DOI 10.54398/20741707_2022_2_92
УДК 004.896

# АНАЛИЗ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ ПРИ МАСШТАБИРОВАНИИ ЧИСЛЕННОСТИ АГЕНТОВ[1]

*Статья поступила в редакцию 26.03.2022, в окончательном варианте – 28.04.2022.*

***Петренко Вячеслав Иванович***, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
кандидат технических наук, заведующий кафедрой организации и технологии защиты информации, ORCID: 0000-0003-4293-7013, e-mail: vipetrenko@ncfu.ru
***Тебуева Фариза Биляловна***, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
доктор физико-математических наук, заведующий кафедрой компьютерной безопасности, ORCID: 0000-0002-7373-4692, e-mail: fbtebueva@ncfu.ru
***Павлов Андрей Сергеевич***, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
старший преподаватель, ORCID: 0000-0002-8413-8706, e-mail: anspavlov@ncfu.ru
***Стручков Игорь Владиславович***, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
аспирант, ORCID: 0000-0001-8744-498X, e-mail: selentar@bk.ru

Применение роевых робототехнических систем (РРТС) в сложных прикладных задачах позволяет существенно увеличить эффективность решения подобных задач. При этом функционирование РРТС в условиях агрессивной окружающей среды, в том числе в условиях противодействия со стороны противника, обусловливает необходимость обеспечения информационной безопасности (ИБ), что особенно важно для стратегических объектов. Основные исследования ИБ в РРТС направлены, как правило, на адаптацию методов обеспечения ИБ для различных видов систем. Однако РРТС как один из видов групповой робототехники имеют ряд отличий и дополнительных требований к обеспечению ИБ. Дополнительные требования обусловлены критическим характером потенциального ущерба при реализации различных сценариев атак. Одним из актуальных направлений ИБ РРТС является вопрос противодействия атакам, не имеющим явно выраженных признаков. В рамках решения данного вопроса основное внимание уделяется задаче выявления и идентификации вредоносных агентов в процессе функционирования системы путем анализа поведения агентов и определения показателя доверия. При этом мало изученным остается вопрос аутентификации и авторизации агентов РРТС, что свидетельствует об отсутствии комплексного решения, позволяющего не только своевременно выявить факт атаки и идентифицировать вредоносных агентов системы, но и снизить вероятность внедрения вредоносных агентов в функционирующую систему. В данной работе проведено обобщение известных результатов в области проектирования и разработки РРТС, представлены обобщенная модель функционирования РРТС, а также проведен анализ приложений РРТС, в результате которого выделен класс пространственно-распределенных задач. Данный класс задач характеризуется рассредоточенностью агентов таким образом, что возможности бортовых телекоммуникационных устройств не обеспечивают стабильного информационного обмена между агентами в процессе выполнения задач. Также данный класс задач подразумевает возможность повышения сложности задачи (например, увеличение рабочей области), что требует привлечения новых агентов для максимизации эффективности выполнения задач. Исходя из полученных результатов, был проведен анализ уязвимостей РРТС при выполнении пространственно-распределенных задач, сформулированы обобщенные модели угроз и нарушителя ИБ РРТС с учетом свойств, характерных для систем данного вида, при этом основной акцент сделан на свойство масштабируемости РРТС. Проведена количественная оценка влияния внедренных вредоносных агентов на результат функционирования РРТС. Обосновано направление дальнейших исследований, которые позволят организовать комплексную защиту информации в РРТС совместно с существующими решениями, тем самым повысив уровень ИБ РРТС при воздействии вредоносных агентов.

**Ключевые слова:** роевые робототехнические системы, информационная безопасность, внедрение вредоносных агентов, распределение задач

# ANALYSIS OF THE INFORMATION SECURITY OF SWARM ROBOTICS IN THE PROCESS OF SCALING THE NUMBER OF AGENTS

*The article was received by the editorial board on 24.03.2022, in the final version – 28.04.2022.*

***Petrenko Vyacheslav I.***, North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,
Cand. Sci. (Engineering), Head of Department of Organization and Technology of Information Security, ORCID: 0000-0003-4293-7013, e-mail: vipetrenko@ncfu.ru
***Tebueva Fariza B.***, North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,
Doct. Sci. (Physics and Mathematics), Head of the Department, of Computer Security, ORCID: 0000-0002-7373-4692, e-mail: fbtebueva@ncfu.ru

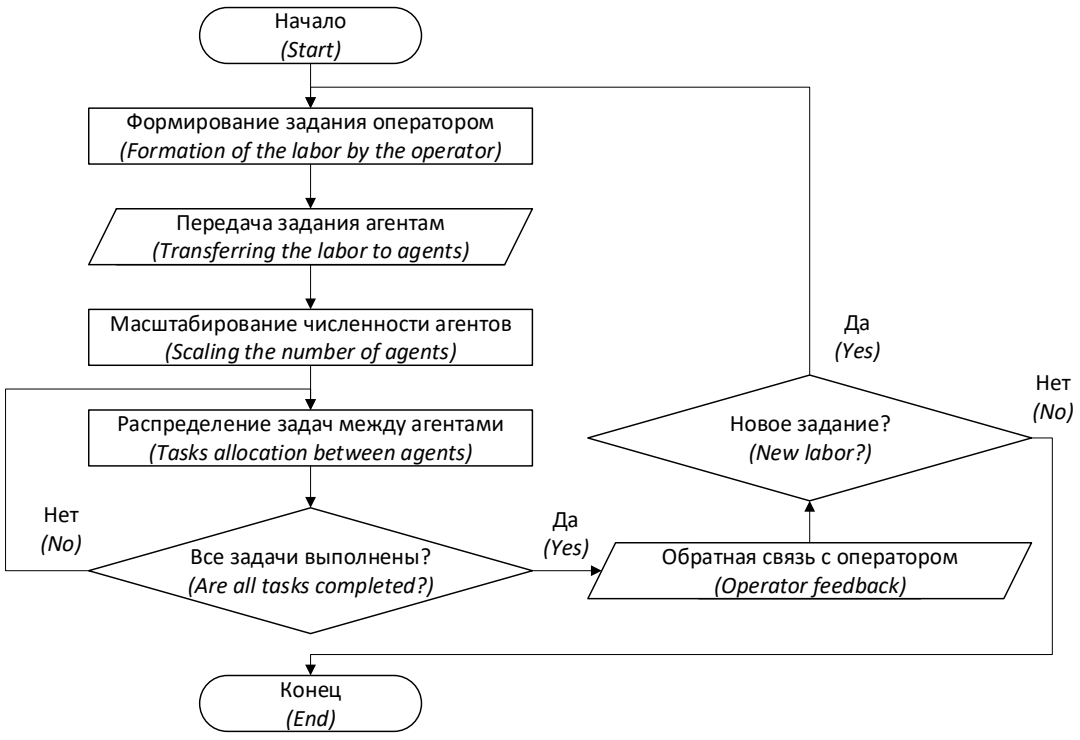
[1] Исследование выполнено при финансовой поддержке Минцифры России (грант ИБ, проект № 45/21-к).

***Pavlov Andrey S.***, North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation, Senior Lecturer, ORCID: 0000-0002-8413-8706, e-mail: anspavlov@ncfu.ru
***Struchkov Igor V.***, North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation, postgraduate student, ORCID: 0000-0001-8744-498X, e-mail: selentar@bk.ru

The use of swarm robotic systems (SRS) in complex applied problems can significantly increase the efficiency of solving such problems. At the same time, the functioning of the SRS in an aggressive environment, including in the face of opposition from the enemy, necessitates information security (IS), which is especially important for strategic facilities. The main IS research in the SRS is usually aimed at adapting the methods of providing IS for various types of systems. However, SRS, as one of the types of group robotics, have a number of differences and additional requirements for providing information security. Additional requirements are due to the critical nature of the potential damage in the implementation of various attack scenarios. One of the topical areas of IS SRS is the issue of countering attacks that do not have explicit signs. As part of solving this issue, the main attention is paid to the task of detecting and identifying malicious agents in the process of system operation by analyzing the behavior of agents and determining the trust indicator. At the same time, the issue of authentication and authorization of SRS agents remains little studied, which indicates the absence of a comprehensive solution that allows not only to timely detect the fact of an attack and identify malicious system agents, but also reduce the likelihood of malicious agents infiltrating a functioning system. In this paper, a generalization of known results in the field of design and development of SRS is carried out, a generalized model of SRS operation is presented, and an analysis of SRS applications is carried out, as a result of which a class of spatially distributed problems is identified. This class of tasks is characterized by dispersed agents in such a way that the capabilities of on-board telecommunication devices do not provide a stable information exchange between agents in the process of performing tasks. Also, this class of tasks implies the possibility of increasing the complexity of the task (for example, increasing the workspace), which requires the involvement of new agents to maximize the efficiency of task execution. Based on the results obtained, an analysis of SRS vulnerabilities was carried out when performing spatially distributed tasks, generalized models of threats and an intruder of SRS IS were formulated, taking into account the properties characteristic of systems of this type, with the main emphasis on the scalability property of SRS. A quantitative assessment of the impact of embedded malicious agents on the result of the functioning of the SRS was carried out. The direction of further research is substantiated, which will allow organizing complex information protection in SRS together with existing solutions, thereby increasing the level of SRS IS under the influence of malicious agents.

**Keywords:** swarm robotic systems, information security, introduction of malicious agents, tasks allocation

**Graphical annotation (Графическая аннотация)**




**Введение.** Переход к передовым цифровым, интеллектуальным производственным технологиям актуализирует направление развития роевой робототехники как вида групповой робототехники. Роевые робототехнические системы (РРТС) предназначены для решения широкого спектра задач: мониторинг и ликвидация чрезвычайных ситуаций, спасательные операции, подводные исследования, сельскохозяйственные работы, разведывательные операции, а также многие другие [1]. Наличие большого количества прикладных задач, решение которых характеризуется высокой трудоемкостью, неопределенностью и требованием работы в масштабе реального времени в условиях воздействия противоречивых, а также

часто меняющихся факторов обусловливает непрерывно растущий интерес к роевой робототехнике. При этом, ввиду увеличения сложности проектирования и разработки РРТС, специалистами в данной области уделяется особое внимание вопросам обеспечения информационной безопасности (ИБ) как всей системы, так и отдельных ее элементов.

Данная работа построена следующим образом. В первой части представлено описание РРТС как вида групповой робототехники, перечислены специфические характеристики и свойства, в результате чего формализована обобщенная модель функционирования РРТС. На основе анализа литературных источников сформулирована классификация сценариев использования систем данного вида, в рамках которой выделен класс пространственно-распределенных задач. Во второй части проведено исследование ИБ РРТС, в рамках которого рассмотрены уязвимости систем данного вида, а также угрозы и механизмы реализации данных угроз. Сформулированы обобщенные модели угроз и нарушителя ИБ РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач. Третья часть содержит анализ литературных источников, направленный на оценку актуального состояния проблемы обеспечения ИБ РРТС при внедрении вредоносных агентов и возможность использования рассмотренных решений в системах данного вида. В четвертой части представлены результаты количественной оценки влияния внедренных вредоносных агентов на функционирование РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач. Представленная структура работы имеет несколько нетрадиционный вариант изложения материала, однако, по мнению авторов, именно такой способ организации элементов статьи позволяет максимально полно и последовательно ознакомить читателя с тематикой исследования, так как результаты и выводы, полученные в каждой последующей части, базируются непосредственно на результатах и выводах предыдущих частей.

**1. Обобщенная модель функционирования РРТС и классификация сценариев использования систем данного вида.** Роевая робототехника является относительно молодой областью исследований и постоянно развивается, однако в публикациях можно встретить такие термины, как «мультиагентные системы», «мультироботизированные системы» и «роевые робототехнические системы», которые часто используются в качестве синонимов. В работе [1] представлена систематизация и разграничение данных терминов. Так, мультиагентные системы представляют собой формализм, позволяющий описать не только робототехнические системы, но и любые информационные системы, состоящие из множества взаимодействующих элементов или подсистем. По этой причине данный термин представляет собой наиболее широкое понятие, которое включает в себя все прочие виды групповой робототехники.

