Инженерный вестник Дона, №11 (2022)
ivdon.ru/ru/magazine/archive/n11y2022/8031

Метод выявления и противодействия распространению вредоносной информации в роевых робототехнических системах в процессе распределения задач

А.С. Павлов[1], *В.И. Петренко*[1], *Ф.Б. Тебуева*[1], *В.В. Копытов*[1], *Е.Н. Тищенко*[2]

[1]*Северо-Кавказский федеральный университет, Ставрополь*
[2]*Ростовский государственный экономический университет (РИНХ), Ростов-на-Дону*

Аннотация: Рост популярности использования групповой робототехники, в том числе роевых робототехнических систем (РРТС), актуализирует вопросы обеспечения информационной безопасности. Известные подходы к выявлению вредоносного поведения агентов или вредоносной информации не учитывают свойства масштабируемости и децентрализации РРТС, что не позволяет обеспечить целостность информации, циркулирующей по каналам связи внутри РРТС. В свою очередь, распространение вредоносной информации в процессе распределения задач между агентами РРТС изначально снижает эффективность выполнения этих задач, то есть осуществляется атака на самый первый и наиболее ответственный этап функционирования системы. Целью настоящей работы является повышение эффективности функционирования агентов РРТС при наличии вредоносных агентов за счет разработки метода выявления и противодействия распространению вредоносной информации. К элементам научной новизны данной работы относится следующее. В рамках решения поставленной задачи предложены ряд специфических критериев, учитывающих особенности распределения задач в РРТС, а также классификатор на основе искусственной нейронной сети для выявления вредоносной информации. Для повышения точности выявления и противодействия распространению вредоносной информации в РРТС предложена модификация механизма репутации. Отличительной особенностью модификации является не только формирование показателя истинности информации сообщения в процессе распределения задач, но и оценка влияния вредоносных агентов на процесс формирования этого показателя. Представленное решение реализовано в виде программного обеспечения на языке программирования Python, которое может быть использовано при моделировании децентрализованных систем управления РРТС.
Ключевые слова: роевые робототехнические системы, распределение задач, искусственные нейронные сети, механизм доверия и репутации.

Введение

В настоящее время одним из наиболее значимых барьеров к широкому использованию роевых робототехнических систем (РРТС) является наличие уязвимостей с точки зрения информационной безопасности (ИБ) [1]. В ряде исследований отечественных и зарубежных авторов рассматривается вопрос

ИБ в РРТС. Так, в работе [2] представлен подробный обзор актуальных вопросов ИБ в РРТС, в работе [3] выполнен анализ потенциальных атак на РРТС, а в работе [4] приведен анализ и исследование основных угроз актуальных для различных принципов, методов и особенностей группового управления РРТС.

К основным механизмам атак на РРТС, формирующим угрозы, относят [5]:

– атаки на каналы связи;

– сложность идентификации и аутентификации агентов в системе;

– внедрение в систему «вредоносных» роботов.

Настоящее исследование направлено непосредственно на последний класс атак, когда нарушитель (вредоносный агент или робототехническое устройство в неисправном состоянии) навязывает собственную альтернативу, не соответствующую реальности, с целью уменьшения эффективности выполнения задач агентами РРТС, вплоть до невозможности завершения актуального списка задач. Например, в процессе распределения задач вредоносные агенты могут выбирать такие задачи, которые требует наибольшее количество затрат электроэнергии от агента. Доверенные агенты РРТС могут выявить вредоносного агента не на стадии распределения задач, а только в процессе их выполнения. В результате этого возможна такая ситуация, когда ни у одного из доверенных агентов РРТС не останется заряда аккумуляторной батареи для выполнения задач, закрепленных за вредоносными агентами, что делает невозможным достижение цели функционирования РРТС.

Согласно проведенному обзору литературы по тематике исследования, описанная проблема может быть решена путем внедрения в процесс взаимодействия агентов процедуры коллективного принятия решения с использованием алгоритмов достижения консенсуса. Наиболее

распространенным вариантом реализации этого подхода является использование технологий распределенного реестра и блокчейна. Так, в работе [6] представлена концепция информационной безопасности киберфизических систем, в основу которой положен «роевый» принцип взаимодействия агентов системы. В качестве инструментальной базы предложенной концепции авторы работы видят технологию распределенного реестра и алгоритм достижения консенсуса. Авторы работы [7] рассмотрели существующие подходы реализации информационного обмена между агентами, а также провели краткий анализ особенностей информационного взаимодействия при использовании различных стратегий управления группой роботов. Однако, оба исследования носят преимущественно теоретический характер без явных практических рекомендаций. С другой стороны, в работе [8] представлен программный интерфейс ARGoS-блокчейн, реализованный с помощью смарт-контрактов на основе блокчейна в качестве «мета-контроллеров» агентов РРТС. Представленное решение использовано для сравнения протоколов достижения консенсуса, используемых в роевой робототехнике, с точки зрения их устойчивости к воздействию византийских роботов. Согласно полученным результатам, использование технологии блокчейн позволяет обеспечить безопасное взаимодействие агентов в условиях наличия византийских роботов или неисправных агентов. Однако, алгоритмы достижения консенсуса имеют вычислительную сложность, поэтому возможность применения технологии блокчейн в РРТС непосредственно зависит от характеристик вычислительных платформ робототехнических устройств, используемых в качестве агентов РРТС.

В литературе встречаются методы обеспечения информационной безопасности РРТС, которые направлены на анализ поведения агентов в процессе их функционирования. Например, авторы работы [9] представили

фреймворк, направленный на выявление нарушителя в РРТС. Это решение базируется на анализе поведения агентов в процессе распределения задач. Так, на основе использования метрики расстояния Кульбака-Лейблера рассчитываются идеальное вероятностные распределение задач (для легитимных агентов) и отклоняемое распределение (для вредоносных агентов). На основе сопоставления этих распределений внешний наблюдатель достаточно эффективно может определить наличие нарушителя в РРТС. В качестве отслеживаемых параметров поведения агента могут быть приведены и физические характеристики состояния агента, например скорость, ускорение, заряд аккумуляторной батареи и т.д. [10]. Использование решений на основе поведенческого подхода обеспечивает высокую эффективность выявления нарушителей преимущественно в задачах коллективного управления РРТС [11]. Однако, рассматриваемый подход может быть применим не во всех реальных приложениях РРТС. Например, такие задачи, как наблюдение за некоторой областью, исследование местности, разведка и т.д., классифицированные в работе [12], как пространственно-распределенные задачи, требуют рассредоточения агентов на достаточно большой площади, вследствие чего агенты могут находится друг от друга на расстоянии, превышающем дальность действия бортовых сенсоров и датчиков. Это делает невозможным сбор информации о поведении агентов и своевременном выявлении нарушителей. Помимо этого, существенную сложность при использовании подхода на основе анализа поведения агентов вызывает задача формирования эталонного поведения агента. Решение этой задачи не является универсальным, так как каждый отдельно взятый сценарий практического применения РРТС требует формирования индивидуальной модели эталонного поведения агентов РРТС.

