась группировка из одного пункта управления, трех ретрансляционных узлов и двадцати РТК. Для каждого сценария и метода выполнялось 30 независимых прогонов по 300 шагов. Основные параметры приведены в таблице 4. Рассматривались пять сценариев: нормальное функционирование, DoS-подобная деградация каналов, подмена или модификация сообщений, рост задержек и комбинированное воздействие. Комбинированный сценарий включал последовательность интервалов: 0–50 – нормальное состояние; 50–120 – DoS-подобная деградация; 120–180 – подмена сообщений; 180–240 – рост задержек; 240–300 – комбинированное воздействие.

Предлагаемый метод сравнивался со статической схемой, резервированием по отказу, пороговым методом без гистерезиса и пороговым методом с гистерезисом. Для оценки использовались доступность K_A, своевременность K_T, целостность K_I, операционная связность K_G, средняя задержка $\bar{D}$, суммарное число принятых ложных сообщений N_{false}, среднее число переключений режима N_{sw} и средний служебный трафик O_{tr}.

ТАБЛИЦА 4. Основные параметры вычислительного эксперимента

TABLE 4. Main Parameters of the Computational Experiment

Параметр	Значение
Число РТК	20
Число ретрансляционных узлов	3
Длительность одного прогона	300 шагов
Число независимых прогонов	30
Допустимая задержка D_{ok}	80 мс
Критическая задержка D_{crit}	350 мс
Параметр гистерезиса H	5 шагов
Минимальная вероятность пригодного маршрута	0,35

4.2. Результаты и обсуждение

Основные результаты для комбинированного сценария приведены в таблице 5. Этот сценарий используется как основной, поскольку отражает изменение профиля нарушения во времени.

Статическая схема имеет минимальную служебную нагрузку, но демонстрирует наихудшие значения доступности и числа принятых ложных сообщений. Это связано с отсутствием реакции на изменение состояния каналов и появление модифицированных сообщений. Резервирование по отказу повышает доставку команд, но практически не решает задачу снижения ложных сообщений и сопровождается большим числом переключений.

Пороговый метод обеспечивает рост доступности и целостности, однако из-за отсутствия гистерезиса выполняет в среднем 151,3 переключения режима за прогон. Пороговый метод с гистерезисом снижает число переключений и имеет наибольшее значение $K_A = 0{,}818$, но сопровождается максимальным служебным трафиком и уступает предлагаемому методу по целостности, задержке и числу принятых ложных сообщений.

$$K_A = 0{,}804 K_I = 0{,}988, N_{false} = 1932 N_{sw} = 6{,}3.$$

Предлагаемый метод обеспечил $K_A = 0{,}804$, что близко к результатам пороговых схем, но при этом показал наилучшее значение $K_I = 0{,}988$, минимальное число принятых ложных сообщений $N_{false} = 1932$ и минимальное число переключений среди адаптивных схем $N_{sw} = 6{,}3$. Средняя задержка составила 158,30 мс, что ниже, чем у пороговых методов.

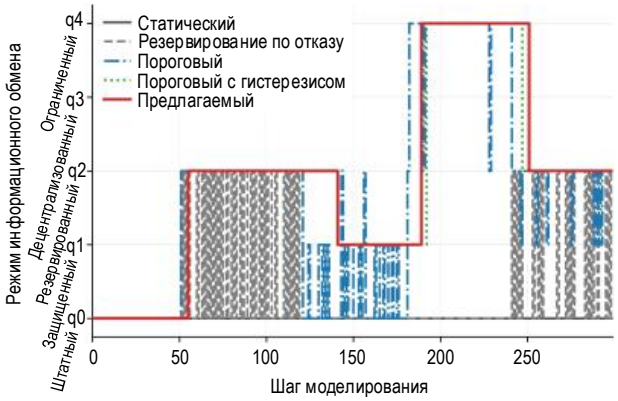


Рис. 3. Динамика выбора режима информационного обмена $q(t)$ при комбинированном кибервоздействии