Под мультироботизированными системами (МРС) понимаются такие системы, которые включают множество робототехнических устройств, в том числе сенсорные сети. МРС могут быть построены с использованием роботов на базе различных архитектур (гомогенные или гетерогенные роботы с различным структурно-функциональным исполнением и назначением), а также могут использовать принципы централизованного, децентрализованного или смешанного типа управления [2]. Так, например, использование термина МРС будет корректным для описания группы беспилотных летательных аппаратов (БПЛА), группы промышленных манипуляторов на конвейерной линии, роботов-футболистов и т.д. Стоит отметить, что роботы, входящие в МРС, необязательно должны иметь одну общую цель и взаимодействовать друг с другом для ее достижения.

РРТС является частным случаем МРС, основным отличием является то, что перед системой ставится общая задача, которую роботы должны решить посредством взаимодействия друг с другом. При этом РРТС в классическом понимании должна обладать следующими свойствами:

- масштабируемость – система управления РРТС строится таким образом, чтобы обеспечить требуемое качество управления с неограниченным количеством роботов;
- децентрализованная система управления – ожидаемое поведение роботов достигается за счет использования принципов самоорганизации. Применение централизованного управления для РРТС накладывает ограничения на масштабируемость системы;
- простота технической реализации роботов – все роботы, входящие в состав РРТС, имеют ограниченные возможности вычислительных устройств, а также бортовых датчиков и сенсоров, что делает невозможным выполнить поставленную задачу с использованием только одного робота (в отличие от роботов с классическим исполнением. Под классическим исполнением робота понимается наличие максимально возможного бортового оснащения для выполнения широкого круга задач, например, антропоморфные роботы [3]);
- локальное взаимодействие роботов – выполнение поставленной перед РРТС задачи возможно только путем взаимодействия роботов друг с другом с использованием различных средств связи, при этом дальность их действия ограничена;
- гомогенность – роботы имеют идентичные структурные и функциональные характеристики (габаритные размеры, наличие нескольких вычислительных платформ, наличие бортовых специализированных исполнительных устройств, датчиков и сенсоров);
- автономность – ввиду отсутствия единого управляющего центра каждый робот самостоятельно принимает решение о своих дальнейших действиях, опираясь на доступную ему информацию.

Иллюстрация иерархии рассмотренной терминологии представлена на рисунке 1.

Преимуществами РРТС по сравнению с робототехническими системами с классическим исполнением являются [4, 5]:

- экономическая эффективность применения большого количества технически простых роботов с сопоставимыми показателями качества решения поставленной задачи;
- возможность достижения требуемых показателей качества решения поставленной задачи за счет варьирования численности роботов в зависимости от сложности задачи;
- высокая надежность системы и устойчивость к воздействиям среды функционирования.

В большинстве исследований в области групповой робототехники, в том числе в РРТС, рассматривается следующий типовой сценарий функционирования роботов (далее «агентов»). Имеется множество агентов $R = 1, \dots, n$ и множество задач $O = 1, \dots, m$. Агенты получают от оператора по каналу связи $c$ данные о задачах и совместно приступают к их выполнению, при этом выполнение задач является последовательным. То есть после выполнения первой задачи агенты выбирают вторую и переходят к ее выполнению. Такая последовательность действий повторяется до тех пор, пока не будут выполнены все $m$ задач. В теоретических исследованиях данный типовой сценарий часто называется задачей коллективного управления группой роботов [6] или задачей обеспечения коллективного поведения группы роботов [7]. С точки зрения практической реализации это может быть задача совместной транспортировки груза группой роботов [8].

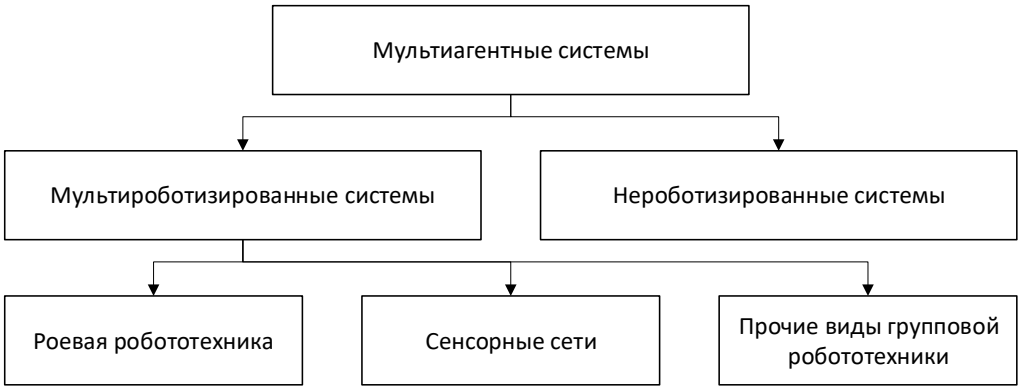



Рисунок 1 – Иерархическое представление терминов, используемых в групповой робототехнике

В последнее время появилось множество исследований, в которых сценарий использования РРТС существенно отличается от вышеописанного сценария [9–11]. Аналогично типовому сценарию, имеется множество агентов $R$ и множество задач $O$. Здесь и далее для краткости множество задач $O$ будем называть «заданием» агентов РРТС. Агенты РРТС получают задание от оператора по каналу связи, после чего перед непосредственным выполнением задач осуществляется процедура распределения задач. В результате выполнения данной процедуры за каждым из агентов будет закреплена по меньшей мере одна задача. Распределение задач может быть описано следующим соотношением [12]:

$$A: O \to R, \tag{1}$$

где $A$ – прямоугольная матрица с элементами $A_{j,i}$; $A_{j,i} = 1$, если задача $o_j$ закрепляется за агентом $r_i$, и $A_{j,i} = 0$ в противном случае.

Основные ограничения процедуры распределения задач заключаются в ограниченных ресурсах выполнения задачи и времени выполнения задачи:

- выполнение задач должно иметь строгую последовательность, то есть время начала следующей задачи $T_{j+1}$ не должно пересекаться с временем завершения выполнения текущей задачи $T_j$. Общее время выполнения задачи состоит из времени начала задачи (получение задания от оператора) $T_j$, времени ожидания перед выполнением задачи (процедура распределения задач) $W_j$ и продолжительности выполнения задачи (планирование пути перемещения и управления движением агента) $M_j$:

$$T_{j+1} \geq T_j + W_j + M_j; \tag{2}$$

- каждая задача $o_j$ может быть назначена только одному агенту $r_i$:

$$\sum_{r_i \in R} T_j = 1, \forall o_j \in O. \tag{3}$$

Цель процедуры распределения задач (ПРЗ) состоит в определении соответствий между элементами множеств $R$ и $O$ таким образом, чтобы обеспечить требуемое качество функционирования РРТС по показателям $Q = q_1, \dots, q_k$, где $k$ – количество показателей эффективности. В качестве таких показателей могут рассматриваться, например, время выполнения задания, расход аккумуляторной батареи агентов

РРТС, количество выполненных задач за ограниченный промежуток времени [13] и т.д. Формальная постановка задачи ПРЗ выглядит следующим образом: обеспечить такой результат распределения задач $O$ между агентами РРТС $R$ при ограничениях (2), (3), что

$$A: R, O, Q \to \{\Delta q_1, \dots, \Delta q_k\} \mid \forall \Delta q_l > 0, q_l \in Q, l = 1, \dots, k. \quad (4)$$

После процедуры распределения задач каждый агент $r_i$ приступает к планированию и выполнению списка закрепленных за ним задач $g_i$:

$$g_i = \{o_{j,1}, o_{j,2}, \dots, o_{j,h}\}, \quad (5)$$

где $h$ – количество задач, закрепленных за агентом $r_i$.

Процедура планирования выполнения задач (ПВЗ) основывается на классической задаче планирования пути (ПП), которую можно описать следующим образом. Необходимо найти последовательность опорных (промежуточных) точек пути $p = \{p_s, p_0, p_1, \dots, p_g\}$ между текущей позицией агента $p_s$ и целевой $p_g$ так, чтобы обеспечить требуемое качество функционирования РРТС по показателям $Q$. В случае процедуры ПВЗ в качестве опорных точек пути выступает список задач, закрепленных за агентом:

$$p_i = \{p_s, g_i\}. \quad (6)$$

В процессе функционирования агентов РРТС последовательность задач множества $p_i$ может быть изменена с целью увеличения эффективности функционирования РРТС. Процедура планирования выполнения задач имеет вид, отличный от задачи планирования пути: для каждого агента $r_i$ необходимо найти такую последовательность выполнения задач $P$ согласно $p_i$, что

$$P: r_i, p_i, Q \to \{\Delta q_1, \dots, \Delta q_k\} \mid \forall \Delta q_l > 0, q_l \in Q, l = 1, \dots, k. \quad (7)$$

Рассмотрим процедуру выполнения задачи (ВЗ) агентом РРТС. Децентрализация системы управления РРТС предполагает, что каждый агент $r_i$ самостоятельно принимает решение о своих действиях в данный момент времени $a_i(t)$ [14.] Каждое следующее действие агента $a_i(t+1)$ зависит от следующих параметров:

- вектор состояния агента $s_i(t)$, компонентами которого могут быть текущие координаты, заряд аккумуляторной батареи, скорость, ускорение и т.д.;
- вектор состояния среды $e_i(t)$, компонентами которого могут быть переменные, определяющие наличие в области видимости агента препятствий, других агентов, задач и т.д.

Таким образом, выбор действия $E$ агентом РРТС в следующий момент времени может быть описан выражением:

$$E: s_i(t), e_i(t), Q \to a_i(t+1). \quad (8)$$

Итоговая эффективность функционирования РРТС может быть представлена в виде зависимости целевого функционала $Y$ от результатов выполнения процедур ПРЗ, ПВЗ и ВЗ:

$$Y \leftarrow A, P, E. \quad (9)$$

Информацию о состоянии среды агент собирает с использованием бортовых датчиков и сенсоров, а также посредством информационного обмена с другими агентами РРТС. Каждый агент получает информацию по каналу связи $c$ лишь от нескольких соседних агентов, расположенных в области видимости $b_i$ агента $r_i$, то есть в области пространства, ограниченного окружностью с радиусом $L$. Иллюстрация информационного обмена между агентами РРТС, а также между агентами и оператором представлена на рисунке 2, где символами $O_p$ и $L'$ обозначены оператор РРТС и дальность действия телекоммуникационных устройств центра управления (ЦУ) соответственно. На практике значение $L'$ может существенно превышать область видимости агентов $L$, так как в отличие от агентов РРТС производительность оборудования ЦУ не лимитирована вычислительными или энергетическими ресурсами.