Другим подходом к анализу поведения агентов РРТС является использование доверительной модели безопасности [5]. В основе этого

подхода используется метрика для расчета доверия и репутации агентов, которая пересчитывается в каждый дискретный момент времени на основе наблюдений всех агентов РРТС. Авторы работы [13] предложили метод противодействия скрытому деструктивному информационному воздействию в группе беспилотных летательных аппаратов. Метод сочетает в себе модель полицейских участков для аутентификации агентов, криптосистему с открытым ключом для шифрования сообщений и репутационный механизм для выявления нарушителя информационной безопасности. Основная идея работы заключается в анализе семантической целостности информации путем сопоставления информации, известной агенту, и информации, получаемой от других агентов. На основе результатов сопоставления корректируется показатели доверия к каждому из агентов системы. Результаты имитационного моделирования, проведенного авторами, подтверждает эффективность метода. Однако, стоит отметить, что применение этого метода будет эффективным в сценариях коллективного управления РРТС, а применимость к сценариям выполнения пространственно-распределенных задач требует дополнительных исследований. Помимо этого, наличие полицейских участков подразумевает гетерогенную систему вместо гомогенной, что не согласуется с концепцией проектирования РРТС.

Помимо рассмотренных выше работ в области робототехники, можно выделить и методы, направленные на обеспечение информационной безопасности, в смежных областях науки и техники. Так, в работе [14] предложен метод авторизации на основе разложения чисел на простые сомножители. Преимуществами этого метода являются простота реализации и низкая вычислительная сложность, так как в основе лежат простейшие арифметические операции. Однако, как отмечают авторы работы, самым главным ограничением является применимость метода только к

малочисленным системам. Это обусловлено тем, что используемые в работе дескрипторы (произведение разных простых чисел), описывающие систему и права доступа агентов, имеют размерность, не превышающую 64 бита, что накладывает ограничение на количество агентов системы – не более 15. Увеличение размерности дескрипторов приедет к усложнению реализации метода и, как следствие, увеличению вычислительной сложности, что не всегда допустимо для РРТС. В работе [15] представлена модель авторизации внешних средств защиты автоматизированных систем управления технологическими процессами на базе Интернета вещей, в которой обеспечение контроля доступа устройств предлагается реализовать на основе на основе атрибутного шифрования (англ. Attribute-Based Encryption, ABE) [16]. К недостаткам этой модели можно отнести наличие доверенного центра (сервера), наличие которого исключается в сценариях пространственно-распределенных задач.

Большая часть рассмотренных решений предполагают выявление нарушителя только после некоторого времени, в течение которого агенты РРТС будут собирать информацию о соседних агентах. Однако, в сценариях пространственно-распределенных задач одним из важнейших этапов является самый первый – распределение задач. Для решения этой проблемы ранее коллективом авторов был предложен расширенный протокол аутентификации агентов РРТС на основе схемы идентификации Фейга-Фиата-Шамира с нулевым разглашением знаний, позволяющий избежать «лавинного эффекта» актов аутентификации между агентами при значительном увеличении их численности. Для этого был разработан набор продукционных правил, представленных в виде дерева решений, позволяющих путем информационного обмена агентов с использованием распределенного реестра выполнить делегированную аутентификацию агентов, которые ранее прошли успешно эту процедуру. С одной стороны,

использование этого протокола позволяет агентам «переключаться» между наиболее приоритетными задачами и взаимодействовать с другими агентами без повторной аутентификации, находясь в области видимости по меньшей мере одного соседнего агента. А это, в свою очередь, позволяет уменьшить время выполнения таких заданий, которые требуют увеличения численности агентов, за счет уменьшения времени, необходимого для аутентификации новых агентов. С другой стороны, можно допустить, что вредоносный агент смог угадать ответы, чтобы подтвердить знание секрета и успешно прошел аутентификацию. Либо агент, действительно знающий секрет, может быть перепрограммирован на то, чтобы «поручаться» за любого агента, в том числе не прошедшего аутентификацию ранее. В результате этого вредоносный агент не только получает возможность для модификации или подмены информации, циркулирующей по каналам связи внутри РРТС, когда вредоносный агент выступает ретранслятором сообщений.

Таким образом, отличие настоящей работы заключается в том, что исследование направлено на минимизацию времени, необходимого для выявления вредоносного агента на самом первом этапе выполнения пространственно-распределенных задач. Исходя из этого, в рамках решения указанной проблемы в настоящей работе предлагается разработка метода авторизации агентов РРТС в процессе их взаимодействия. Под авторизацией в данной работе понимается предоставление определенному агенту права на участие в информационном взаимодействии системы, а также процесс проверки такого права при попытке инициализации информационного взаимодействия.

Постановка задачи

Пусть имеется РРТС численностью n агентов r_i, $R=r_1, \ldots, r_n$; O – множество, содержащее m элементарных задач (далее просто «задач»), $O=o_1, \ldots, o_m$; Y – множество выходных параметров (количество выполненных задач

агентами РРТС); Z – множество внутренних параметров РРТС (текущая позиция, заряд батареи, скорость, ускорение и т.д.); E – множество параметров среды (условий функционирования), $E=e_1, \ldots, e_M$, где e_j – изменяющиеся параметры среды, $j=1, \ldots, M$; Q – множество показателей качества функционирования РРТС; $q_1, \ldots, q_k$ – контролируемые показатели качества функционирования РРТС. Основная цель функционирования РРТС заключается в оптимальном распределении задач и их выполнении за минимальное время. В данной работе агенты РРТС рассматриваются как абстрактные объекты без учета их кинематических или динамических параметров. Это затрудняет расчет времени выполнения последней задачи агентами РРТС, поэтому в качестве основного показателя качества функционирования РРТС предлагается рассматривать максимальную длину пути, пройденную агентами в процессе выполнения задач. Поведение неисправных или вредоносных агентов заключается в выборе задачи / задач на этапе их распределения, оповещения других агентов РРТС о своем выборе и прекращения выполнения выбранных задач. Таким образом, доверенные агенты РРТС, обнаружив невыполненные задачи, будут вынуждены выполнить дополнительные задачи, что увеличит общее пройденное расстояние и, как следствие, время выполнения последней задачи.

Целью настоящей работы является повышение защищенности информационной безопасности роевых робототехнических систем при наличии внедренных агентов с неисправным или вредоносным поведением. Под защищенностью информационной безопасности РРТС понимается обеспечение таких показателей качества функционирования РРТС, которые соответствуют идеальным условиям, то есть отсутствию неисправных или вредоносных агентов в системе.