Fig. 3. Dynamics of Information Exchange Mode Selection under Combined Cyber Impact

По сравнению со статической схемой предложенный метод повысил доступность доставки с 0,689 до 0,804 и снизил число принятых ложных сообщений с 5038 до 1932, т. Е. примерно на 61,7 %. По сравнению с пороговым методом без гистерезиса он уменьшил число переключений со 151,3 до 6,3 за прогон и снизил число принятых ложных сообщений с 2590 до 1932. По сравнению с пороговой схемой с гистерезисом предлагаемый метод несколько уступил по доступности, но показал лучшие значения по целостности, задержке, числу ложных сообщений, числу переключений и служебному трафику.

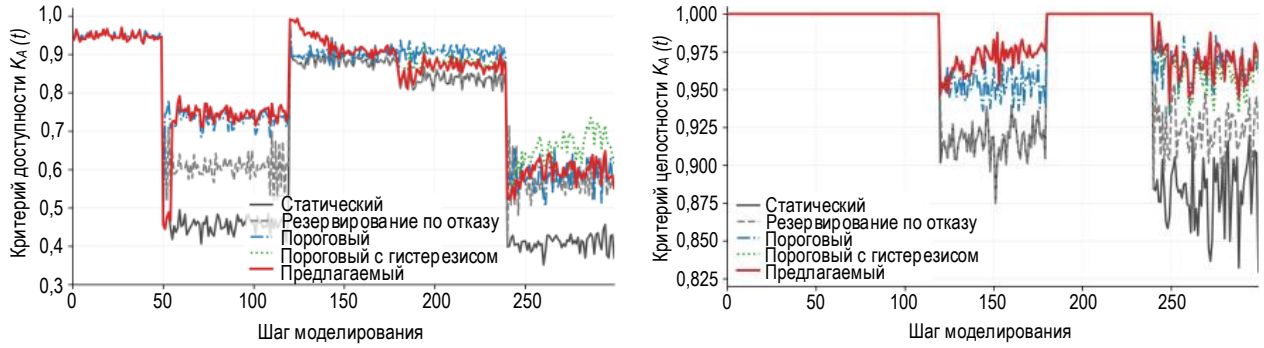
Изменение критериев доступности и целостности при комбинированном воздействии приведено на рисунке 4, а суммарное число принятых ложных сообщений и среднее число переключений режима – на рисунке 5.

ТАБЛИЦА 5. Сравнительные результаты методов при комбинированном кибервоздействии

TABLE 5. Comparative Results of the Methods under Combined Cyber Impact

Метод	K_A	K_T	K_I	K_G	$D_{ср}$, мс	N_{false}	N_{sw}	O_{tr}
Статический	0,689	0,704	0,960	0,978	154,78	5038	0,0	20,00
Резервный	0,757	0,689	0,968	0,989	158,88	4579	115,9	31,14
Пороговый	0,807	0,677	0,984	0,984	163,22	2590	151,3	41,61
Порог.+гист.	0,818	0,684	0,986	0,994	162,05	2182	8,3	43,25
Предлагаемый	0,804	0,698	0,988	0,992	158,30	1932	6,3	38,93