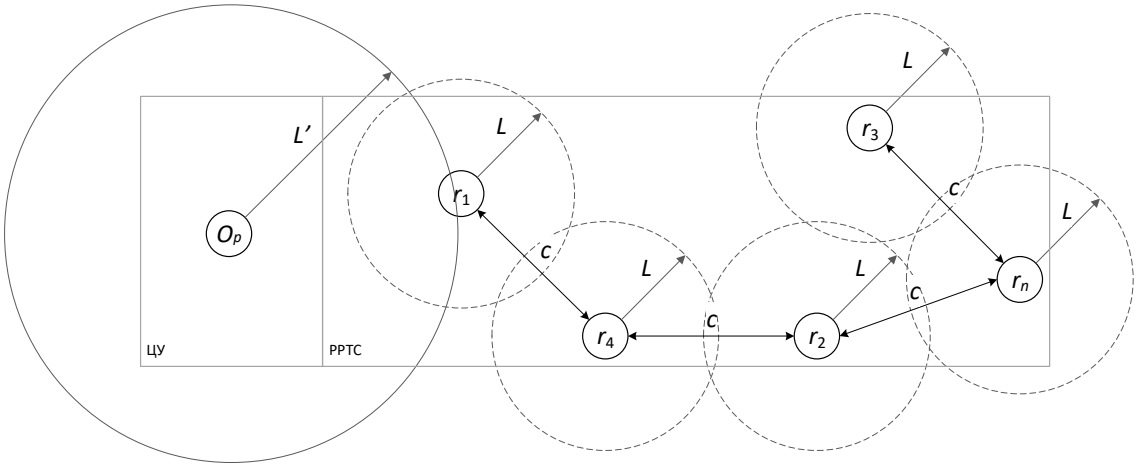



Рисунок 2 – Иллюстрация информационного обмена в РРТС

Исходя из этого, двухсторонний информационный обмен между оператором и агентами РРТС возможен только в том случае, когда расстояние между РРТС и оператором $d$ не превышает радиус видимости агентов $L$. В том случае, когда $L < d \leq L'$, то есть агенты находятся на некотором расстоянии от оператора, но в пределах действия телекоммуникационных устройств ЦУ, информационный обмен носит однонаправленный характер – от оператора к агентам РРТС. Агенты РРТС могут принимать данные от оператора (без возможности подтверждения получения сообщения), а также осуществлять информационный обмен друг с другом. Данные, которые отправляет оператор агентам РРТС, могут содержать как информацию о задании (множество задач $O$), так и любые другие необходимые инструкции для выполнения задания, за исключением конкретных управляющих сигналов для исполнительных устройств агентов (в отличие от ЦУ при централизованной стратегии управления). В том случае, если $d > L'$, агенты РРТС переходят в полностью автономное функционирование. При необходимости обратной связи с оператором, например, в результате выполнения задания или при возникновении внештатной ситуации, агентам РРТС необходимо вернуться в окрестность ЦУ. Также канал обратной связи с оператором может быть организован «по цепочке» между агентами, находящимися в области видимости друг друга, при условии нахождения хотя бы одного агента на расстоянии от ЦУ, не превышающем область видимости бортовых средств связи агента. Однако возможность реализации такого канала ограничена спецификой задания, которое выполняют агенты РРТС.

Информационный обмен между агентами РРТС осуществляется посредством широковещательной или групповой рассылки сообщений. Так как дальность действия бортовых средств связи агентов РРТС ограничена, то агент, сгенерировавший сообщение, рассылает его агентам в своей области видимости, после чего соседние агенты пересылают сообщения далее «по цепочке», то есть выступают ретрансляторами. Данный подход, с одной стороны, привносит в информационный обмен избыточность данных, а с другой стороны, компенсирует нестабильность каналов связи, что особенно актуально при функционировании агентов РРТС в недетерминированных или агрессивных средах.

Схематически процесс управления агентами РРТС представлен на рисунке 3, где $t_0$ означает момент получения задания от оператора, $t_f$ – момент завершения выполнения задания, а $t_b$ – момент передачи сообщения (отчета) оператору. С учетом ограниченной области видимости агентов РРТС, в том случае, если выполнение задания предполагает удаление агентов на расстояние $d > L'$, то отрезок времени между моментами $t_f$ и $t_b$ предполагает перемещение агентов в окрестность ЦУ для передачи данных оператору.

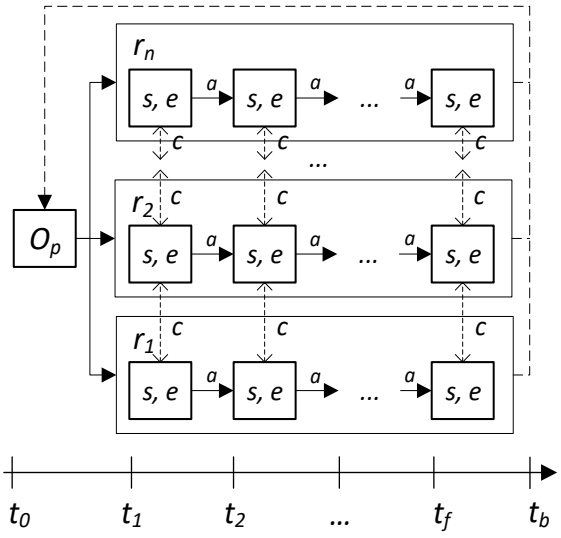



Рисунок 3 – Схематическое представление процесса управления РРТС

Таким образом, основное отличие рассмотренного сценария заключается в том, что агенты РРТС выполняют задачи не последовательно, а параллельно, что требует обязательного использования процедуры распределения задач между агентами РРТС. Такой подход позволяет существенно сократить время выполнения задания РРТС. На практике к подобным задачам можно отнести, например, мониторинг большой территории с целью поиска лесных пожаров [15] или объектов/людей после чрезвычайного происшествия [16]. В описанных задачах предполагается, что площадь рабочей области РРТС $S(O)$ существенно превышает площадь охвата бортовых датчиков и сенсоров агентов РРТС с учетом их области видимости $b_i$, то есть $S(O) > \sum S(b_i)$. Исходя из этого, данный сценарий предлагается называть пространственно-распределенной задачей. Блок-схема обобщенного сценария выполнения РРТС пространственно-распределенной задачи показана на рисунке 4.

На рисунке 4 блок 1 соответствует процедуре информационного обмена, инициированного оператором, в результате выполнения которой агенты РРТС получают задание $O$. Блоки 2–4 соответствуют процедурам ПРЗ, ПВЗ и ВЗ, описанным ранее. Блок 5 представляет собой процедуру информационного обмена между агентами РРТС с целью получения информации о состоянии ближайших агентов и возможности выполнения закрепленных за ними задач. В случае невозможности выполнения задачи определенным агентом, процедура ПРЗ повторяется, то есть осуществляется перераспределение задач и корректировка последовательности их выполнения каждым агентом. Блок 6 аналогичен блоку 1 с той разницей, что инициализацию информационного обмена осуществляют агенты РРТС с целью предоставления информации о результатах выполнения задания. Блок 7 представляет собой процедуру самодиагностики агента на предмет исправности бортовых датчиков и сенсоров, исполнительных устройств, а также уровня заряда аккумуляторной батареи. Эта процедура также выполняется на пятом этапе представленной блок-схемы для получения текущего состояния агента (блок 5 раскрывает особенности коллективного поведения агентов в случае неисправности, а блок 7 – индивидуального). При невозможности продолжения функционирования агент посылает соседним агентам или оператору соответствующее сообщение и отправляется в ЦУ для последующего ремонта или зарядки. Данный блок размещен в конце блок-схемы, так как предполагается, что перед началом функционирования агента его диагностику проводит обслуживающий персонал или оператор. А в процессе функционирования агента процедура самодиагностики может выполняться через заданный промежуток времени.

Одним из ключевых преимуществ использования РРТС является возможность масштабирования количества агентов как при увеличении сложности задания (например, увеличение площади территории, на которой необходимо осуществить мониторинг или разведку для сбора данных) [17], так и в случае неисправности или выхода из строя одного или нескольких агентов.

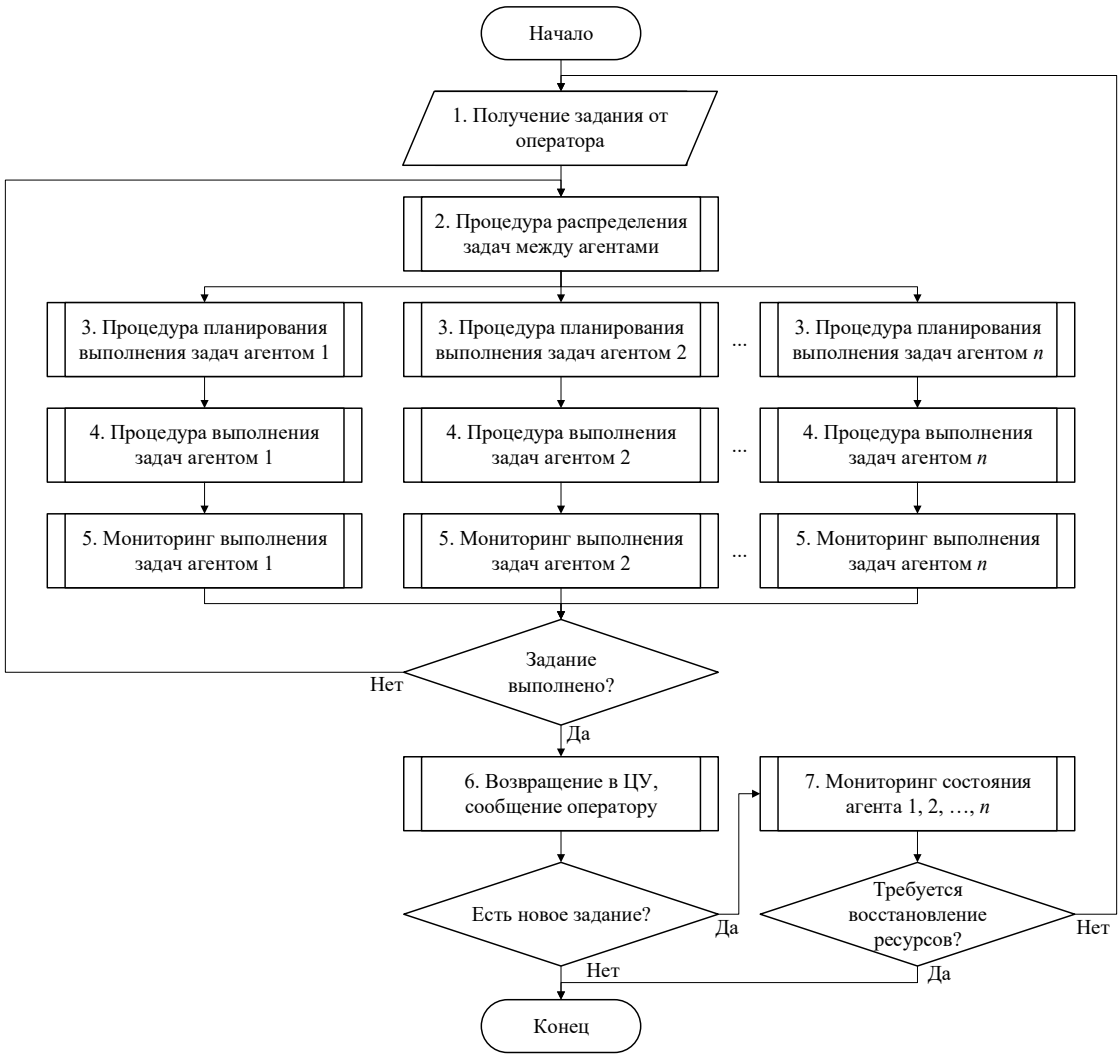



Рисунок 4 – Блок-схема обобщенного сценария выполнения РРТС пространственно-распределенной задачи

Дополнительно привлеченные агенты могут быть как направлены оператором из ЦУ, так и переназначены в ходе выполнения ранее закрепленной за агентом задачи с меньшим приоритетом важности (при условии нахождения агентов в области видимости средств связи ЦУ). Процесс масштабирования численности агентов РРТС $R$ может быть представлен как объединение двух множеств:

$$R = R_1 \cup R_2, \quad (10)$$

где $R_1$ – исходное множество агентов РРТС; $R_2$ – множество привлеченных агентов. При необходимости масштабирования численности агентов $R$ переназначение привлеченных агентов $R_2$ осуществляется оператором при формировании задания $O$ на первом этапе блок-схемы, представленной на рисунке 4. Возможна ситуация, когда требуемое для масштабирования системы количество агентов в ЦУ отсутствует, тогда привлечение новых агентов осуществляется в процессе выполнения задания агентами РРТС $R_1$. Передача информации о задании осуществляется посредством информационного обмена между агентами, и в этом случае в качестве оператора в блоке 1 рисунка 4 выступает тот агент множества $R_1$, который передал данные агенту множества $R_2$. Далее привлеченные агенты функционируют согласно блокам 2–7 обобщенного сценария выполнения РРТС пространственно-распределенной задачи.