Содержательная постановка научной задачи исследования можно сформулировать следующим образом. Разработать метод F повышения

качества/эффективности функционирования РРТС R по показателям q_1, …, q_k в диапазоне значений входных и выходных параметров (O,Y) системы, за счет варьирования значений внутренних параметров Z, в условиях изменяющихся параметров среды e_1, …, e_M, ($e_j \in E$, $j=1$, …, M).

Формальная постановка научной задачи: найти метод F такой, что

$$F:\langle R,O,Y,Z,E,Q\rangle \to \{\Delta q_1,...,\Delta q_k\} \mid \forall \Delta q_i > 0, q_i \in Q, i=1,...,k, \quad (1)$$

при этом: $\Delta q_i = q_i^{\text{п}} - q_i^{\text{д}}, i=1,...,k,$ где индекс «д» значит «до использования метода», индекс «п» – «после использования метода».

Методы и материалы

Критерии выявления вредоносной информации в процессе распределения задач между агентами РРТС

Наиболее близким аналогом для решения задачи настоящего исследования является работа [10]. Однако, в РРТС наблюдается избыточность пакетов данных в процессе коммуникации, так как агенты постоянно ретранслируют друг другу множество сообщений при распределении задач. Поэтому критерии активности сетевого узла, общего трафика сети и остаточной энергии могут быть недостаточно показательны для выявления вредоносных агентов. Исходя из особенностей процесса распределения задач, в РРТС предлагается использовать следующие критерии:

– процент закрепленных за агентом задач x_c относительно общего количества задач m, то есть:

$$x_c = \frac{|O_i|}{m}, \quad (2)$$

где $O_i \in O$ – множество задач, закрепленных за агентом r_i в текущий момент времени;

– текущий заряд аккумуляторной батареи x_e, выраженный в процентном отношении к максимально возможному заряду батареи. Полный заряд аккумуляторной батареи x_e^{max} не может превышать максимальную емкость батареи. А так как РРТС по определению является гомогенной [17], то значение x_e^{max} будет одинаковым для всех агентов. В процессе функционирования каждый агент должен оставлять определенный процент заряда батареи для возвращения на базу из точки, соответствующей последней выполненной задачи. Обозначим это значение, как x_e^{min}. Таким образом, доверительный интервал заряда аккумуляторной батареи x_e будет равен $x_e \in \left[x_e^{min}, x_e^{max} \right]$;

– расчетная трудоемкость выполнения закрепленных за агентом задач x_l, которая выражается процентным отношением затрат энергии на выполнение задач к текущему заряду аккумуляторной батареи x_e,

$$x_l = \frac{W\left(O_i\right)}{x_e},, \tag{3}$$

где $W(O_i)$ – функция, описывающая ориентировочный расход энергии в зависимости от длины пути, пройденной в результате выполнения задач. Для реализации этой функции могут быть использованы методы планирования пути перемещения агента или траектории его движения [18-20];

– среднее значение расстояния между задачами, которые выбирают агенты на текущей итерации распределения задач x_d:

$$x_d = \frac{\sum_{i=1}^{n} D\left(o_{j,i}, r_i\right)}{n}, \tag{4}$$

где $D\left(o_{j,i}, r_i\right)$ – функция расчета расстояния между агентом r_i и задачей $o_{j,i} \in O$, которая выбрана этим агентом на текущей итерации. Большинство

известных методов и алгоритмов распределения задач направлены на выбор задач, расположенных на минимальном расстоянии друг от друга, поэтому на каждой итерации агенты выбирают ближайшие к себе свободные задачи. Если предположить, что вредоносный агент будет выбирать задачи не согласно этому принципу, а, например, случайно, то выход за диапазон $(0, x_d]$ агента r_i в совокупности с другими критериями может означать вредоносное поведение этого агента.

Обработка значений предложенных критериев может быть осуществлена аналитически, например, на основе ряда продукционных правил. Однако, зависимости между предложенными критериями не являются полностью очевидными, поэтому, по мнению авторов работы, наиболее эффективное решение этой задачи может быть получены с помощью аппроксиматора в виде искусственной нейронной сети (ИНС).

Подготовка набора размеченных данных и обучение ИНС для выявления вредоносной информации

На вход ИНС должны быть поданы два кортежа, содержащие значения критериев $x(t) = \langle x_c, x_d, x_e, x_l \rangle$ в текущий момент времени t, а также аналогичный кортеж $x(t–1)$, значения которого соответствуют предыдущей итерации $t–1$. На выходе ИНС должна быть получена вероятность принадлежности агента к классу доверенных агентов или нарушителей, то есть должна выполняться бинарная классификация.

Подготовку набора размеченных данных для обучения ИНС предлагается осуществлять путем программной симуляции сценария атаки на РРТС в процессе распределения задач. Блок-схема программной симуляции представлена на рисунке 1.

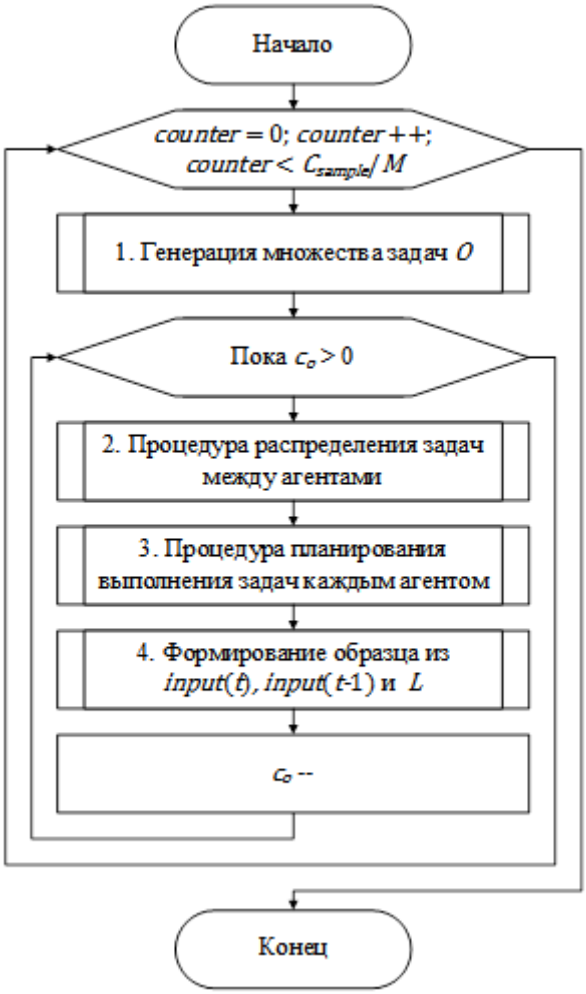

Рис. 1 – Блок-схема формирования набора размеченных данных для обучения ИНС

На первом этапе представленной блок-схемы формируется множество задач O, соответствующих реальному сценарию пространственно-распределенной задачи. Далее итерационно выполняется распределение и планирование последовательности выполнения задач агентами РРТС. Для распределения задач предлагается использовать метод на основе жадного алгоритма [21], суть которого заключается в выборе каждым агентом ближайшей свободной задачи. А выбор последующих задач выполняется путем поиска ближайшей незанятой другими агентами задачи. С учетом новых задач, закрепленных за агентом, пересчитываются значения $x(t)$ и при

необходимости выполняется нормализация данных в пределах $[0,1]$, например, с помощью сигмоидальной логистической функции:

$$f(x)=\frac{1}{1+e^{-x}}. \quad (5)$$

После этого в полученный образец добавляется метка класса L, к которой принадлежит отдельно взятый агент.

