ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.896
DOI: 10.21822/2073-6185-2023-50-2-134-141 Оригинальная статья /Original Paper

Модель доверенного взаимодействия агентов в децентрализованной киберфизической среде

В.И. Петренко, Ф.Б. Тебуева, И.В. Стручков, С.С. Рябцев
Северо-Кавказский федеральный университет,
355029, г. Ставрополь, пр-кт Кулакова, 2, Россия

Резюме. Цель. Целью исследования является повышение эффективности выполнения задач агентами киберфизической системы при наличии агентов с неисправным или вредоносным поведением за счет установления доверенного взаимодействия между агентами и быстрого выявления вредоносного воздействия. **Метод.** Доверенное взаимодействие осуществляется с помощью технологии распределенного реестра и показателя уверенности агентов при коллективном решении. Новизна предлагаемого решения состоит в том, что информация о действиях агентов будет храниться и агрегироваться с использованием смарт-контрактов через заданные интервалы времени. Отдельный агент хранит локальную копию цепочки взаимодействия агентов, если несколько агентов взаимодействуют между собой, то они обмениваются информацией, хранящейся в их распределенном реестре. **Результат.** Для апробации предложенного метода была выполнена его программная реализация на языке программирования C++. Для проведения экспериментов использован сценарий коллективного восприятия агентами децентрализованной киберфизической среды в специализированной имитационной программе Contiki's Cooja. **Вывод.** Метод, реализованный с помощью предложенных в работе решений, оказался эффективнее, чем метод на основе динамического расчета показателя уверенности. Предложенные решения можно применять не только в киберфизических системах, но и в других системах с децентрализованным управлением.

Ключевые слова: доверенное взаимодействие, информационная безопасность, технология распределённого реестра, киберфизические системы

Для цитирования: В.И. Петренко, Ф.Б. Тебуева, И.В. Стручков, С.С. Рябцев. Модель доверенного взаимодействия агентов в децентрализованной киберфизической среде. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(2):134-141. DOI:10.21822/2073-6185-2023-50-2-134-141

Model of trusted interaction of agents in decentralized cyber-physical environmentv

V.I. Petrenko, F.B. Tebueva, I.V. Struchkov, S.S. Ryabtsev
North-Caucasus Federal University,
2 Kulakov Ave., Stavropol 355029, Russia

Abstract. Objective. The purpose of the work is to increase the efficiency of the functioning of agents of a cyber-physical system in the presence of agents with incorrect or malicious behavior. The goal is achieved by establishing a trusted interaction between agents and quick detection of malicious impact. **Method.** Trusted interaction is carried out using distributed ledger technology and agent confidence indicators. The novelty of the proposed solution lies in the fact that information about the actions of agents is stored and aggregated using smart contracts at specified time intervals. Each agent keeps a local copy of the agent interaction chain. If several agents interact with each other, then they exchange information stored in their copies of the ledger. **Result.** To test the proposed method, we implemented it in C++. For the experiments, the scenario of collective perception by agents of a decentralized cyber-physical environment in a specialized simulation program Contiki Cooja was used.**Conclusion.** The method implemented using the solu-

tions proposed in this work showed higher efficiency than the method based on the dynamic calculation of the confidence index. The proposed solutions can be applied not only in cyber-physical systems, but also in any other systems with decentralized control.

Keywords: trusted interaction, information security, distributed ledger technologies, cyber-physical systems

For citation: V.I. Petrenko, F.B. Tebueva, I.V. Struchkov, S.S. Ryabtsev. Model of trusted interaction of agents in decentralized cyber-physical environmentv. Herald of Daghestan State Technical University. Technical Science. 2023; 50(2):134-141. DOI:10.21822/2073-6185-2023-50-2-134-141

Введение. Киберфизические системы (КФС) – это системы, которые объединяют компьютерные и физические компоненты в единое целое. Они представляют собой сеть распределенных датчиков, исполнительных механизмов, устройств управления и информационных технологий, которые взаимодействуют друг с другом, обмениваясь данными и управляющими сигналами в режиме реального времени [1, 2]. КФС широко используются в различных областях: в производстве, энергетике, автоматизации транспорта, медицине, безопасности и т.д. На практике при решении ряда задач, требующих покрытия больших пространств параллельного выполнения большого числа типовых заданий в неблагоприятных условиях, эффективным является децентрализованное взаимодействие и принятие решений между отдельными устройствами КФС, которые образуют децентрализованную киберфизическую среду (ДКФС). ДКФС является пространством, объединяющим физические объекты с кибернетическими системами и технологиями, работающими децентрализовано и не имеющими единого центра управления. Это среда, в которой действия и решения принимаются автономно между устройствами и сетями, которые обмениваются информацией и принимают решения без прямого участия оператора.