**2. Обобщенные модели угроз и нарушителя ИБ РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач.** В работах [18, 19] рассмотрены общие уязвимости информационной безопасности МРС, в число которых входят:

- децентрализованное управление МРС;
- пространственная удаленность агентов МРС и нахождение их вне пределов контролируемой территории;
- необходимость использования телекоммуникационных технологий для обмена информацией между агентами системы;
- ограниченность информации агентов обо всей системе;
- непредсказуемая динамика среды функционирования.

Перечисленные уязвимости характерны и для РРТС ввиду специфики архитектуры систем данного вида, а также ввиду особенностей функционирования при выполнении пространственно-распределенных задач. Выявленные уязвимости РРТС делают возможным возникновение и реализацию следующих угроз информационной безопасности [20]:

- несанкционированный перехват сообщений в процессе информационного обмена между агентами;
- нарушение целостности данных, передаваемых в процессе информационного обмена между агентами;
- несанкционированный доступ к данным;
- отказ в обслуживании;
- перехват данных с последующей их модификацией и воспроизведением.

К основным механизмам атак на РРТС, формирующим рассмотренные угрозы, относятся [18, 20, 21]:

- атаки на каналы связи;
- сложность идентификации и аутентификации в РРТС ввиду отсутствия идентификаторов у агентов и отсутствия информации обо всех агентах системы;
- внедрение «вредоносных» агентов, которыми могут быть захваченные и перепрограммированные злоумышленником агенты РРТС.

В разрезе процесса масштабирования численности агентов РРТС наиболее значимым из рассмотренных механизмов атак можно считать внедрение вредоносных агентов, задачей которых является недопущение или снижение эффективности выполнения задания РРТС. Данный механизм реализуется путем внедрения вредоносного агента в состав РРТС для формирования множества сообщений при информационном обмене, которые приводят к снижению эффективности принимаемых агентами решений $a(t+1)$, что затрудняет приращение целевого функционала.

В работах [16–18] рассмотрены и считаются наиболее перспективными следующие виды атак на РРТС:

- перехват вредоносным агентом сообщений с последующей их модификацией и воспроизведением (атаки Man in the Middle);
- генерация и передача вредоносным агентом ложных данных о собственном состоянии, состоянии среды и выбранных действиях, направленных на уменьшение приращения целевого функционала $\Delta Y$.

В работах [19, 22] перечисленные атаки относят к классу «мягких атак», особенностью которых является отсутствие явно идентифицируемых признаков нарушения ИБ РРТС, так как при вредоносном воздействии, с одной стороны, все подсистемы агентов функционируют в штатном режиме, а с другой стороны, агенты не могут выявить факт уменьшения эффективности принимаемых действий.

Потенциальные нарушители ИБ РРТС могут быть разделены на два типа с точки зрения наличия возможности постоянного или разового доступа к агентам РРТС:

- нарушители, не имеющие права доступа к агентам РРТС, – внешние нарушители;
- нарушители, имеющие права доступа к агентам РРТС, – внутренние нарушители.

К внутренним нарушителям ИБ РРТС можно отнести лиц, привлеченных к разработке и обслуживанию РТС, которые используются в составе РРТС:

- проектировщики;
- разработчики программно-аппаратной части системы управления;
- операторы;
- обслуживающий персонал (например, сотрудники, производящие калибровку датчиков, настройку параметров программной части системы управления, ремонтные работы РТС и т.д.).

Внутренние нарушители могут оказывать влияние как на программную, так и аппаратную часть системы управления агентов РРТС. Исходя из этого, угрозы, исходящие от данной группы нарушителей, совпадают со списком всех рассмотренных угроз ИБ РРТС.

Внешние нарушители способны оказать воздействие преимущественно на аппаратную составляющую системы управления агента РРТС (нарушение работы датчиков и сенсоров РРТС, каналов связи). Воздействие на программную составляющую системы управления агентов РРТС требует от нарушителя понимания принципов построения децентрализованных систем управления, протоколов и алгоритмов функционирования агентов, навыков программирования на низкоуровневых языках программирования, а также достаточное количество времени для внесения изменений в определенный модуль системы управления агента РРТС (например, при физическом захвате агента и попытке его перепрограммировать). Только в этом случае угрозы от данной группы нарушителей будут совпадать со списком всех рассмотренных угроз ИБ РРТС.

Обобщенные модели угроз и нарушителя ИБ РРТС, приведенные в данном разделе, носят декларативно-описательный характер. Это обусловлено тем фактом, что данные модели построены на основе концептуального описания РРТС как архитектуры робототехнической системы без учета конкретных характеристик устройств, входящих в состав системы. Таким образом, приведенные результаты не могут рассматриваться как завершенные самостоятельные документы, однако могут быть использованы в качестве абстрактных шаблонов или вспомогательной информации при разработке моделей для конкретной робототехнической системы.

**3. Актуальное состояние проблемы обеспечения ИБ РРТС при внедрении вредоносного агента.** В настоящее время известен ряд исследований, направленных на обеспечение информационной безопасности МРС. Разработано множество подходов, моделей и методов, позволяющих либо уменьшить ущерб от реализации угроз, либо уменьшить вероятность их реализации. Рассмотрим результаты этих исследований с точки зрения возможности их применения в РРТС.

В статье [19] рассмотрен вопрос информационной безопасности робототехнических комплексов с роевым интеллектом. В данной работе рассматривается класс поведенческих алгоритмов, в частности муравьиный алгоритм поиска кратчайшего пути [23]. Поведенческие алгоритмы, по сути, являются оптимизационными, то есть направлены на повышение эффективности системы по определенному критерию, поэтому будем считать, что описанная уязвимость характерна для всего класса алгоритмов подобного рода, например, алгоритм роя частиц [24], пчелиный алгоритм [25] и т.д. В работе описана атака типа «ложный путь», направленная на сенсорное восприятие роботами группы наилучшей альтернативы (предоставление ложной информации о стоимости того или иного пути). Продемонстрирован пример численного моделирования данной атаки, согласно которой воздействие одного вредоносного агента практически несущественно, но если соотношение вредоносных и обычных агентов в группе будет приближаться 1 к 1, то вероятность выбора группой роботов рационального пути существенно уменьшается. На основе этого исследования тем же коллективом авторов предложена модель безопасности мобильных мультиагентных робототехнических систем с коллективным управлением на основе полицейских участков (англ. POM – police office model) [26] и ее модификация [27]. Согласно этой идее, группа роботов изначально проектируется как гетерогенная группа, в которой часть агентов выполняют задачу обеспечения ИБ. Рабочая область группы роботов декомпозируется на ряд зон, для которых вводится зональная и межзональные процедуры безопасности. Недостатком такого подхода с точки зрения РРТС является сложность формирования полицейских участков как ввиду высокой масштабируемости системы, так и возможной пространственной рассредоточенности агентов при функционировании в недетерминированной среде.

В работе [22] представлен ряд методов, направленных на повышение эффективности обнаружения нарушений семантической целостности информации в группах беспилотных транспортных средств (БТС) для обеспечения их безопасного информационного взаимодействия в процессе функционирования. Основная идея заключается в комбинации репутационных механизмов и подхода, предполагающего формирование временных подгрупп БТС, один из которых будет выполнять оценку целостности информации. Данная идея имеет некоторое сходство с моделью полицейских участков и аналогичные недостатки применительно к РРТС.

В ряде исследований [28–30] рассмотрена задача выявления вредоносных роботов при их воздействии на коллективное принятие решений в процессе функционирования РРТС. Согласно полученным результатам, достаточно одного вредоносного агента для формирования цепных реакций в процессе достижения консенсуса для снижения эффективности функционирования всей системы. Авторами работы рассмотрены

задачи, направленные на обеспечение ИБ процесса достижения консенсуса относительно выбора наилучшей альтернативы. В работе предложен критерий уверенности агента, который позволяет после $n$-й итерации выявить вредоносного агента и предпринять меры для обеспечения ИБ РРТС. Недостатком данного подхода является тот факт, что разработанные методы направлены на анализ поведения агентов, что требует некоторого времени для сбора данных об агентах и расчета показателя уверенности. Согласно представленной на рисунке 3 схеме управления РРТС при выполнении пространственно-распределенной задачи вредоносный агент может осуществить атаку на первом шаге функционирования РРТС, что приведет к неэффективному распределению задач и последующему уменьшению целевого функционала.

Авторами статьи [31] рассмотрены уязвимости и угрозы безопасности роя дронов, проанализированы различные стратегии взлома роя дронов, разработан ряд предложений и рекомендаций по повышению безопасности использования БПЛА и дронов. Среди предложенных решений рассматриваются различные методы, включая нейронные сети и системы предотвращения вторжений на основе нечеткой логики. Однако основное внимание уделено аппаратной составляющей системы управления БПЛА без учета их программной составляющей.

В работе [32] представлен набор методов для обеспечения информационной безопасности систем управления группой роботов на основе анализа поведения роботов и вычисления уровня доверия к ним. Предложенные решения позволяют формировать доверительные отношения между роботами и выявлять аномальное поведение вредоносных роботов, внедренных в группу. Стоит отметить, что данное решение предполагает наличие в группе роботов лидера, обеспечивающего эффективность выполнения задания. Такой подход позволяет использовать разработанные методы для групп роботов с централизованным и смешанным типом управления, а для децентрализованного типа управления – только в случае выполнения задач коллективного движения, так как все роботы группы находятся на относительно малом расстоянии друг от друга и попадают в область видимости других роботов. Таким образом, данное решение невозможно использовать для РРТС при выполнении пространственно-распределенных задач без модификации, например, путем выделения ряда подгрупп агентов РРТС с локальными лидерами на основе оценки расстояния между агентами. Однако эффективность такой модификации будет сильно зависеть как от площади рабочей области, так и от количества агентов РРТС, так как возможна такая ситуация, что в определенный момент времени при выполнении задач отдельные подгруппы будут состоять лишь из одного агента.

В работе [33] рассматривается задача выявления и идентификации угроз нарушения ИБ МРС. В рамках решения данной задачи предложен ряд методов, направленных на минимизацию времени выявления информационных воздействий вредоносных агентов. Основная идея заключается в формировании шаблонов эталонного и аномального поведения агентов на основе косвенных признаков (скорость, ускорение и т.д.). К недостаткам данного решения можно отнести необходимость формирования базы данных аномального поведения с учетом особенностей аппаратной реализации агентов, а также необходимость нахождения агентов в области видимости друг друга для своевременного выявления вредоносного поведения, что не всегда обеспечивается в случае выполнения пространственно-распределенных задач.

В статье [34] представлен метод идентификации вредоносных агентов в РРТС на основе анализа истории действий агентов, которые встречаются в процессе выполнения задания. В качестве основного задания рассматривается задача перемещения агентов для формирования топологии регулярной решетки на заданной области. Исходя из этого, авторы работы вводят допущение, что каждый агент встретится с 8 ближайшими соседними агентами с некоторой вероятностью, что, в свою очередь, сделает возможным своевременно выявить вредоносного агента. Представлен численный эксперимент, подтверждающий работоспособность предложенного решения. Однако применимость данного метода ограничена задачами коллективного движения, а эффективность решения при выполнении агентами РРТС пространственно-распределенных задач требует дополнительных экспериментальных исследований.

Рассмотренные методы направлены на выявление вредоносных агентов после факта их внедрения в состав РРТС. Однако в литературе встречается ряд решений, направленных на разработку технологий аутентификации и авторизации агентов РРТС, позволяющих минимизировать количество внедренных вредоносных агентов. Так, в рамках проведенного аналитического обзора по данной тематике, авторы работы [35] выделяют данную задачу как одну из важнейших проблем обеспечения комплексной ИБ РРТС, при этом отмечают сложность ее реализации ввиду отсутствия идентификаторов у агентов. В качестве одного из перспективных вариантов решения задачи авторами предложено использовать групповой идентификатор агентов, например, на основе выданного оператором задания. Однако данная идея не получила дальнейшего развития авторами статьи.