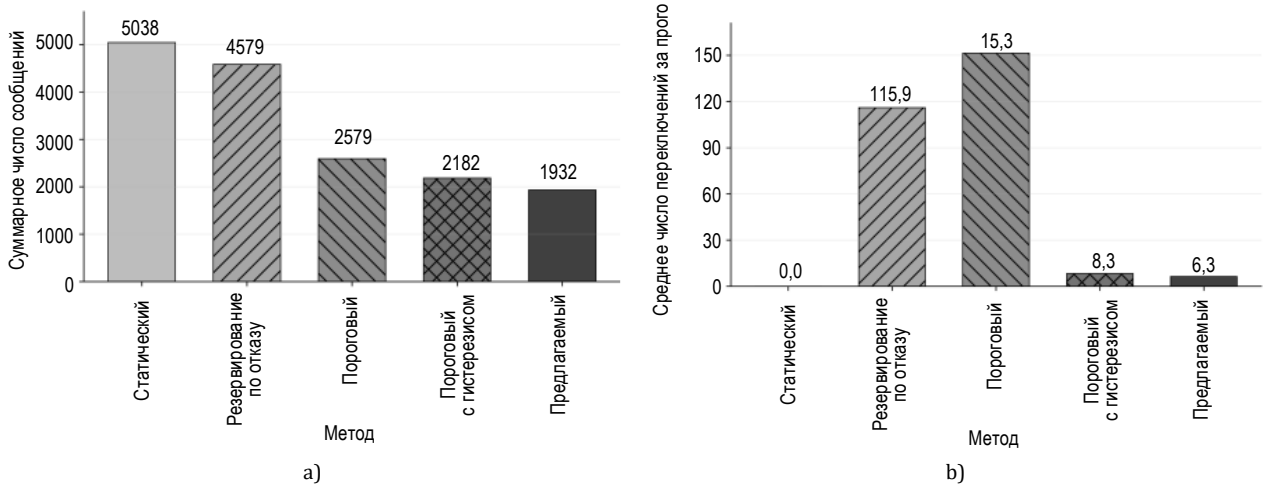
Примечание: Порог.+гист. – пороговый метод с гистерезисом



a) b)

Рис. 4. Изменение при комбинированном воздействии критериев: a) доступности $K_A(t)$; b) целостности $K_I(t)$

Fig. 4. Changes in Criteria under Combined Impact: (a) Availability; (b) Integrity



a) b)

Рис. 5. Суммарное число принятых ложных сообщений при комбинированном воздействии (a) и среднее число переключений режима информационного обмена за один прогон (b)

Fig. 5. Total Number of Accepted False Messages under Combined Impact (a) and Average Number of Information Exchange Mode Switches per Run (b)

Следовательно, предлагаемый метод не максимизирует один отдельный показатель, а обеспечивает более сбалансированное управление информационным обменом. Это важно для системы связи управления группировкой РТК, где чрезмерное резервирование, частые переключения режима и избыточный служебный трафик также могут снижать устойчивость функционирования.

Заключение

В работе рассмотрена задача адаптивного выбора режима информационного обмена в системе связи для оптимизации управления группировкой РТК при кибервоздействиях и деградации каналов связи. Предложена модель системы связи в виде динамического графа, включающего пункт управления, ретрансляционные узлы и РТК. Для оценки состояния обмена использованы критерии доступности, целостности, своевременности доставки и операционной связности.

Разработан метод адаптивного выбора режима информационного обмена по профилю нарушения. В зависимости от состояния критериев выбирается штатный, защищенный, резервированный, децентрализованный или ограниченный режим. Для уменьшения числа необоснованных переключений используется механизм гистерезиса.

Вычислительный эксперимент показал, что при комбинированном воздействии предлагаемый метод обеспечивает более сбалансированное управление обменом по сравнению с базовыми схемами. Он повысил доступность доставки управляющих сообщений по сравнению со статической схемой, снизил число принятых ложных сообщений и существенно уменьшил число переключений по сравнению с пороговым методом без гистерезиса. При этом преимущество метода заключается не в максимизации одного отдельного показателя, а в достижении компромисса между доступностью, целостностью, своевременностью, операционной связностью и стабильностью переключения режимов.

Ограничением исследования является использование имитационной модели, в которой не учитывались полная физическая динамика РТК, особенности конкретных радиопротоколов, криптографические задержки реальных средств защиты и влияние выбранного режима обмена на выполнение прикладной миссии. Дальнейшее развитие работы целесообразно связать с учетом мобильности узлов, неоднородности РТК, энергоограничений, реальных протоколов межроботного обмена и интеграции метода с модулями обнаружения аномалий и вторжений.

Список источников

1. Kabir H., Tham M.-L., Chang Y. C. Internet of Robotic Things for Mobile Robots: Concepts, Technologies, Challenges, Applications, and Future Directions // Digital Communications and Networks. 2023. Vol. 9, No. 6. P. 1265–1290. DOI: 10.1016/j.dcan.2023.05.006.