Таким образом, в результате выполнения одной итерации вложенного цикла будет получено N образцов (с учетом k образцов с вредоносными агентами), а завершение одной итерации основного цикла позволит получить M образцов. В связи с этим, для получения требуемого количества образцов C_{sample} необходимо выполнить C_{sample}/M итераций основного цикла.

В качестве ИНС предлагается использовать многослойный персептрон с тремя скрытыми слоями. Согласно описанному выше формату входных и выходных данных соответствующие слои ИНС состоят из 8 и 2 нейронов соответственно. Количество нейронов h в скрытых слоях выбирается произвольно (с учетом возможностей вычислительных платформ робототехнических устройств, которые используются в качестве агентов РРТС). В настоящей работе использовано по 64 нейрона в каждом скрытом слое.

В качестве функции активации входного слоя предлагается использовать сигмоидальной логистическую функцию (5). Так как на выходе ИНС необходимо получить вероятности принадлежности входного сигнала к одному из двух классов, то для выходного слоя целесообразно применить ступенчатую функцию активации:

$$f(x)=\begin{cases}1, x\geq z,\\ 0, x\leq z,\end{cases} \quad (6)$$

где z – пороговый параметр.

Для каждого из скрытых слоев предлагается использовать в качестве функции активации линейный выпрямитель с «утечкой» (англ. Leaky rectified linear unit, ReLU) [22], который задается выражением:

$$f(x)=\max(0, wx+b), \quad (7)$$

где w – вектор весовых коэффициентов; x – вектор входных значений, b – смещение.

Схематически структура предлагаемой ИНС представлена на рис. 2.

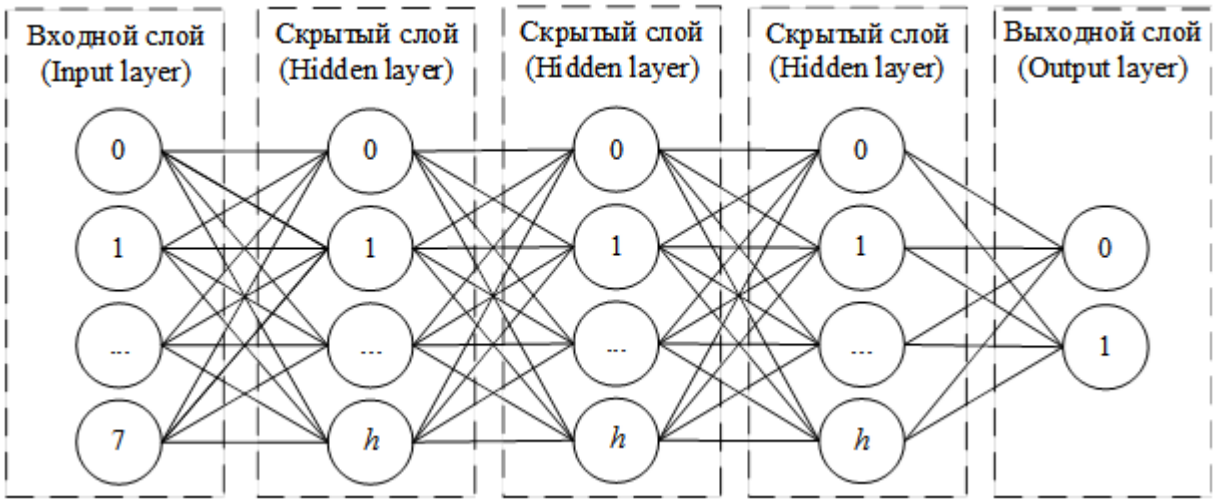

Рис. 2. – Структура ИНС

Для оценки качества классификации ИНС предлагается использовать метрику процентного соотношения количества ложных результатов к общему количеству результатов:

$$\frac{s_n}{s_p + s_n}, \quad (8)$$

где s_p обозначает количество правильных результатов, а s_n – количество ложных результатов.

Реализация механизма репутации для противодействия распространению вредоносной информации в РРТС

Результат работы классификатора μ позволит определить, является ли информация в сообщении, полученная от любого из агентов РРТС,

вредоносной. Однако, делать однозначное заключение о вредоносности агента, отправившего сообщение, на основе единичного случая не показательно, так как в реальной системе допустимы как ложные срабатывания классификатора, так и последствия воздействия случайных факторов (неисправность канала связи, помехи, случайные ошибки и т.д.). Поэтому, в настоящей работе предлагается реализация механизма репутации на основе доверительной модели информационной безопасности, предложенной в работе [5].

Пусть $s_{i,j,k}$ – результат классификации сообщения, отправленного агентом-субъектом r_i агентам-объектам $R_{v_i} \in R$ на k-той итерации процедуры распределения задач. Количество n_{v_i} агентов-объектов R_{v_i} определяется областью видимости v_i агента r_i. Получив сообщение от агента-субъекта r_i, агенты-объекты $r_j \in R_{v_i}, j = 1,...,n_{v_i}$ должны сформировать обобщенную оценку истинности информации полученного сообщения как среднее значение полученных результатов:

$$\theta_{i,k} = \frac{\sum_{j=1}^{n_{v_i}} s_{i,j,k}}{n_{v_i}}, \tag{9}$$

где $\theta_{i,k}$ будем называть далее «показателем истинности информации сообщения». При этом введем ограничение на значения этого показателя в диапазоне $[0,1]$.

Необходимо учитывать, что вредоносные агенты могут распространять не только информацию о выбранных задачах, но и целенаправленно искусственно уменьшать показатель истинности сообщений легитимных агентов. А также, наоборот, увеличивать показатель истинности сообщений от вредоносных агентов, если они осуществляют атаку сообща. Поэтому, в отличие от оригинальной работы, в настоящем исследовании предлагается

введение порогов α и β для ограничения возможности влияния вредоносных агентов на показатели истинности информации сообщения.