Авторы работы [36] провели исследование и оценку эффективности обеспечения информационной безопасности РРТС, состоящей из 3 БПЛА, при наличии внешних информационных воздействии в процессе коммуникации каждого из агентов с центром управления. Эксперимент был проведен в среде моделирования Gazebo [37] с использованием средств аутентификации, встроенных в фреймворк ROS2 (англ. «Robotic operation system» – робототехническая операционная система) [38]. Результаты проведенных исследований подтвердили эффективность применения данного инструмента, но его использование вызвало задержку при передаче данных между сторонами, что существенно увеличило время симуляции.

Работа [39] направлена на повышение эффективности выполнения задания группой БПЛА путем модификации инерциальной системы навигации и обеспечения защищенной передачи измерений данной системы другим БПЛА. Данный подход позволяет оптимально осуществлять планирование пути перемещения агентов в динамических средах с множеством препятствий, а также в агрессивных средах, которые предполагают возможность воздействия злоумышленника на информационный обмен между БПЛА. Авторы предложили гибридную криптосистему, включающую процедуру аутентификации по подписи с использованием алгоритма RSA. Основной акцент в работе авторами сделан на модификацию инерциальной системы навигации БПЛА, вследствие чего оценка эффективности обеспечения информационной безопасности не приведена. Также авторами упоминается, что обеспечение работы предложенного решения в реальном масштабе времени возможно при использовании дополнительного аппаратного обеспечения, что требует проведения экспериментальных исследований, направленных на оценку возможности применения данного решения в условиях ограниченных вычислительных платформ агентов РРТС.

В работе [40] представлен протокол взаимной аутентификации для группы БПЛА на основе механизма вычисления репутации и доверия. Авторы подтвердили работоспособность предложенного решения путем проведения серии экспериментов с 20 БПЛА с наличием от 10 до 40 процентов вредоносных агентов. К особенностям данного протокола можно отнести обязательное требование наличия индивидуальных идентификаторов у агентов, что затрудняет использование данного решения без его модификации. К подобной модификации можно отнести, например, использование технологии блокчейн [41] для закрепления идентификатора за каждым агентом РРТС. Такой подход, с одной стороны, позволит использовать методы и протоколы аутентификации с обязательным наличием идентификаторов для РРТС, а с другой стороны, увеличит вычислительную сложность решения, что не всегда допустимо.

**4. Количественная оценка влияния нарушителя на функционирование РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач.**

***4.1. Постановка задачи проведения эксперимента.*** В качестве пространственно-распределенной задачи рассмотрим задачу поиска пострадавших людей в результате чрезвычайного происшествия для их последующего спасения [16]. Допустим, что имеется некоторая территория, на которой определено множество задач $O = 1, \dots, m$. Будем считать, что каждая задача $o_j \in O$ содержит координаты пространства, в котором потенциально находятся пострадавшие люди. Тогда каждому агенту из множества $R_1 = 1, \dots, n$ необходимо переместиться в определенную область и провести мониторинг с помощью бортовых сенсоров, например, устройства видеозаписи. После этого необходимо вернуться на базу и передать собранные данные оператору для дальнейшей обработки и принятия решений по проведению дальнейших поисково-спасательных мероприятий.

Допустим, количество агентов $n$ множества $R_1$ меньше количества задач $m$, что не позволяет распределить задачи между агентами и выполнить задание. Тогда оператор привлекает дополнительное множество агентов $R_2$ численностью $z = m - n$ агентов, а общее количество агентов системы становится равным $n+= z$. Целевая функция заключается в оптимизации выбора задач агентами РРТС таким образом, чтобы минимизировать время выполнения задания. При этом общим временем выполнения задания будем считать максимальное время выполнения задачи отдельным агентом:

$$T = \max\left(t_i(o_j)\right) \to min, i = \overline{1,n}, \tag{11}$$

где $t_i(o_j)$ – время, необходимое для выполнения закрепленных за агентом РРТС задач.

Далее, согласно обобщенному сценарию выполнения РРТС пространственно-распределенной задачи, система численностью $n$ агентов, находясь в ЦУ, получает задание $O$ от оператора по каналу связи. После этого агенты РРТС в автономном режиме осуществляют распределение задач и их выполнение с последующим возвращением в ЦУ для передачи собранных данных оператору и получения следующего задания $O_{next}$.

Предположим, что среди множества агентов $R_2$ может быть некоторое количество вредоносных агентов $\hat{z}$. Под поведением вредоносного агента будем понимать выбор наиболее удаленной задачи для выполнения в процессе ПРЗ, при этом выполнять задачу агент не будет (вредоносный агент остается на исходной позиции, не влияя явно на показатель $T$). Аналогичное поведение вредоносных агентов рассмотрено в эксперименте в работе [42], однако количественные показатели влияния внедренных вредоносных агентов не представлены. С учетом описанного поведения вредоносных агентов и ограниченных возможностей аппаратной реализации агентов РРТС вводим допущение, что энергетический ресурс агентов позволяет выполнить не более 2 задач из общего списка. В ходе выполнения задания первый освободившийся агент РРТС запрашивает у соседних агентов статус выполнения задач, в результате чего выявляется задача, не закрепленная ни за одним из агентов. Тогда этот агент выбирает дополнительную задачу для выполнения. В результате целевая функция будет зависеть от времени выполнения всех задач, закрепленных за агентом:

$$T' = \max\left(t_i(g_i)\right) \to min, i = \overline{1,n}. \tag{12}$$

С позиции информационной безопасности задача исследования заключается в том, чтобы определить уменьшение целевого функционала $\Delta T$ выполнения задания РРТС при воздействии внедренных вредоносных агентов:

$$\Delta T = T' - T. \tag{13}$$

***4.2. Результаты эксперимента.*** Для проведения эксперимента была выполнена программная реализация на языке программирования Python. Визуализация пути перемещения агентов РРТС, а также формирование графиков для оценки влияния вредоносных агентов выполнены с помощью библиотеки Matplotlib. При проведении симуляции был использован компьютер со следующими характеристиками: процессор Intel Core i7-8550U с тактовой частотой 1,8 ГГц, 8 ГБ оперативной памяти. Использованы параметры моделирования, указанные в таблице 1.

Таблица 1 – Параметры моделирования

| **Наименование параметра** | **Значение** |
|---|---|
| Количество агентов РРТС, $n$ | 10, 50, 100 |
| Количество вредоносных агентов, $\hat{z}$ | 0, 1, 25 %, 50 % |
| Количество экспериментов | 100 |
| Количество задач, $m$ | 10, 50, 100 |
| Скорость перемещения агентов | 0,5 м/с |
| Размер карты | 60 х 60 м |

На рисунке 5 представлены примеры экспериментов без вредоносных агентов (рис. 5а), с 1 вредоносным агентом (рис. 5б), с 3 вредоносными агентами (рис. 5в) и с 5 вредоносными агентами (рис. 5г).

На рисунке 5 цветные точки обозначают исходные позиции агентов РРТС, а серые квадраты – позиции задач. Цветные сплошные линии обозначают пути перемещения агентов РРТС, а пунктирные линии (рис. 5б–г) – предполагаемые пути вредоносных агентов к закрепленным за ним задачам. Оси на представленном рисунке определяют размерность карты.

В случае отсутствия вредоносных агентов процедура распределения задач выполнялась один раз, в результате чего за каждым из агентов было закреплено по одной задаче. В качестве алгоритма распределения задач использован метод на основе жадного алгоритма [43].

При наличии вредоносных агентов в РРТС процедура распределения задач выполнялась дважды: первый раз при получении списка задач от оператора, а второй раз – после выполнения первой задачи. Таким образом, некоторые пути перемещения агентов представляют собой ломанные линии, как показано на рисунках 5б–г.

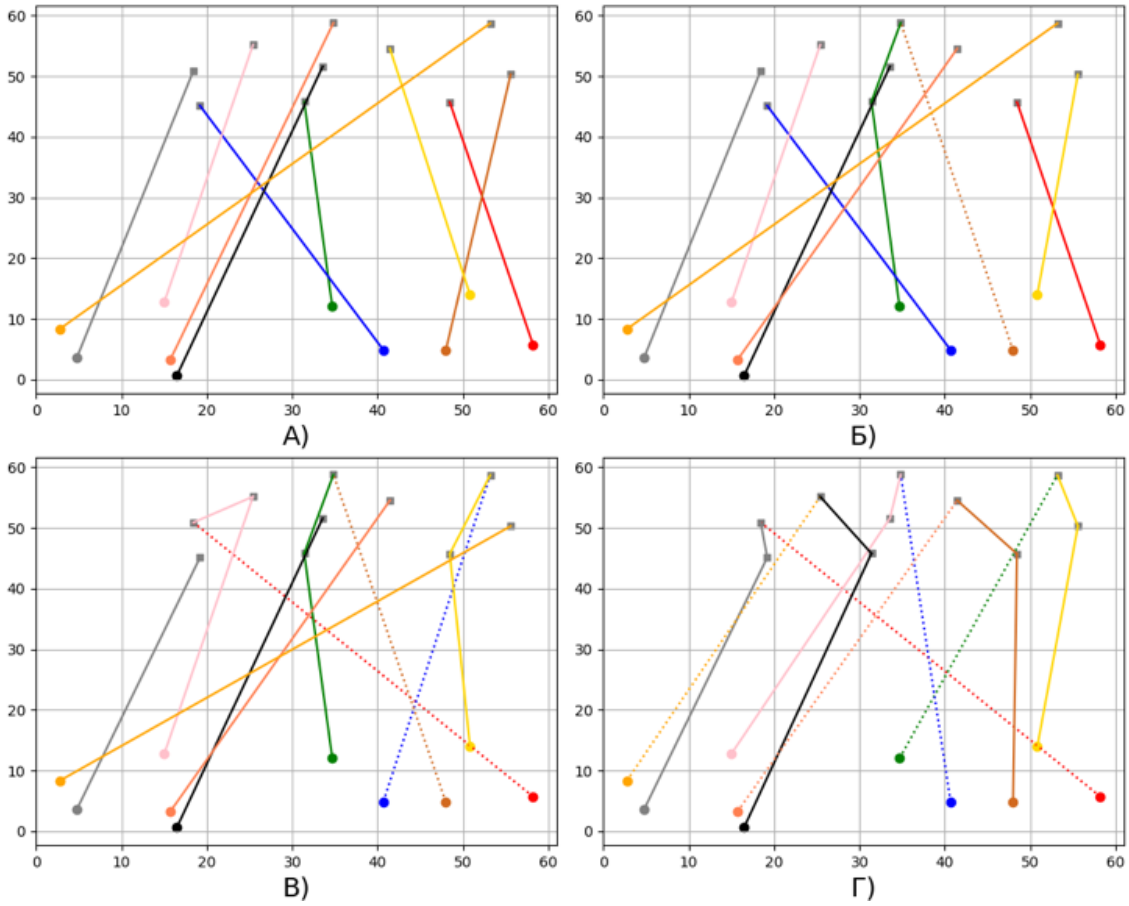



Рисунок 5 – Пример выполнения задания РРТС из 10 агентов: а) без вредоносных агентов; б) с 1 вредоносным агентом; в) с 3 вредоносными агентами; г) с 5 вредоносными агентами

На рисунках 6–8 показаны результаты моделирования выполнения задания РРТС численностью 10, 50 и 100 агентов соответственно, где полупрозрачные линии демонстрируют результаты отдельных экспериментов, а непрозрачные линии представляют собой линии тренда.