2. Krejčí J., Babiuch M., Suder J., Krys V., Bobovský Z. Internet of Robotic Things: Current Technologies, Challenges, Applications, and Future Research Topics // Sensors. 2025. Vol. 25, No. 3. Article 765. DOI: 10.3390/s25030765.

3. Rahim M. A., Rokonuzzaman M., Alqumsan A. A., Arogbonlo A., Islam M. Z., Trinh H., Islam M. S. An Intelligent and Secure Internet of Robotic Things: A Review and Conceptual Framework // Internet of Things. 2025. Vol. 33. Article 101684. DOI: 10.1016/j.iot.2025.101684.

4. Zafir E. I., Akter A., Islam M. N., Hasib S. A., Islam T., Sarker S. K., Muyeen S. M. Enhancing Security of Internet of Robotic Things: A Review of Recent Trends, Practices, and Recommendations with Encryption and Blockchain Techniques // Internet of Things. 2024. Vol. 28. Article 101357. DOI: 10.1016/j.iot.2024.101357.

5. Gielis J., Shankar A., Prorok A. A Critical Review of Communications in Multi-Robot Systems // Current Robotics Reports. 2022. Vol. 3. P. 213–225. DOI: 10.1007/s43154-022-00090-9.

6. Botta A., Rotbei S., Zinno S., Ventre G. Cyber Security of Robots: A Comprehensive Survey // Intelligent Systems with Applications. 2023. Vol. 18. Article 200237. DOI: 10.1016/j.iswa.2023.200237.

7. Tanimu J. A., Abada W. Addressing Cybersecurity Challenges in Robotics: A Comprehensive Overview // Cyber Security and Applications. 2025. Vol. 3. Article 100074. DOI: 10.1016/j.csa.2024.100074.

8. Papoutsakis M., Hatzivasilis G., Michalodimitrakis E., Ioannidis S., Michael M., Savva A., Nikolaou P., Stokkou E., Bozdemir G. SESAME: Automated Security Assessment of Robots and Modern Multi-Robot Systems // Electronics. 2025. Vol. 14, No. 5. Article 923. DOI: 10.3390/electronics14050923.

9. Bhardwaj A., Bharany S., Rehman A. U., Tejani G. G., Hussen S. Securing Cyber-Physical Robotic Systems for Enhanced Data Security and Real-Time Threat Mitigation // EURASIP Journal on Information Security. 2025. Vol. 2025. Article 1. DOI: 10.1186/s13635-025-00186-7.

10. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.CSWP.29.

11. Zhou L., Tokekar P. Multi-Robot Coordination and Planning in Uncertain and Adversarial Environments // Current Robotics Reports. 2021. DOI: 10.1007/s43154-021-00046-5.

12. Lee S., Min B.-C. Distributed Control of Multi-Robot Systems in the Presence of Deception and Denial of Service Attacks. arXiv:2102.00098. 2021.

13. Taheri M., Khorasani K., Shames I., Meskin N. Undetectable Cyber Attacks on Communication Links in Multi-Agent Cyber-Physical Systems. arXiv:2009.06173. 2020.

14. Bahrami R., Jafarnejadsani H. Distributed Detection of Adversarial Attacks for Resilient Cooperation of Multi-Robot Systems with Intermittent Communication. arXiv:2410.04547. 2024.

15. Yeke D., et al. Automated Discovery of Semantic Attacks in Multi-Robot Navigation Systems // Proceedings of the USENIX Security Symposium. 2025.

16. Bahrami R., Jafarnejadsani H. Multi-Robot Coordination with Adversarial Perception. arXiv:2504.09047. 2025.

17. Tasooji T. K., Parasuraman R. Distributed Fault-Tolerant Multi-Robot Cooperative Localization in Adversarial Environments. arXiv:2507.06750. 2025.

18. Li P., Liu J., Wu Y., Zhou L. Failure-Aware Multi-Robot Coordination for Resilient and Adaptive Target Tracking. arXiv:2508.02529. 2025.