Обозначим T_i как показатель репутации агента-субъекта r_i и ограничим возможные значения этого показателя в диапазоне $[0,1]$. Установим значения порогов α и β равными 0,75 и 0,5 соответственно. Порог β предназначен для противодействия агентам, у которых значения показателя репутации будут меньше порогового. Таким образом, подобные агенты считаются вредоносными и полностью исключаются из процесса коммуникации с другими агентами РРТС.

Агенты со значением показателя репутации $\alpha \le T_i \le \beta$ могут участвовать в процессе распределения задач, однако, уровень доверия к ним считается сниженным и их оценки, полученные с помощью ИНС, предлагается инвертировать при каждом расчете показателя истинности сообщения $\theta_{i,k}$ от агента r_i:

$$\theta_{i,k} = \frac{\sum_{j=1}^{n_{v_i}} I(T_j)}{n_{v_i}}, \tag{10}$$

где функция $I(T_j)$ рассчитывается следующим образом:

$$I(T_j) = \begin{cases} s_{i,j,k}, T_j \ge \alpha, \\ 1 - s_{i,j,k}, \alpha \le T_j \le \beta. \end{cases} \tag{11}$$

В соответствии со скорректированным показателем истинности информации сообщения $\theta_{i,k}$ предлагается осуществлять расчет показателя репутации T_i к агенту r_i, согласно следующему выражению:

$$\begin{cases} T_i -= \gamma\theta_{i,k}, \theta_{i,k} \le \beta, \\ T_i += \gamma\theta_{i,k}, \theta_{i,k} \ge \beta, \\ T_i = 1, T_i \ge 1, \end{cases} \tag{12}$$

где γ – коэффициент нормирования.

Изменение значения γ позволяет ускорить или замедлить выявление вредоносных агентов. В настоящей работе предлагается использовать значение γ равное 0,2. Тогда при последовательном проведении атаки на каждой итерации, вредоносный агент будет выявлен и заблокирован на 4-ой итерации процесса распределения задач, а лишится возможности влиять на показатели истинности сообщений других агентов – уже на 3-ей итерации.

После вычисления показателя репутации T_i агента r_i соседние агенты передают это значение другим агентам «по цепочке». Таким образом, при динамическом изменении топологии агентов РРТС, все агенты будут осведомлены об актуальном показателе репутации T_i, который будет использоваться для формирования показателей истинности сообщений, передаваемых по каналам связи между агентами как на последующих итерациях процесса распределения задач, так и в процессе выполнения задач.

Эксперимент

Для проведения эксперимента была выполнена программная реализация метода-аналога [10] и предложенного решения на языке программирования Python. Визуализация взаимодействий агентов РРТС, а также формирование графиков для оценки эффективности рассматриваемых методов выполнены с помощью библиотеки Matplotlib. При проведении моделирования 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.

Значения количества агентов РРТС n, приведенные в таблице 1, выбраны таким образом, чтобы продемонстрировать возможность масштабирования системы, при этом количество вредоносных агентов n' будет кратным общему числу агентов системы. Значение 0 в строке

«Количество вредоносных агентов РРТС, n', ед.» можно рассматривать как идеальные условия функционирования РРТС. Значение 1 в этой же строке является статичными и приведено для наглядности, остальные значения – динамически вычисляются при изменении количества агентов.

Таблица № 1

Параметры моделирования

Наименование параметра	Значение
Общее количество агентов РРТС, n, ед.	12, 56, 100
Количество вредоносных агентов РРТС, n', ед.	0, 1, 25%, 50%
Количество задач, m, ед.	100
Количество экспериментов, ед.	100
Размер карты, м×м	60×60

Предложенная модель ИНС реализована на языке программирования Python с применением библиотек TensorFlow [23] и Keras [24]. Для обучения ИНС использовался алгоритм ADADELTA [25]. В рамках подготовки размеченных данных было сформировано 15000 образцов. Из них 80% образцов использованы в качестве обучающей выборки, а остальные 20% – в качестве тестовой.

Для оценки результатов моделирования использованы следующие показатели качества функционирования РРТС:

– количество шагов симуляции, необходимых для начала выявления вредоносных агентов, ед.;

– точность выявления вредоносных агентов, %;

– максимальная дистанция, пройденная агентами РРТС в процессе выполнения задач, м.

Первый и второй показатели определяют эффективность выявления ложной или вредоносной информации в РРТС, а последний – демонстрирует эффективность выполнения задач агентами РРТС.

В настоящей работе не вводятся ограничения на запас аккумуляторной батареи агентов РРТС, поэтому предполагается, что все задачи будут выполнены. Также не рассматриваются кинематические и динамические характеристики агентов, что затрудняет расчет времени выполнения задач агентами РРТС. Таким образом, показатель пройденной дистанции является единственным показателем качества функционирования РРТС.

На рисунке 3 представлен пример сценария функционирования 12 агентов РРТС с 3 вредоносными агентами.