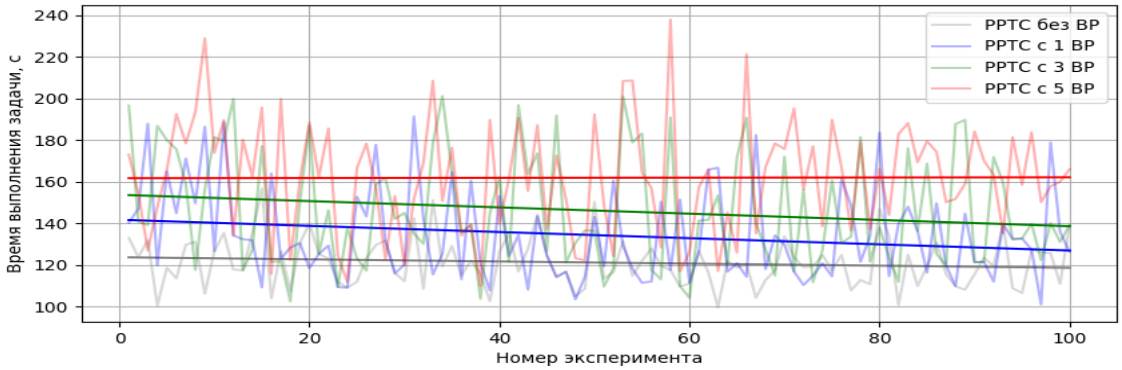



Рисунок 6 – Результаты выполнения задания РРТС из 10 агентов

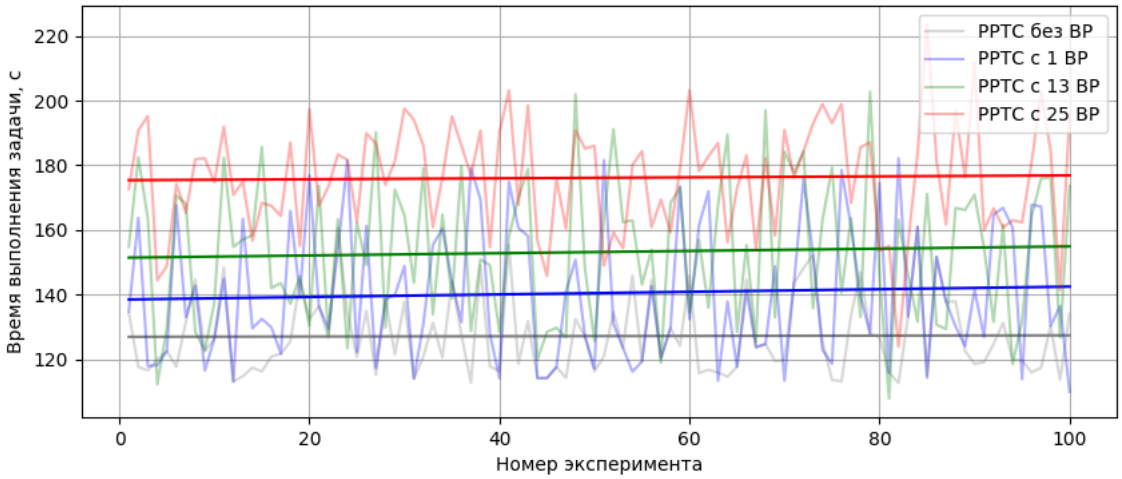



Рисунок 7 – Результаты выполнения задания РРТС из 50 агентов

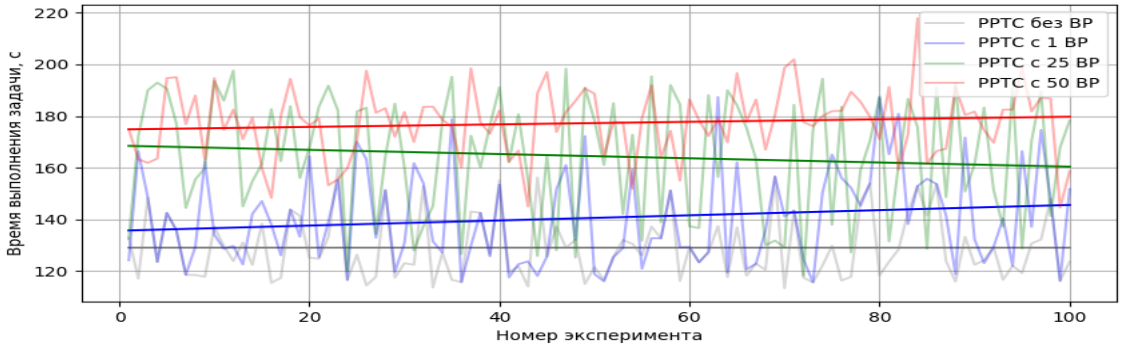



Рисунок 8 – Результаты выполнения задания РРТС из 100 агентов

При оценке времени выполнения задания РРТС в данной работе не учитывались кинематические характеристики агентов РРТС, а также возможность столкновения агентов друг с другом, что требует маневрирования, тем самым увеличивая продолжительность выполнения задачи. Таким образом, общее время выполнения задания считается максимальной продолжительностью выполнения задачи отдельным агентом, который движется с постоянной скоростью. Также стоит отметить, что в реальной системе также итоговое время будет несколько больше, так как не учитывается время, затраченное на выполнение процедуры распределения задач, и не учитывались задержки в каналах связи в процессе информационного обмена между агентами РРТС.

Для оценки влияния вредоносных агентов на результат функционирования РРТС интерес также представляют максимальные, средние и минимальные значения показателей эффективности выполнения задания, представленные в таблице 2. Согласно полученным результатам, при наличии 1 вредоносного

агента среднее время выполнения задания РРТС увеличивается до 8,23 % (129,08 с против 140,67 с). При этом в реальных условиях использования РРТС необходимо учитывать, что подобное уменьшение эффективности будет только в том случае, если хотя бы у одного из агентов РРТС останется энергетический заряд для выполнения задачи, закрепленной за вредоносным агентом. В противном случае агенты РРТС должны вернуться на базу для заряда аккумулятора и последующего выполнения оставшейся задачи. Если же рассматривать задачи, для которых оперативность их выполнения является критически важным показателем (как в текущей задаче), то подобное задание можно считать невыполненным.

Необходимо отметить, что наблюдаются и такие ситуации, когда при наличии вредоносных агентов минимальное время выполнения задания РРТС было меньше по сравнению с симуляцией без вредоносного агента. Это объясняется тем, что позиции задач генерировались случайным образом и задачи, которые выбрали обычный и вредоносный агенты, оказались на малом расстоянии друг от друга.

При масштабировании численности агентов РРТС и увеличении количества вредоносных агентов до 25 % среднее время выполнения задания увеличивается на 17 % (127,12 с против 153,16 с), а при наличии 50 % вредоносных агентов – на 25,14 % (121,23 с против 161,95 с). Приведенные значения можно считать минимальной величиной ущерба в результате реализации атаки внедренного вредоносного агента. Рассмотренные значения взяты по минимальной границе, но являются достаточно наглядными. Расчет более точных значений показателей является достаточно трудной задачей без рассмотрения конкретной программно-аппаратной реализации робототехнических устройств, используемых в качестве агентов РРТС.

Таблица 2 – Показатели качества выполнения задания РРТС с различным количеством вредоносных агентов

| **Критерий** | **Время выполнения задания, с** | | | |
|---|---|---|---|---|
| Количество агентов $n$ / вредоносных агентов $\hat{z}$ | 10/0 | 10/1 | 10/3 | 10/5 |
| Максимальное значение | 156,72 | 191,32 | 201,12 | 237,81 |
| Среднее значение | 121,23 | 134,34 | 146,14 | 161,95 |
| Минимальное значение | 99,73 | 101,17 | 102,61 | 110,07 |
| Количество агентов $n$ / вредоносных агентов $\hat{z}$ | 50/0 | 50/1 | 50/13 | 50/25 |
| Максимальное значение | 160,97 | 182,17 | 202,81 | 223,65 |
| Среднее значение | 127,12 | 140,45 | 153,16 | 176,15 |
| Минимальное значение | 112,62 | 109,94 | 107,79 | 123,79 |
| Количество агентов $n$ / вредоносных агентов $\hat{z}$ | 100/0 | 100/1 | 100/25 | 100/50 |
| Максимальное значение | 159,71 | 187,38 | 198,38 | 217,9 |
| Среднее значение | 129,08 | 140,67 | 164,46 | 177,32 |
| Минимальное значение | 113,43 | 115,65 | 118,28 | 144,57 |

Согласно результатам проведенного эксперимента, вредоносный агент начинает атаку на первом шаге функционирования РРТС, в результате чего снижается эффективность выполнения задания. Так, работы, рассмотренные в части 3, позволяют выявить вредоносного агента, однако в представленном эксперименте его выявление не имеет смысла, так как агент уже осуществил атаку и больше может не находиться в области видимости агентов РРТС. Впоследствии этот же агент может внедриться в другую РРТС и повторно осуществить вредоносное воздействие. Исходя из этого, решением подобной задачи является разработка методов и алгоритмов аутентификации и авторизации агентов РРТС, которые позволят учесть все особенности систем данного вида, а также минимизировать возможность влияния вредоносных агентов на первый шаг функционирования РРТС. Результаты проведенных литературного анализа и эксперимента наглядно демонстрируют противоречие в теории и практике проектирования и разработки систем управления РРТС, которое заключается в необходимости комплексного подхода к обеспечению безопасного функционирования РРТС с одной стороны, и недостаточном уровне развития научно-методического аппарата обеспечения ИБ РРТС с другой стороны, чем и определяется актуальность дальнейших исследований в данной области.

**Заключение.** В данной работе рассмотрен вопрос информационной безопасности РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач. В ходе проведенных исследований были получены следующие основные результаты:

1. Формализована обобщенная модель функционирования РРТС. Выделен класс пространственно-распределенных задач, характеризующийся обязательным использованием процедуры распределения задач.

2. Сформированы обобщенные модели угроз и нарушителя информационной безопасности РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач. Данные результаты могут быть полезны специалистам в области проектирования и разработки РРТС.

3. Проведен анализ исследований, направленных на обеспечение информационной безопасности МРС с точки зрения возможности их применения в РРТС. Выявлены работы, которые в перспективе могут быть использованы для комплексной защиты информации в РРТС.

4. Проведена количественная оценка воздействия внедренных вредоносных агентов на результат функционирования РРТС при реализации атаки. Обоснована необходимость разработки технологий аутентификации и авторизации агентов РРТС в процессе масштабирования их численности агентов для выполнения пространственно-распределенных задач.

Дальнейшие исследования будут направлены на реализацию методов и алгоритмов аутентификации и авторизации агентов РРТС в процессе масштабирования численности агентов при выполнении пространственно-распределенных задач, предназначенных для комплексного обеспечения информационной безопасности функционирования РРТС совместно с известными методами выявления и идентификации вредоносных агентов.

**Библиографический список**

1. Zakiev, A. Swarm Robotics: Remarks on Terminology and Classification / A. Zakiev, T. Tsoy, E. Magid // Interactive Collaborative Robotics (ICR 2018). – 2018. – P. 291–300.

2. Каляев, И. А. Модели и алгоритмы коллективного управления в группах роботов / И. А. Каляев, А. Р. Гайдук, С. Г. Капустян. – Москва : ФИЗМАТЛИТ, 2009. – 280 с.

3. Петренко, В. И. Прогнозная оценка траектории руки оператора для решения обратной задачи динамики при копирующем управлении / В. И. Петренко, Ф. Б. Тебуева, М. М. Гурчинский, В. О. Антонов, А. С. Павлов // Труды СПИИРАН. – 2019. – Т. 18, № 1. – С. 123–147.

4. Павлов, А. С. Методика планирования траектории движения группы мобильных роботов в неизвестной замкнутой среде с препятствиями / А. С. Павлов // Системы управления, связи и безопасности. – 2021. – № 3. – С. 38–59.

5. Kovács, G. Resource management simulation using multi-agent approach and semantic constraints / G. Kovács, N. Yussupova, D. Rizvanov // Pollack Period. – 2017. – Vol. 12, № 1. – P. 45–58.

6. Пшихопов, В. Х. Групповое управление движением мобильных роботов в неопределенной среде с использованием неустойчивых режимов / В. Х. Пшихопов, М. Ю. Медведев // Труды СПИИРАН. – 2018. – Т. 60, № 5. – С. 39–63.

7. Кривенко, М. П. Компьютерная модель возникновения коллективного поведения роботов / М. П. Кривенко, М. И. Анчеков // Известия Кабардино-Балкарского научного центра РАН. – 2019. – № 6. – С. 21–26.