19. Ballotta L., Talak R. Safe Distributed Control of Multi-Robot Systems with Communication Delays // IEEE Transactions on Vehicular Technology. 2025. arXiv:2402.09382.

20. Jo D., Kwon Y. Generation of Critical Information and Sharing Mechanism for Multi-Robot Mission Success // IEEE Access. 2025. Vol. 13. P. 146855–146873. DOI: 10.1109/ACCESS.2025.3600319.

21. Kikissagbe B. R., Adda M. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review // Electronics. 2024. Vol. 13, No. 18. Article 3601. DOI: 10.3390/electronics13183601.

22. Hozouri A., Mirzaei A., Effatparvar M. A Comprehensive Survey on Intrusion Detection Systems with Advances in Machine Learning, Deep Learning and Emerging Cybersecurity Challenges // Discover Artificial Intelligence. 2025. Vol. 5. Article 314. DOI: 10.1007/s44163-025-00578-1.

23. Котенко И.В., Саенко И.Б., Липатников В.А., Андреев И.А. Метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей // Прикладная информатика. 2026. Т. 21. № 2. С. 102–118. DOI: 10.37791/2687-0649-2026-21-2-102-118.

24. Липатников В.А., Мелехов К.В. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации. В сборнике: Актуальные проблемы защиты и безопасности. Труды XXVII Всероссийской научно-практической конференции. Санкт-Петербург, 2024. С. 306-310.

25. Липатников В.А., Парфиров В.А. Метод поддержки принятия решения при управлении сетью связи на основе технологии нейронных сетей. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). Материалы XIII Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2024. С. 467-472.

26. Chen W., Chi W., Ji S., Ye H., Liu J., Jia Y., Yu J., Cheng J. A Survey of Autonomous Robots and Multi-Robot Navigation: Perception, Planning and Collaboration // Biomimetic Intelligence and Robotics. 2025. Vol. 5, No. 2. Article 100203. DOI: 10.1016/j.birob.2024.100203.

27. Vijay V., Pant K.A., Cho M., Guo Y., Goppert J.M., Hwang I. Range-Based Multi-Robot Integrity Monitoring For Cyberattacks and Faults: An Anchor-Free Approach // IEEE Robotics and Automation Letters. 2025. Vol. 10, No. 3.

28. Aouedi O., Vu T.-H., Sacco A., Nguyen D.C., Piamrat K., Marchetto G., Pham Q.-V. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions // IEEE Communications Surveys & Tutorials. 2025. Vol. 27, No. 2. P. 1238–1292. DOI: 10.1109/COMST.2024.3430368.

29. Wang C., Yu C., Xu X., Gao Y., Yang X., Tang W., Yu S., Chen Y., Gao F., Jian Z., Chen X., Gao F., Zhou B., Wang Y. Multi-Robot System for Cooperative Exploration in Unknown Environments: A Survey. arXiv:2503.07278. 2025.

30. Holdbrook R., Odeyomi O., Yi S., Roy K. Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey // Electronics. 2024. Vol. 13, No. 22. Article 4440. DOI: 10.3390/electronics13224440.

31. Wang X., Zhao Z., Yi L., Ning Z., Guo L., Yu F.R., Guo S. A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures // ACM Computing Surveys. 2024. Vol. 57, No. 3. Article 74. DOI: 10.1145/3703625.

32. Ceviz O., Sen S., Sadioglu P. A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions // IEEE Communications Surveys & Tutorials. 2025. Vol. 27, No. 5. P. 3227–3265. DOI: 10.1109/COMST.2024.3515051.

References

1. Kabir H., Tham M.-L., Chang Y. C. Internet of Robotic Things for Mobile Robots: Concepts, Technologies, Challenges, Applications, and Future Directions // Digital Communications and Networks. 2023. Vol. 9, No. 6. P. 1265–1290. DOI: 10.1016/j.dcan.2023.05.006.