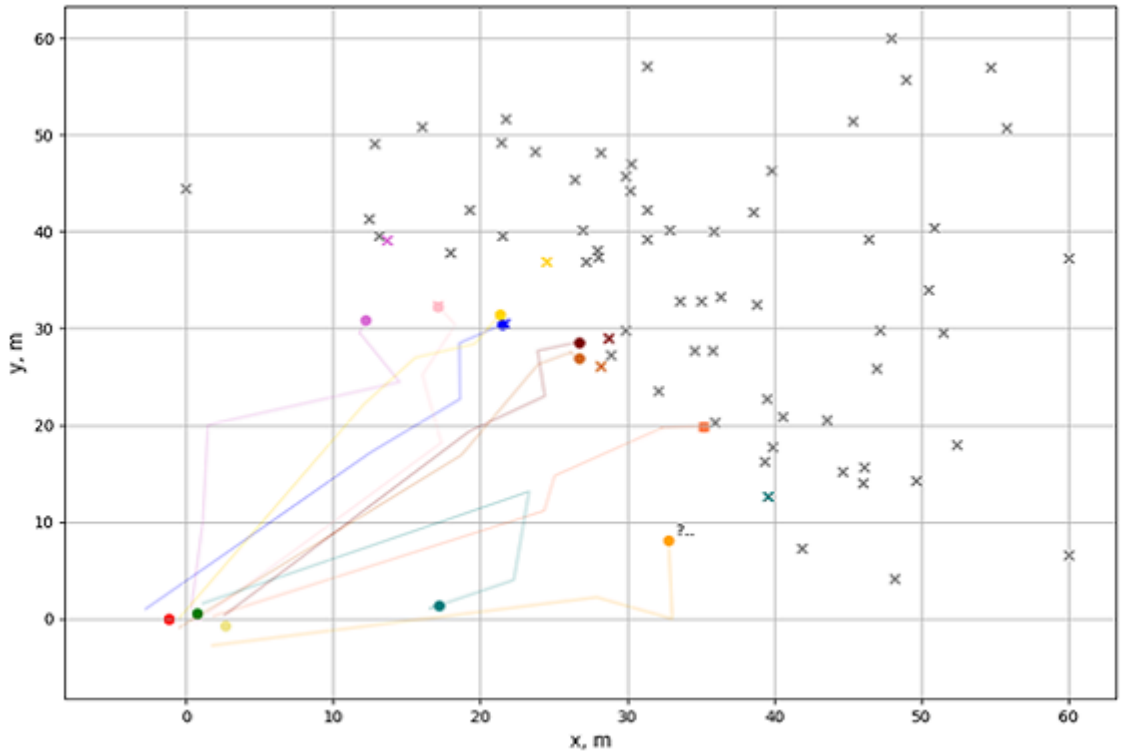

Рис. 3 – Пример выполнения задания РРТС из 12 агентов с 3 вредоносными агентами

Цветными кругами на рисунке 3 обозначены агенты РРТС, цветными крестиками – выполняемые на настоящий момент задачи. Серые крестики показывают еще не выполненные задачи. Полупрозрачные цветные ломаные

линии показывают путь, который прошли каждый из агентов в процессе выполнения задач. Как показано на рисунке, вредоносные агенты, помеченные красным, желтым и зеленым цветами, остаются на исходной позиции после этапа распределения задач.

В таблицах 2 и 3 представлены результаты выявления вредоносных агентов в процессе функционирования РРТС. Аббревиатуры МА и РМ обозначают метод-аналог и предложенное решение соответственно. Эти обозначения будут использованы и далее. Сравнение полученных результатов в таблицах 2 и 3 приводится по количеству вредоносных агентов n'. Это обусловлено тем, что независимо от общего количества агентов системы n, изменение численности вредоносных агентов приводит к сопоставимым изменениям в получаемых результатах.

Таблица №2

Средние значения показателя количества шагов симуляции, необходимых для начала выявления вредоносных агентов

Критерий	Количество шагов симуляции, ед.		
Количество вредоносных агентов n'	1	25%	50%
МА	5,03	5,57	5,23
ПР	4,74	4,49	4,31

Согласно данным, представленным в таблице 2, увеличение количества вредоносных агентов в РРТС позволяет незначительно ускорить выявление вредоносных агентов. При этот, стоит отметить, результаты использования МА и ПР полностью сопоставимы.

Таблица №3

Средние значения показателя точности выявления вредоносных агентов

Критерий	Точность выявления вредоносных агентов, %		
Количество вредоносных агентов n'	1	25%	50%
МА	82,65	76,81	71,39
ПР	84,23	84,02	83,72

Согласно данным, представленным в таблице 3, изменение количества вредоносных агентов практически не влияет на точность их выявления при использовании ПР, которая составила ~84%. Однако, при использовании МА в результате увеличения количества вредоносных агентов наблюдается увеличение количества ложных срабатываний, что сказывается на точности (от 82,55 до 71,39%).

На рисунках 4-6 представлены показатели качества выполнения задач агентами РРТС для каждого из рассматриваемых значений количества агентов системы с использованием диаграмм размаха для более наглядного представления полученных результатов.