8. Alonso-Mora, J. Multi-robot formation control and object transport in dynamic environments via constrained optimization / J. Alonso-Mora, S. Baker, D. Rus // The International Journal of Robotics Research. – 2017. – Vol. 36, № 9. – P. 1000–1021.

9. Dai, W. Multi-robot dynamic task allocation for exploration and destruction / W. Dai, H. Lu, J. Xiao, Z. Zeng, Z. Zheng // Journal of Intelligent and Robotic Systems: Theory and Applications. – 2020. – Vol. 98, № 2. – P. 455–479.

10. Dutta, A. Correlation Clustering Based Coalition Formation for Multi-Robot Task Allocation / A. Dutta, V. Ufimtsev, A. Asaithambi // Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. – 2019. – P. 906–913.

11. Tkach, I. A Modified Distributed Bees Algorithm for Multi-Sensor Task Allocation / I. Tkach, A. Jevtić, S. Y. Nof, Y. Edan // Sensors. – 2018. – Vol. 18. – P. 759–775.

12. Saravanan, S. Review on state-of-the-art dynamic task allocation strategies for multiple-robot systems / S. Saravanan, K. C. Ramanathan, M. M. Ramya, M. N. Janardhanan // Industrial Robot. – 2020. – Vol. 47, № 6. – P. 929–942.

13. Khamis, A. Multi-robot Task Allocation: A Review of the State-of-the-Art / A. Khamis, A. Hussein, A. Elmogy // Cooperative Robots and Sensor Networks. – 2015. – P. 31–51.

14. Dorigo, M. Swarm intelligence / M. Dorigo, M. Birattari // Scholarpedia. – 2007. – Vol. 9, № 2. – P. 1462.

15. Sujit, P. B. Cooperative forest fire monitoring using multiple UAVs / P. B. Sujit, D. Kingston, R. Beard // 46th IEEE Conference on Decision and Control, 10–11 December 2007, New Orleans, Louisiana, USA. – 2007. – P. 4875–4880.

16. Чжай, М. Многоагентная робототехническая система спасения при землетрясениях : дис. ... канд. техн. наук / М. Чжай. – Москва : Московский государственный технический университет имени Н. Э. Баумана, 2019.

17. Petrenko, V. Path Planning Method in the Formation of the Configuration of a Multifunctional Modular Robot Using a Swarm Control Strategy / V. Petrenko, F. Tebueva, A. Pavlov, V. Antonov, M. Kochanov // Proceedings of the 7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019). – 2019. – P. 165–170.

18. Higgins, F. Threats to the swarm: Security considerations for swarm robotics / F. Higgins, A. Tomlinson, K. M. Martin // International Journal on Advances in Security. – 2009. – Vol. 2, № 2. – P. 288–297.

19. Зикратов, И. А. Анализ уязвимостей робототехнических комплексов с роевым интеллектом / И. А. Зикратов, Е. В. Козлова, Т. В. Зикратова // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – Т. 5, № 87. – С. 149–154.

20. Зикратов, И. А. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением / И. А. Зикратов, Т. В. Зикратова, И. С. Лебедев // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – Т. 2, № 90. – Р. 47–52.

21. Коваль, Е. Н. Общая модель безопасности робототехнических систем / Коваль Е. Н., Лебедев И. С. // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – Т. 4, № 86. – С. 153–154.

22. Викснин, И. И. Модели и методы обнаружения нарушений целостности информации в группах беспилотных транспортных средств : дис. ... канд. техн. наук / И. И. Викснин. – Санкт-Петербург : Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2018.

23. Dorigo, M. Ant System: Optimization by a Colony of Cooperating Agents / M. Dorigo, V. Maniezzo, A. Colorni // IEEE Transactions on Systems, Man, and Cybernetics. Part B. – 1996. – Vol. 26, № 1. – P. 29–41.

24. Poli, R. Particle swarm optimization / R. Poli, J. Kennedy, T. Blackwell // Swarm Intelligence. – 2007. – Vol. 1, № 1. – P. 33–57.

25. Pham, D. The Bees Algorithm Technical Note / D. Pham, A. Ghanbarzadeh, E. Koç, S. Otri, S. Rahim, M. Zaidi // Manufacturing Engineering Centre. – Cardiff University, UK, 2005. – P. 1–57.

26. Зикратов, И. А. Модель безопасности мобильных мультиагентных робототехнических систем с коллективным управлением / И. А. Зикратов, И. И. Викснин, Т. В. Зикратова, А. А. Шлыков, Д. И. Медведков // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17, № 3. – С. 439–449.

27. Зикратов, И. А. Совершенствование police office model для обеспечения безопасности роевых робототехнических систем / И. А. Зикратов, А. В. Гуртов, Т. В. Зикратова, Е. В. Козлова // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – Т. 5, № 93. – С. 99–109.

28. Петренко, В. И. Анализ технологий обеспечения информационной безопасности мультиагентных робототехнических систем с роевым интеллектом / В. И. Петренко, Ф. Б. Тебуева, М. М. Гурчинский, С. С. Рябцев // Наука и бизнес: пути развития. – 2020. – Т. 4, № 106. – С. 96–99.

29. Петренко, В. И. Метод достижения консенсуса для роя роботов относительно наиболее часто встречающейся особенности окружающей среды на основе технологии блокчейн / В. И. Петренко, Ф. Б. Тебуева, С. С. Рябцев, И. В. Стручков // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации : сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь, 30 ноября 2020 года. – Ставрополь, 2020. – С. 249–254.

30. Tebueva, F. A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems / F. Tebueva, S. Ryabtsev, I. Struchkov // International scientific forum on computer and energy Sciences (WFCES 2021). – 2021. – P. – 1–8.

31. Довгаль, В. А. Анализ уязвимостей и угроз безопасности роя дронов с поддержкой wi-fi, противостоящего атакам злоумышленников / В. А. Довгаль, Д. В. Довгаль // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – Т. 3, № 266. – С. 67–73.

32. Басан, А. С. Анализ и разработка средств обеспечения безопасности для систем группового управления автономными мобильными роботами / А. С. Басан, Е. С. Басан, О. Б. Макаревич // Вопросы кибербезопасности. – 2017. – Т. 5, № 24. – С. 42–49.

33. Юрьева, Р. А. Метод и модель выявления и идентификации угроз нарушения информационной безопасности мультиагентных робототехнических систем : дис. ... канд. техн. наук / Р. А. Юрьева. – Санкт-Петербург : Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2017.

34. Chen, L. Securing emergent behaviour in swarm robotics / L. Chen, S.-L. Ng // Journal of Information Security and Applications. – 2021. – Vol. 64. – P. 1–17.

35. Sargeant, I. Review of Potential Attacks on Robotic Swarms / I. Sargeant, A. Tomlinson // Lecture Notes in Networks and Systems. – 2018. – P. 628–646.

36. Sandoval, S. Cyber Security Assessment of the Robot Operating System 2 for Aerial Networks / S. Sandoval, P. Thulasiraman // 2019 IEEE International Systems Conference (SysCon). – 2019. – P. 1–8.

37. Gazebo // Gazebo. – Режим доступа: http://gazebosim.org/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 17.02.2022).

38. ROS2 // Github. – Режим доступа: https://github.com/ros2/ros2/wiki/DDS-and-ROS-middlewareimplementations/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 17.02.2022).

39. Madhu, A. Positioning Optimization of Drones using IMU and Securing UAV Communication by implementing Hybrid Cryptosystem / A. Madhu, M. B. Harshith, Prajeesha // 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI). – 2021. – P. 681–686.

40. Khanh, T. D. TRA: Effective Authentication Mechanism for Swarms of Unmanned Aerial Vehicles / T. D. Khanh, I. Komarov, L. D. Don, R. Iureva, S. Chuprov // 2020 IEEE Symposium Series on Computational Intelligence (SSCI). – 2020. – P. 1852–1858.

41. Chen, A. ToAM: a task-oriented authentication model for UAVs based on blockchain / A. Chen, K. Peng, Z. Sha // EURASIP Journal on Wireless Communications and Networking. – 2021. – Vol. 2021, № 1. – P. 1–16.

42. Мариненков, Е. Д. Анализ защищенности информационного взаимодействия группы беспилотных летательных аппаратов / Е. Д. Мариненков, И. И. Викснин, Ю. А. Жукова, М. А. Усова // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18, № 5. – С. 817–825.

43. Sánchez-Ibáñez, J. R. Path Planning for Autonomous Mobile Robots: A Review / J. R. Sánchez-Ibáñez, C. J. Pérez-del-Pulgar, A. García-Cerezo // Sensors. – 2021. – Vol. 21, № 7898. – P. 1–29.

**References**

1. Zakiev, A., Tsoy, T., Magid, E. Swarm Robotics: Remarks on Terminology and Classification. *Interactive Collaborative Robotics (ICR 2018)*, 2018, pp. 291–300.

2. Kalyaev, I. A., Gaiduk, A. R., Kapustyan, S. G. *Modeli i algoritmy kollektivnogo upravleniya v gruppakh robotov* [Models and Algorithms for Collective Control in Groups of Robots]. Moscow, FIZMATLIT Publ., 2009.

3. Petrenko, V. I., Tebueva, F. B., Gurchinsky, M. M., Antonov, V. O., Pavlov, A. S. Prognoznaya otsenka traektorii ruki operatora dlya resheniya obratnoy zadachi dinamiki pri kopiruyushhem upravlenii [Predictive assessment of operator's hand trajectory with the copying type of control for solution of the inverse dynamic problem]. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2019, vol. 18, no. 1, pp. 123–147.

4. Pavlov, A. S. Metodika planirovaniya traektorii dvizheniya gruppy mobilnykh robotov v neizvestnoy zamknutoy srede s prepyatstviyami [Methodology for Planning the Trajectory of a Group of Mobile Robots in Unknown Closed Environment with Obstacles]. *Sistemy upravleniya, svyazi i bezopasnosti* [Systems of Control, Communication and Security], 2021, no. 3, pp. 38–59.

5. Kovács, G., Yussupova, N., Rizvanov, D. Resource management simulation using multi-agent approach and semantic constraints. *Pollack Period*, 2017, vol. 12, no. 1, pp. 45–48.

6. Pshikhopov, V. K., Medvedev, M. Yu. Gruppovoe upravlenie dvizheniem mobilnykh robotov v neopredelennoy srede s ispolzovaniem neustoychivykh rezhimov [Group Control of Autonomous Robots Motion in Uncertain Environment via Unstable Modes]. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2018, vol. 60, no. 5, pp. 39–63.

7. Anchekov, M. I., Krivenko, M. P. Kompyuternaya model vozniknoveniya kollektivnogo povedeniya robotov [Computer model of the emergence of collective robot behavior]. *Izvestiya Kabardino-Balkarskogo nauchnogo tsentra RAN* [Proceedings of the Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences], 2019, no. 6, pp. 21–26.

8. Alonso-Mora, J., Baker, S., Rus, D. Multi-robot formation control and object transport in dynamic environments via constrained optimization. *The International Journal of Robotics Research*, 2017, vol. 36, no. 9, pp. 1000–1021.

9. Dai, W., Lu, H., Xiao, J., Zeng, Z., Zheng, Z. Multi-robot dynamic task allocation for exploration and destruction. *Journal of Intelligent and Robotic Systems: Theory and Applications*, vol. 98, no. 2, pp. 455–479.

10. Dutta, A., Ufimtsev, V., Asaithambi, A. Correlation Clustering Based Coalition Formation For Multi-Robot Task Allocation. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 2019, pp. 906–913.

11. Tkach, I., Jevtić, A., Nof, S. Y., Edan, Y. A Modified Distributed Bees Algorithm for Multi-Sensor Task Allocation.

*Sensors,* 2018, vol. 18, p. 759.

12. Saravanan, S., Ramanathan, K. C., Ramya, M. M., Janardhanan, M. N. Review on state-of-the-art dynamic task allocation strategies for multiple-robot systems. *Industrial Robot*, 2020, vol. 47, no. 6, pp. 929–942.