Примерами ДКФС являются сети умных домов, в которых каждое устройство может принимать решения по управлению энергопотреблением, освещением и т.д. на основе информации, полученной от других устройств; это может быть система управления транспортным потоком, которая автоматически регулирует движение автомобилей и пешеходов на улицах города; это может быть производственная линия, в которой различные машины сами принимают решения о необходимости изменения траектории движения или замены инструментов. ДКФС обеспечивает повышенную безопасность и гибкость систем, снижает риски сбоев и увеличивает производительность при параллельном выполнении большого количества схожих задач. В большинстве работ по киберфизическим системам предлагаемые методы апробируются в лабораторных условиях и не учитывают наличие неблагоприятной внешней среды и угроз информационной безопасности (ИБ). Наряду с традиционными угрозами ИБ, КФС подвержены угрозам реализации специфических атак за счет системных свойств КФС [3], например, вредоносных воздействий нарушителей при реализации доверенного взаимодействия (ДВ).

Под вредоносным воздействием понимаются действия узлов децентрализованной системы – вредоносных агентов (ВА), которые демонстрируют непреднамеренное или непоследовательное поведение независимо от основной причины, оказывают негативный эффект на функционирование системы, в том числе из-за поломки или сбоя [4]. Наличие скомпрометированных узлов при реализации ДВ киберфизических устройств может привести к негативным последствиям и невозможности выполнить целевую функцию КФС. Обобщенно модель ДВ в КФС можно представить в виде 4 последовательных этапов, выполняющихся непрерывно и последовательно, представленных рис. 1.

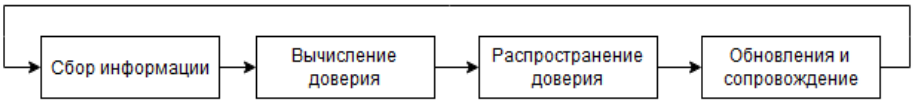


Рис. 1. Обобщённая модель доверенных отношений
Fig.1. General Model of trusted interaction

На этапе «Сбор информации» определяются предварительные требования и сведения для вычисления оценки доверия. На этом этапе затрагиваются вопросы: какие параметры следует выбрать для определения доверия к системе; как собирается информация; как представить информацию в необходимой форме?

На этапе «Вычисление доверия» осуществляется выбор подходящей вычислительной модели для оценки надежности объектов. Распространение доверия – это передача информации о доверии между объектами, может осуществляться по двум следующим архитектурам: централизованной и распределенной. При этом при централизованной архитектуре для того, чтобы узнать рейтинг доверия устройства, доверитель запрашивает централизованный орган, который, в свою очередь, сделает все необходимое и вернет оценку доверия к устройству. В распределенном типе архитектуры нет центрального объекта для вычисления и управления показателя доверия. Вместо этого каждый объект вносит свой вклад в процесс обмена информацией и хранит мнения о прошлом поведении. Преимущество использования распределенного подхода заключается в том, что ни одна точка отказа не влияет на управление доверием. В то же время требования к памяти и стоимость вычислений на объект увеличиваются. Также такие подходы имеют более высокое время сходимости по сравнению с централизованной архитектурой.

На заключительном этапе «Обновление и обслуживание» выполняется обновление и поддержка оценки доверия с течением времени. В частности, в распределенных и динамических сценариях, таких как ДКФС, поведение устройства не является постоянным во времени и необходимо обновлять вычисленный показатель доверия.