2. Krejčí J., Babiuch M., Suder J., Krys V., Bobovský Z. Internet of Robotic Things: Current Technologies, Challenges, Applications, and Future Research Topics // Sensors. 2025. Vol. 25, No. 3. Article 765. DOI: 10.3390/s25030765.

3. Rahim M. A., Rokonuzzaman M., Alqumsan A. A., Arogbonlo A., Islam M. Z., Trinh H., Islam M. S. An Intelligent and Secure Internet of Robotic Things: A Review and Conceptual Framework // Internet of Things. 2025. Vol. 33. Article 101684. DOI: 10.1016/j.iot.2025.101684.

4. Zafir E. I., Akter A., Islam M. N., Hasib S. A., Islam T., Sarker S. K., Muyeen S. M. Enhancing Security of Internet of Robotic Things: A Review of Recent Trends, Practices, and Recommendations with Encryption and Blockchain Techniques // Internet of Things. 2024. Vol. 28. Article 101357. DOI: 10.1016/j.iot.2024.101357.

5. Gielis J., Shankar A., Prorok A. A Critical Review of Communications in Multi-Robot Systems // Current Robotics Reports. 2022. Vol. 3. P. 213–225. DOI: 10.1007/s43154-022-00090-9.

6. Botta A., Rotbei S., Zinno S., Ventre G. Cyber Security of Robots: A Comprehensive Survey // Intelligent Systems with Applications. 2023. Vol. 18. Article 200237. DOI: 10.1016/j.iswa.2023.200237.

7. Tanimu J. A., Abada W. Addressing Cybersecurity Challenges in Robotics: A Comprehensive Overview // Cyber Security and Applications. 2025. Vol. 3. Article 100074. DOI: 10.1016/j.csa.2024.100074.

8. Papoutsakis M., Hatzivasilis G., Michalodimitrakis E., Ioannidis S., Michael M., Savva A., Nikolaou P., Stokkou E., Bozdemir G. SESAME: Automated Security Assessment of Robots and Modern Multi-Robot Systems // Electronics. 2025. Vol. 14, No. 5. Article 923. DOI: 10.3390/electronics14050923.

9. Bhardwaj A., Bharany S., Rehman A. U., Tejani G. G., Hussen S. Securing Cyber-Physical Robotic Systems for Enhanced Data Security and Real-Time Threat Mitigation // EURASIP Journal on Information Security. 2025. Vol. 2025. Article 1. DOI: 10.1186/s13635-025-00186-7.

10. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.CSWP.29.

11. Zhou L., Tokekar P. Multi-Robot Coordination and Planning in Uncertain and Adversarial Environments // Current Robotics Reports. 2021. DOI: 10.1007/s43154-021-00046-5.

12. Lee S., Min B.-C. Distributed Control of Multi-Robot Systems in the Presence of Deception and Denial of Service Attacks. arXiv:2102.00098. 2021.

13. Taheri M., Khorasani K., Shames I., Meskin N. Undetectable Cyber Attacks on Communication Links in Multi-Agent Cyber-Physical Systems. arXiv:2009.06173. 2020.

14. Bahrami R., Jafarnejadsani H. Distributed Detection of Adversarial Attacks for Resilient Cooperation of Multi-Robot Systems with Intermittent Communication. arXiv:2410.04547. 2024.

15. Yeke D., et al. Automated Discovery of Semantic Attacks in Multi-Robot Navigation Systems // Proceedings of the USENIX Security Symposium. 2025.

16. Bahrami R., Jafarnejadsani H. Multi-Robot Coordination with Adversarial Perception. arXiv:2504.09047. 2025.

17. Tasooji T. K., Parasuraman R. Distributed Fault-Tolerant Multi-Robot Cooperative Localization in Adversarial Environments. arXiv:2507.06750. 2025.

18. Li P., Liu J., Wu Y., Zhou L. Failure-Aware Multi-Robot Coordination for Resilient and Adaptive Target Tracking. arXiv:2508.02529. 2025.