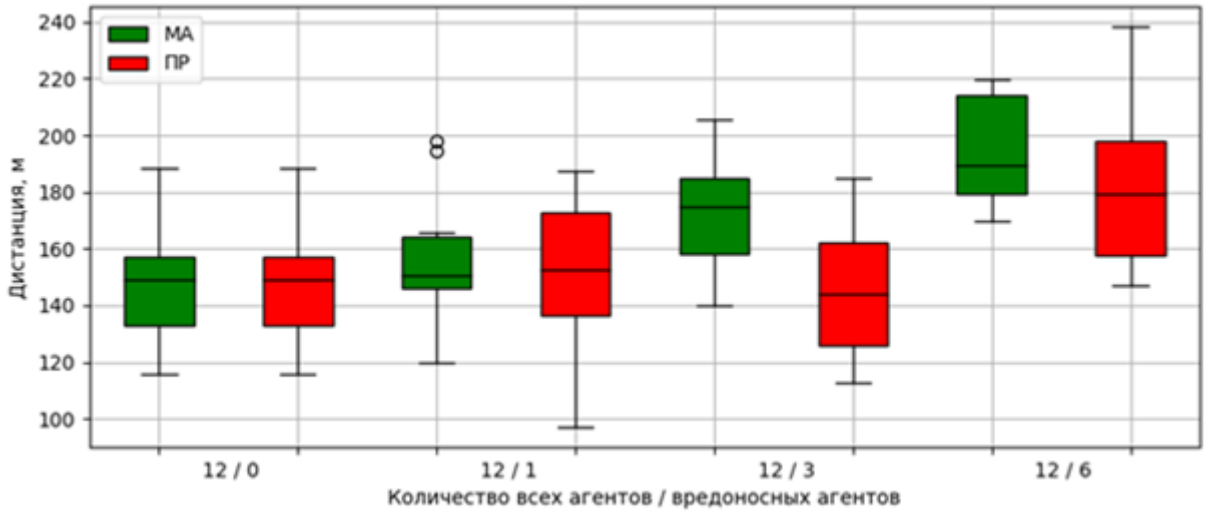

Рис. 4 – Результаты выполнения задания РРТС из 12 агентов

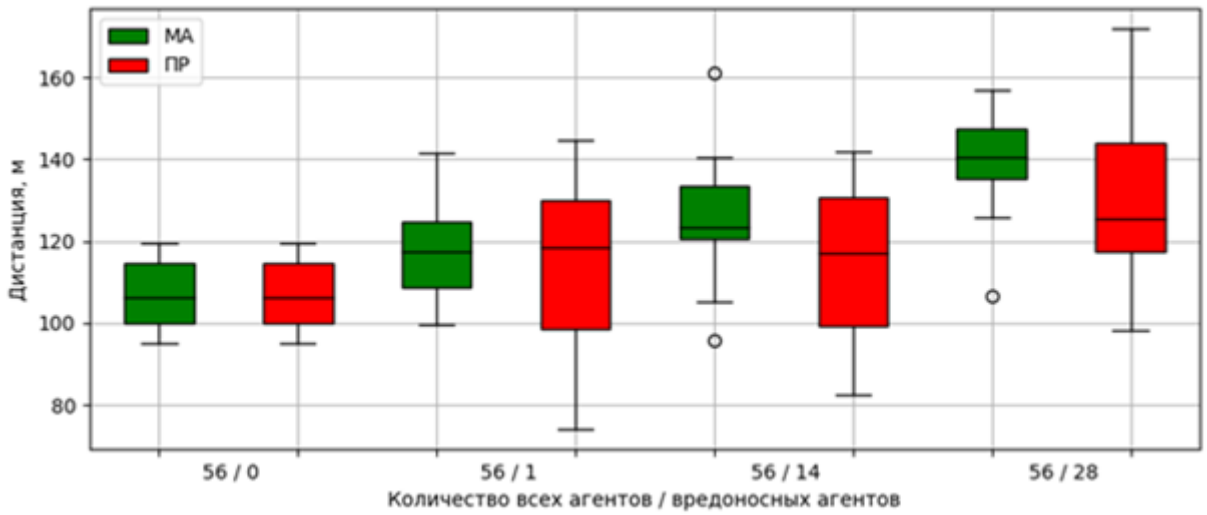

Рис. 5 – Результаты выполнения задания РРТС из 56 агентов

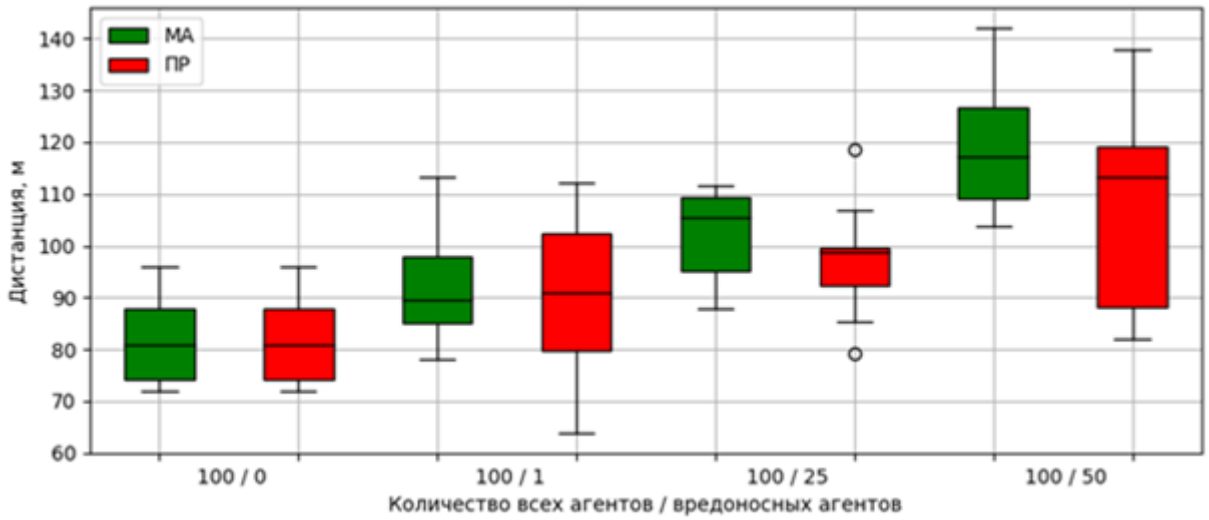

Рис. 6 – Результаты выполнения задания PPTC из 100 агентов

Для наглядности усредненные значения показателя дистанции, пройденной агентами PPTC в процессе выполнения задач, представлены в таблице 4.

Таблица № 4

Средние значения показателя максимальной дистанции, пройденной агентами PPTC в процессе выполнения задач

Критерий	Пройденная дистанция, м			
Соотношение n / n'	12 / 0	12 / 1	12 / 3	12 / 6
МА	146,48	157,82	172,08	194,36
ПР	146,48	150,11	144,99	182,85
Соотношение n / n'	56 / 0	56 / 1	56 / 14	56 / 28
МА	106,7	118,06	125,51	138,68
ПР	106,7	114,03	115,28	131,17
Соотношение n / n'	100 / 0	100 / 1	100 / 25	100 / 50
МА	81,45	92,75	102,32	119,46
ПР	81,45	90,5	97,27	107,54

Согласно результатам, представленным в таблице 4, использование ПР позволяет уменьшить значение максимальной дистанции, пройденной агентами PPTC в процессе выполнения задач от 2,43% (90,5 с против 92,75 с) до 15,74% (144,99 с против 172,08 с) по сравнению с МА. Таким образом,

результаты проведенного моделирования свидетельствует о повышении эффективности функционирования РРТС за счет разработанного решения.

Заключение

Для повышения эффективности функционирования РРТС при выполнении пространственно-распределенных задач в настоящей работе предложен метод выявления вредоносной информации на этапе распределения задач между агентами системы.

В основе предлагаемого метода лежат две основные идеи:

– анализ выполнимости и истинности заявляемых агентом данных в процессе распределения задач;

– механизм расчета показателей репутации агентов РРТС с учетом результатов проведенного ранее анализа данных.

Таким образом, научная новизна предложенного решения состоит в предложенных процедурах, отличительной особенностью которых является ориентированность на выявление ложной информации исключительно на этапе распределения задач между агентами РРТС.

Дальнейшие исследования будут направлены на разработку системы разграничения доступа к информационным ресурсам РРТС на основе комплекса разработанных ранее программно-алгоритмических решений и проведение экспериментальных исследований с использованием среды имитационного моделирования CoppeliaSim с целью анализа эффективности обеспечения информационной безопасности в РРТС.

Благодарности

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

Литература

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

2. 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, № 2. P. 288–297.

3. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms // IntelliSys 2016: Proceedings of SAI Intelligent Systems Conference (IntelliSys). 2018. P. 628–646.

4. Басан А.С., Басан Е.С. Модель угроз для систем группового управления мобильными роботами // VIII Всероссийская научная конференция «Системный синтез и прикладная синергетика». 2017. С. 205–212.

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

6. Правиков Д.И., Щербаков А.Ю. Концепция информационной безопасности «роя» киберфизических систем // Вестник современных цифровых технологий. 2021. № 7. С. 39–44.

7. Шабанов В.Б., Иванов Д.Я. Применение хаотических моделей и блокчейн-технологий для организации защищенного информационного обмена в группах роботов // Известия Тульского государственного университета. Технические науки. 2019.№ 10. С. 128–134.

8. Strobel V., Castelló Ferrer E., Dorigo M. Blockchain Technology Secures

Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots // Front. Robot. AI. 2020. Vol. 7. P. 1–22.

9. Maushart F., Prorok A., Hsieh M.A., Kumar V. Intrusion detection for stochastic task allocation in robot swarms // IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2017. P. 1830–1837.

10. Басан Е.С., Басан А.С., Макаревич О.Б. Разработка и реализация метода обнаружения аномального поведения узлов в группе роботов // Безопасность информационных технологий. 2018. № 25, № 4. С. 75–85.

11. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с.

12. Петренко В.И., Тебуева Ф.Б., Павлов А.С., Стручков И.В. Анализ рисков нарушения информационной безопасности в роевых робототехнических системах при масштабировании численности агентов // Прикаспийский журнал управление и высокие технологии. 2022. № 2. С. 92–109.