ИБ - это одна из проблем, влияющих на эффективность работы агентов в КФС [5]. Часто для решения проблемы ИБ используются такие механизмы «Hard Security» [6].Однако подобные механизмы не обеспечивают надежность КФС при наличии злонамеренных действий со стороны инсайдера из-за изменения его поведения. Методы доверительного управления [7, 8] решают эту проблему, измеряя степень уверенности в поведении, ожидаемом другими. Концепция доверия относится к категории «Soft Security». Одним из популярных подходов является применение технологии распределенного реестра для обеспечения ИБ в ДКФС [9]. Это связано со схожестью принципов взаимодействия участников блокчейн системы с агентами ДКФС, которая также не имеет централизованного контроля и необходима для работы нехватки доверия к участникам [10, 11].

Постановка задачи. В данной работе рассматриваются вопросы обеспечения эффективности выполнения задач агентам КФС при наличии агентов с неисправным или вредоносным поведением. Для решения задач, связанных с улучшением защищенности агентов в ДКФС, первоочередной целью является построение архитектурной модели, в которой будет создан алгоритм работы ДВ на основе применения технологии распределенного реестра. Основная цель для злоумышленника – это слабый узел всей системы. Уязвимости в узловой системе часто возникают из-за технологических недостатков в результате необходимости быстрого выпуска продукции, вследствие чего проблемы ИБ необходимо учитывать в уже функционирующей системе, быстро идентифицировать и блокировать вредоносных агентов.

Целью работы является повышение эффективности выполнения задач агентам КФС при наличии агентов с неисправным или вредоносным поведением за счет установления ДВ между агентами КФС и быстрого выявления ВА.

Дано: S – КФС, состоящая из агентов a_i, X – множество входных параметров (P_{trust} – физические показатели агента i; Y_{trust} – степень уверенности агента i; R_{trust} – время отклика агента i), Y – множество выходных параметров (T_{direct_i} – оценки доверия устройства).

Постановкой задачи является нахождение модели M, такой что:

$$M : \langle S, X, Y \rangle \mid a_i \in S \exists T_{direct_i} \in [0,1] \quad ,$$

при этом: при наличии у a_i, показателя T_{direct_i} ниже требуемого уровня запрещает взаимодействие и информационный обмен с этим агентом для всей КФС.

Исследование процесса ДВ осуществлялось на примере задачи мониторинга признаков ограниченной стенами среды, которая сводится к сценарию коллективного восприятия агентов в ДКФС [12]. Альтернативами в процессе КПР A_i в данном случае служат суждения о качестве параметров. При проведении экспериментов изменяющиеся факторы внешней среды E представлены цветами на некоторой сцене, разделенной координационной сеткой, полученной на основании спутниковых снимков и базовых сведений об исследуемой среде.

Цель агентов КФС состоит в том, чтобы достичь консенсуса, выполнить коллективное принятие решения (КПР) и выбрать на основе данных о внешней среде одну из нескольких альтернатив A_i (голосование за то, что определенный параметр внешней среды обладает определённым качеством на сцене, что необходимо для эффективного распределения задач) при наличии изменения с течением времени качества альтернатив среды, которое в экспериментах данной статьи изменялось случайным образом в диапазоне каждые 100 раундов процесса КПР. Сложность задачи можно варьировать, изменяя соотношение между количеством присутствующих в среде альтернатив для выбора агентом. В простой задаче с двумя альтернативами, разница между их процентным соотношением должна быть велика, в сложной – напротив, минимальной. Таким образом, чем соотношение между альтернативами более близко к равновероятному распределению, тем сложнее агенту выбрать наиболее преобладающий признак.

Для оценки эффективности представленных решений используется показатель среднего затраченного времени агентами (t) КФС для выполнения задач и вероятность принятия решения (p)в условиях негативного воздействия со стороны ВА. В качестве ВА рассматриваются агенты, посылающие случайные данные о внешней среде, поведение такого агента можно описать следующим образом:

$$N_{\hat{i}j} = rand\ N_{ij}\text{'}$$

где N_{ij}, полезность для каждого действия A_i и состояния S_j, которое определяется подсчитанными агентами на данный момент областями на сцене, исходя из соотношения между двумя альтернативами A_1 и A_2, $\hat{i}$ номер выбранной агентами альтернативы.