19. Ballotta L., Talak R. Safe Distributed Control of Multi-Robot Systems with Communication Delays // IEEE Transactions on Vehicular Technology. 2025. arXiv:2402.09382.

20. Jo D., Kwon Y. Generation of Critical Information and Sharing Mechanism for Multi-Robot Mission Success // IEEE Access. 2025. Vol. 13. P. 146855–146873. DOI: 10.1109/ACCESS.2025.3600319.
21. Kikissagbe B. R., Adda M. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review // Electronics. 2024. Vol. 13, No. 18. Article 3601. DOI: 10.3390/electronics13183601.
22. Hozouri A., Mirzaei A., Effatparvar M. A Comprehensive Survey on Intrusion Detection Systems with Advances in Machine Learning, Deep Learning and Emerging Cybersecurity Challenges // Discover Artificial Intelligence. 2025. Vol. 5. Article 314. DOI: 10.1007/s44163-025-00578-1.
23. Котенко И.В., Саенко И.Б., Липатников В.А., Андреев И.А. Метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей // Прикладная информатика. 2026. Т. 21. № 2. С. 102–118. DOI: 10.37791/2687-0649-2026-21-2-102-118.
24. Липатников В.А., Мелехов К.В. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации. В сборнике: Актуальные проблемы защиты и безопасности. Труды XXVII Всероссийской научно-практической конференции. Санкт-Петербург, 2024. С. 306-310.
25. Липатников В.А., Парфиров В.А. Метод поддержки принятия решения при управлении сетью связи на основе технологии нейронных сетей. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). Материалы XIII Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2024. С. 467-472.
26. Chen W., Chi W., Ji S., Ye H., Liu J., Jia Y., Yu J., Cheng J. A Survey of Autonomous Robots and Multi-Robot Navigation: Perception, Planning and Collaboration // Biomimetic Intelligence and Robotics. 2025. Vol. 5, No. 2. Article 100203. DOI: 10.1016/j.birob.2024.100203.
27. Vijay V., Pant K.A., Cho M., Guo Y., Goppert J.M., Hwang I. Range-Based Multi-Robot Integrity Monitoring For Cyberattacks and Faults: An Anchor-Free Approach // IEEE Robotics and Automation Letters. 2025. Vol. 10, No. 3.
28. Aouedi O., Vu T.-H., Sacco A., Nguyen D.C., Piamrat K., Marchetto G., Pham Q.-V. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions // IEEE Communications Surveys & Tutorials. 2025. Vol. 27, No. 2. P. 1238–1292. DOI: 10.1109/COMST.2024.3430368.
29. Wang C., Yu C., Xu X., Gao Y., Yang X., Tang W., Yu S., Chen Y., Gao F., Jian Z., Chen X., Gao F., Zhou B., Wang Y. Multi-Robot System for Cooperative Exploration in Unknown Environments: A Survey. arXiv:2503.07278. 2025.
30. Holdbrook R., Odeyomi O., Yi S., Roy K. Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey // Electronics. 2024. Vol. 13, No. 22. Article 4440. DOI: 10.3390/electronics13224440.
31. Wang X., Zhao Z., Yi L., Ning Z., Guo L., Yu F.R., Guo S. A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures // ACM Computing Surveys. 2024. Vol. 57, No. 3. Article 74. DOI: 10.1145/3703625.
32. Ceviz O., Sen S., Sadioglu P. A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions // IEEE Communications Surveys & Tutorials. 2025. Vol. 27, No. 5. P. 3227–3265. DOI: 10.1109/COMST.2024.3515051.

Статья поступила в редакцию 15.06.2026; одобрена после рецензирования 24.06.2026; принята к публикации 27.06.2026.
The article was submitted 15.06.2026; approved after reviewing 24.06.2026; accepted for publication 27.06.2026.

Информация об авторах:

РАБИН Алексей Владимирович — доктор технических наук, доцент, проректор по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0001-5641-0410

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0000-0002-3736-4743

АНДРЕЕВ Илья Андреевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С.М. Буденного
https://orcid.org/0009-0007-3617-3439

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.