13. Викснин И.И., Мариненков Е.Д. Противодействие скрытому деструктивному воздействию в роях беспилотных летательных аппаратов // Int. J. Open Inf. Technol. 2018. Vol. 6, № 12. P. 1–11.

14. Курилец А.В., Смелов В.В., Горанин Н. Метод авторизации на основе разложения чисел на простые сомножители // Труды БГТУ. Серия 3, Физико-математические науки и информатика. 2021. Т. 1, № 242. С. 43–47.

15. Захаров А.А., Пономарев К.Ю., Несговоров Е.С., Ниссенбаум О.В. Построение модели авторизации внешних средств защиты АСУ ТП на базе Интернета вещей // Вестник Тюменского государственного университета. Физико-математическое моделирование. Нефть, газ, энергетика. 2017. Т. 3, № 1. С. 99–110.

16. Sahai A., Waters B. Fuzzy Identity-Based Encryption // Adv. Cryptol. Eurocrypt. 2005. P. 457–473.

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

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

19. Антонов В.О., Гурчинский М.М., Петренко В.И., Тебуева Ф.Б. Метод планирования траектории движения точки в пространстве с препятствием на основе итеративной кусочно-линейной аппроксимации // Системы управления, связи и безопасности. 2018. № 1. С. 168–182.

20. Юдинцев Б.С. Синтез нейросетевой системы планирования траекторий для группы мобильных роботов // Системы управления, связи и безопасности. 2019. № 4. С. 163-186.

21. Koubaa A. Performance Analysis of the MRTA Approaches for Autonomous Mobile Robot BT - Robot Path Planning and Cooperation: Foundations, Algorithms and Experimentations // Computational Intelligence. 2018. P. 169–188.

22. Maas A.L., Hannun A.Y., Ng A.Y. Rectifier Nonlinearities Improve Neural Network Acoustic Models // Proc. 30th Int. Conf. Mach. Learn. 2013. Vol. 28, № 3. P. 1–6.

23. TensorFlow. URL: github.com/tensorflow/tensorflow (дата обращения: 17.09.2022).

24. Keras. URL: https://keras.io/ (дата обращения: 17.09.2022).

25. Zeiler M.D. ADADELTA: An Adaptive Learning Rate Method // arXiv:1212.5701. – 2012. – Режим доступа: http://www.matthewzeiler.com/pubs/googleTR2012/googleTR2012.pdf.

References

1. Petrenko V.I., Tebueva F.B., Gurchinsky M.M., Ryabtsev S.S. Nauka i biznes: puti razvitiya. 2020. № 4 (106). P. 96-99.

2. Higgins F., Tomlinson A., Martin K.M. International Journal on Advances in Security. 2009. Vol. 2, № 2. P. 288-297.

3. Sargeant I., Tomlinson A. Review of Potential Attacks on Robotic Swarms. IntelliSys 2016: Proceedings of SAI Intelligent Systems Conference (IntelliSys). 2018. P. 628-646.

4. Basan A.S., Basan E.S. Model' ugroz dlya sistem gruppovogo upravleniya mobil'nymi robotami [Threat model for group control systems of mobile robots]. VIII Vserossijskaya nauchnaya konferenciya «Sistemnyj sintez i prikladnaya sinergetika». 2017. P. 205-212.

5. Zikratov I.A., Zikratova T.V., Lebedev I.S. Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2014. Vol. 2, № 90. Pp. 47–52.

6. Pravikov D.I., Shherbakov A.Ju. Vestnik sovremennyh cifrovyh tehnologij. 2021. № 7. P. 39-44.

7. Shabanov V.B., Ivanov D.Ja. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2019.№ 10. P. 128-134.

8. Strobel V., Castelló Ferrer E., Dorigo M. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots. Front. Robot. AI. 2020. Vol. 7. Pp. 1-22.

9. Maushart F., Prorok A., Hsieh M.A., Kumar V. Intrusion detection for stochastic task allocation in robot swarms. IEEE RSJ International Conference on Intelligent Robots and Systems (IROS). 2017. Pp. 1830-1837.

10. Basan E.S., Basan A.S., Makarevich O.B. Bezopasnost' informacionnyh tehnologij. 2018. № 25, № 4. P. 75–85.

11. Kaljaev I.A., Gajduk A.R., Kapustjan S.G. Modeli i algoritmy kollektivnogo upravlenija v gruppah robotov [Models and algorithms of collective

control in groups of robots]. M.: FIZMATLIT, 2009. 280 p.

12. Petrenko V.I., Tebueva F.B., Pavlov A.S., Struchkov I.V. Prikaspijskij zhurnal: upravlenie i vysokie tehnologii. 2022. № 2. P. 92-109.

13. Viksnin I.I., Marinenkov E.D. Int. J. Open Inf. Technol. 2018. Vol. 6, № 12. P. 1-11.

14. Kurilec A.V., Smelov V.V., Goranin N. Trudy BGTU. Serija 3, Fiziko-matematicheskie nauki i informatika. 2021. T. 1, № 242. P. 43–47.

15. Zaharov A.A., Ponomarev K.Ju., Nesgovorov E.S., Nissenbaum O.V. Vestnik Tjumenskogo gosudarstvennogo universiteta. Fiziko-matematicheskoe modelirovanie. Neft', gaz, jenergetika. 2017. № 3(1). P. 99-110.

16. Sahai A., Waters B. Adv. Cryptol. Eurocrypt. 2005. P. 457-473.

17. Zakiev A., Tsoy T., Magid E. Swarm Robotics: Remarks on Terminology and Classification BT - Interactive Collaborative Robotics. Interactive Collaborative Robotics (ICR 2018). 2018. Pp. 291-300.

18. Pavlov A.S. Sistemy upravleniya, svyaazi i bezopasnosti. 2021. № 3. P. 38-59.

19. Antonov V.O., Gurchinsky M.M., Petrenko V.I., Tebueva F.B. Sistemy upravleniya, svyazi i bezopasnosti. 2018. № 1. Pp. 168–182.

20. Judincev B.S. Sistemy upravleniya, svyazi i bezopasnosti. 2019. № 4. Pp. 163-186.

21. Koubaa A. Computational Intelligence. 2018. pp. 169–188.

22. Maas A.L., Hannun A.Y., Ng A.Y. Rectifier Nonlinearities Improve Neural Network Acoustic Models. Proc. 30th Int. Conf. Mach. Learn. 2013. Vol. 28, № 3. pp. 1–6.

23. TensorFlow/ URL: github.com/tensorflow/tensorflow (accessed: 17.09.2022).

24. Keras. URL: keras.io (accessed: 17.09.2022).

25. Zeiler M.D. ADADELTA: An Adaptive Learning Rate Method.

arXiv:1212.5701. 2012. Available at: matthewzeiler.com/pubs/googleTR2012/googleTR2012.pdf.