13. Khamis, A., Hussein, A., Elmogy, A. Multi-robot Task Allocation: A Review of the State-of-the-Art. *Cooperative Robots and Sensor Networks*, 2015, pp. 31–51.

14. Dorigo, M., Birattari, M. Swarm intelligence. *Scholarpedia*, 2007, vol. 9, no. 2, p. 1462.

15. Sujit, P. B., Kingston, D., Beard, R. Cooperative forest fire monitoring using multiple UAVs. *46th IEEE Conference on Decision and Control, 10–11 December 2007, New Orleans, Louisiana USA*, 2007, pp. 4875–4880.

16. Chzhaj, M. Mnogoagentnaya robototekhnicheskaya sistema spaseniya pri zemletryaseniyakh [Multi-agent robotic earthquake rescue system]. Moscow, Bauman Moscow State Technical University, 2019. 158 p.

17. Petrenko, V., Tebueva, F., Pavlov, A., Antonov, V., Kochanov, M. Path Planning Method in the Formation of the Configuration of a Multifunctional Modular Robot Using a Swarm Control Strategy. *Proceedings of the 7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2019)*, 2019, pp. 165–170.

18. Higgins, F., Tomlinson, A., Martin, K. M. Threats to the swarm: Security considerations for swarm robotics. *International Journal on Advances in Security*, 2009, vol. 2, no. 2, pp. 288–297.

19. Zikratov, I. A., Kozlova, E. V., Zikratov, T. B. Analiz uyazvimostey robototehnicheskikh kompleksov s roevym intellektom [Analysis of vulnerabilities of robotic systems with swarm intelligence]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2013, vol. 5, no. 87, pp. 149–154.

20. Zikratov, I. A., Zikratov, T. B., Lebedev, I. S. Doveritelnaya model informatsionnoy bezopasnosti multiagentnykh robototehnicheskikh sistem s detsentralizovannym upravleniem [Trust model for information security of multi-agent robotic systems with a decentralized management]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2014, vol. 2, no. 90, pp. 47–52.

21. Koval, E. N., Lebedev, I. S. Obshchaya model bezopasnosti robototehnicheskikh sistem [General safety model for robotic systems]. *Nauchno-tehnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2013, vol. 4, no. 86, pp. 153–154.

22. Viksnin, I. I. *Modeli i metody obnaruzheniya narusheniy tselostnosti informatsii v gruppakh bespilotnykh transportnykh sredstv* [Models and methods for detecting information integrity violations in groups of unmanned vehicles]. St. Petersburg, ITMO University, 2018. 207 p.

23. Dorigo, M., Maniezzo, V., Colorni, A. Ant System: Optimization by a Colony of Cooperating Agents. *IEEE Transactions on Systems, Man, and Cybernetics. Part B*, 1996, vol. 26, no. 1, pp. 29–41.

24. Poli, R., Kennedy, J., Blackwell, T. Particle swarm optimization. *Swarm Intelligence*, 2007, vol. 1, no. 1, pp. 33–57.

25. Pham, D., Ghanbarzadeh, A., Koç, E., Otri, S., Rahim, S., Zaidi, M. The Bees Algorithm Technical Note. *Manufacturing Engineering Centre*. Cardiff University, UK, 2005, pp. 1–57.

26. Zikratov, I. A., Viksnin, I. I., Zikratov, T. B., Shlykova, A. A., Medvedkov, D. I. Model bezopasnosti mobilnykh multiagentnykh robototekhnicheskikh sistem s kollektivnym upravleniem [Security model of mobile multi-agent robotic systems with collective management]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2017, no. 3, pp. 439–449.

27. Zikratov, I. A., Gurtov, A. V., Zikratova, T. V., Kozlova, E. V. Sovershenstvovanie police office model dlya obespecheniya bezopasnosti roevykh robototekhnicheskikh sistem [Improving the police office model to ensure the safety of swarm robotic systems]. *Nauchno-tehnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2014, vol. 5, no. 93, pp. 99–109.

28. Petrenko, V. I., Tebueva, F. B., Gurchinsky, M. M., Ryabtsev, S. S. Analiz tekhnologiy obespecheniya informatsionnoy bezopasnosti multiagentnykh robototekhnicheskikh sistem s roevym intellektom [Analysis of information security technologies for multi-agent robotic systems with swarm intelligence]. *Nauka i biznes: puti razvitiya* [Science and Business: Development Ways], 2020, vol. 4, no. 106, pp. 96–99.

29. Petrenko, V. I., Tebueva, F. B., Ryabtsev, S. S., Struchkov, I. V. Metod dostizheniya konsensusa dlya roya robotov otnositelno naibolee chasto vstrechayushcheysya osobennosti okruzhayushhey sredy na osnove tekhnologii blokcheyn [A method for achieving consensus for a swarm of robots on the most frequently occurring feature of the environment based on blockchain technology]. *Fundamentalnye problemy informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii : sbornik dokladov II Vserossiyskoy nauchnoy konferentsii (s priglasheniem zarubezhnykh uchenykh)* [Fundamental problems of information security in the context of digital transformation : proceedings of the II All-Russian Scientific Conference (with the invitation of foreign scientists)], Stavropol, 2020, pp. 249–254.

30. Tebueva, F., Ryabtsev, S., Struchkov, I. A method of counteracting Byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems. *International scientific forum on computer and energy Sciences (WFCES 2021)*, 2021, pp. 1–8.

31. Dovgal, V. A., Dovgal, D. V. Analiz uyazvimostey i ugroz bezopasnosti roya dronov s podderzhkoy wi-fi, protivostoyashchego atakam zloumyshlennikov [Analysis of vulnerabilities and security threats of a swarm of wi-fi-enabled drones that resist attacks by intruders]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki* [Proceedings of Adygea State University. Series 4: Natural-mathematical and technical sciences], 2020, vol. 3, no. 266, pp. 67–73.

32. Basan, A. S., Basan, E. S., Makarevich, O. B. Analiz i razrabotka sredstv obespecheniya bezopasnosti dlya sistem gruppovogo upravleniya avtonomnymi mobilnymi robotami [Analisys of ways to secure group control for autonomus mobile robots]. *Voprosy kiberbezopasnosti* [Cyber security issues], 2017, vol. 5, no. 24, pp. 42–49.

33. Urieva, R. A. *Metod i model vyyavleniya i identifikatsii ugroz narusheniya informatsionnoy bezopasnosti multiagentnykh robototehnicheskikh sistem* [Method and model for detecting and identifying threats to information security violations of multi-agent robotic systems]. St. Petersburg, ITMO University, 2017. 132 p.

34. Chen, L., Ng, S.-L. Securing emergent behaviour in swarm robotics. *Journal of Information Security and Applications,* 2021, vol. 64, pp. 1–17.

35. Sargeant, I., Tomlinson, A. Review of Potential Attacks on Robotic Swarms. *Lecture Notes in Networks and Systems*, 2018, pp. 628–646.

36. Sandoval, S., Thulasiraman, P. Cyber Security Assessment of the Robot Operating System 2 for Aerial Networks.

*2019 IEEE International Systems Conference (SysCon)*, 2019, pp. 1–8.

37. Gazebo. Available at: http://gazebosim.org/ (accessed 17.02.2022).

38. ROS2. Available at: https://github.com/ros2/ros2/wiki/DDS-and-ROS-middlewareimplementations/ (accessed 17.02.2022).

39. Madhu, A., Harshith, M. B., Prajeesha. Positioning Optimization of Drones using IMU and Securing UAV Communication by implementing Hybrid Cryptosystem. *5th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2021, pp. 681–686.

40. Khanh, T. D., Komarov, I., Don, L. D., Iureva, R., Chuprov, S. TRA: Effective Authentication Mechanism for Swarms of Unmanned Aerial Vehicles. *IEEE Symposium Series on Computational Intelligence (SSCI)*, 2020, pp. 1852–1858

41. Chen, A., Peng, K., Sha, Z. ToAM: a task-oriented authentication model for UAVs based on blockchain. *EURASIP Journal on Wireless Communications and Networking*, 2021, vol. 2021, no. 1, pp. 1–16.

42. Marinenkov, E. D., Viksnin, I. I., Zhukova, Yu. A., Usova, M. A. Analiz zashchishhennosti informatsionnogo vzaimodeystviya gruppy bespilotnykh letatelnykh apparatov [Security analysis of information interaction of a group of unmanned aerial vehicles]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2018, vol. 18, no. 5, pp. 817–825.

43. Sánchez-Ibáñez, J. R., Pérez-del-Pulgar, C. J., García-Cerezo, A. Path Planning for Autonomous Mobile Robots: A Review. *Sensors*, 2021, vol. 21, no. 7898, pp. 1–29.

УДК 004.056

## ПРОБЛЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ СОЗДАНИИ ЦИФРОВОГО ДВОЙНИКА ДИСЦИПЛИНЫ

*Статья поступила в редакцию 01.05.2022, в окончательном варианте – 10.05.2022.*

***Попов Алексей Михайлович***, Сибирский государственный университет науки и технологий имени М.Ф. Решетнева, 660037, Российская Федерация, г. Красноярск, пр. им. газеты «Красноярский рабочий», 31,

доктор физико-математических наук, профессор, директор Института информатики и телекоммуникаций, ORCID: 0000-0002-6011-9375, e-mail: vm_popov@sibsau.ru

***Золотарев Вячеслав Владимирович***, Сибирский государственный университет науки и технологий имени М.Ф. Решетнева, 660037, Российская Федерация, г. Красноярск, пр. им. газеты «Красноярский рабочий», 31,

кандидат технических наук, доцент, заведующий кафедрой безопасности информационных технологий, ORCID: 0000-0002-8054-8564, e-mail: zolotorev@sibsau.ru

***Кунц Екатерина Юрьевна***, Сибирский государственный университет телекоммуникаций и информатики, 630102, Российская Федерация, г. Новосибирск, ул. Кирова, 86,

начальник отдела дистанционного обучения, ORCID: 0000-0003-3903-4737, e-mail: kuntsey@sibguti.ru

При формировании образовательного содержания дисциплин наблюдается проблема управления информационной безопасностью больших объемов накапливаемых данных. Особенно это характерно для дисциплин, предполагающих использование данных цифрового следа, виртуализации, конфигурационных файлов как средств подготовки среды развертывания образовательного контента. В случае обучения информационной безопасности такой оперативной информацией является цифровой след, формируемый на уровне лабораторных работ. В работе показаны некоторые схемы управления информационной безопасностью при использовании цифрового следа и виртуальных лабораторий на уровне формирования цифрового двойника дисциплины. Использование предлагаемых схем может быть полезно для создания индивидуальных образовательных траекторий обучающихся на основе оперативных данных, образовательного контента виртуальных лабораторий, накопления и использования опыта обучения.

**Ключевые слова:** цифровой двойник, цифровой след, индивидуальная траектория, рабочая программа, сбор цифрового следа, образовательный процесс, информационная инфраструктура, информационно-образовательная среда, виртуальная лаборатория

## INFORMATION SECURITY MANAGEMENT PROBLEM FOR CREATING A DISCIPLINE DIGITAL TWIN

*The article was received by the editorial board on 01.05.2022, in the final version – 10.05.2022.*

***Popov Alexey M.***, Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,

Doct. Sci. (Physics and Mathematics), Professor, Director of the Institute of Informatics and Telecommunications, ORCID: 0000-0002-6011-9375, e-mail: vm_popov@sibsau.ru

***Zolotarev Vyacheslav V.***, Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, Head of Information Technologies Security Department, ORCID: 0000-0002-8054-8564, e-mail: zolotorev@sibsau.ru

***Kunts Ekaterina Yu.***, Siberian State University of Telecommunications and Informatics, 86 Kirov St., Novosibirsk, 630102, Russian Federation,

Head of Distance Learning Department, ORCID: 0000-0003-3903-4737, e-mail: kuntsey@sibguti.ru