Методы исследования. Схематическое представление предлагаемой модели доверенного взаимодействия агентов в ДКФС показано на рис. 2.

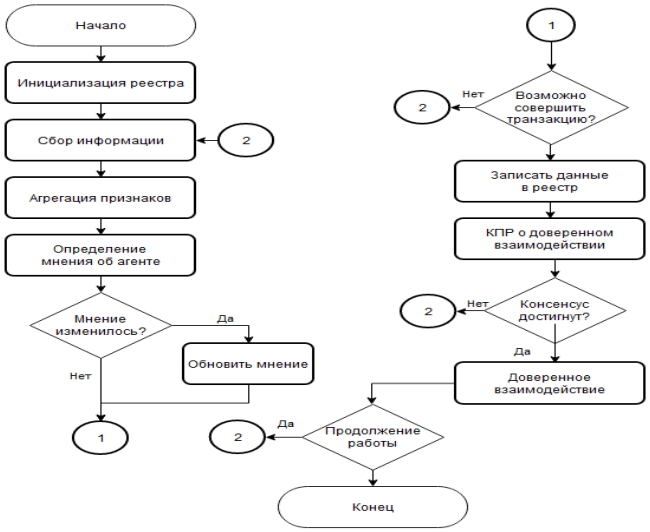


Рис. 2. Схематическое представление предлагаемой модели
Fig. 2 Schematic representation of the proposed model

Взаимодействие с агентами в ДКФС осуществляется с помощью смарт-контрактов. Предусмотрены 4 функции: setInfo, getTrust, vote и isConsensusArchieved. Функция setInfo добавляет или обновляет отправленные агентом данные об измерениях внешней среды и

показателях доверия в реестр. Смарт-контракт игнорирует «просроченные» данные, опубликованные более 25 блоков назад, данные агента, опубликовавшего более 50 транзакций в один блок, а также данные агента, имеющего отличную версию блокчейна. Для выполнения этой функции агенту необходимо отправить 0.9 ether. Данное ограничение не позволит бесконтрольно изменять данные, хранящиеся в блокчейне и, тем самым, защитит их от недобросовестных, либо вышедших из строя элементов КФС. Сумма назначена с учетом того, что награда за созданный блок при майнинге составляет 1 ether, чего будет достаточно для того, чтобы выполнить данную функцию с учетом ее цены, а также предусмотренной в сети Ethereum комиссии.

Функция getTrust позволяет агентам КФС выяснить показатели доверия с учетом данных, размещенных в реестре всеми элементами КФС. Показатель доверия формируется как взвешенная сумма всех измерений, хранимых в реестре. Переда началом эксперимента с помощью программы geth инициализируется и запускается локальная версия блокчейна Ethereum, в которой публикуется описанный выше смарт-контракт. К этому процессу в течение эксперимента подключаются агенты КФС для публикации собранных ими данных, а также получения и обработки данных, собранных другими агентами КФС. Кроме того, на протяжении всей работы каждый агент осуществляет майнинг, необходимый ему для отправки данных в реестр. Данное действие не отображено в блок-схеме, так как осуществляется непрерывно в фоновом режиме и заключается в исследовании признаков внешней среды и сборе данных о взаимодействии с другими агентами. Сложность открытия нового блока зависит от вычислительной мощности КФС и установлена таким образом, чтобы в минуту появлялось в среднем два новых блока. После инициализации блокчейна агенты совершают агрегацию признаков в единый реестр и выполняют процедуру вычисления доверия. Для вычисления доверия используется формула:

$$T_{direct_i} = \alpha * P_{trust_i} + \beta * Y_{trust_i} + \gamma * R_{trust_i},$$

где T_{direct} – оценка доверия, рассчитываемая для агента i, P_{trust} – физические показатели агента i, Y_{trust} – степень уверенности агента i, $\mathrm{P}_{\mathrm{trust}}$ – время отклика агента i, α, β, γ – коэффициенты приоритета показателя, зависящие от требований и типа КФС и изменяющиеся от 0 до 1. При этом должно выполняться условие формулы:

$$\alpha + \beta + \gamma = 1$$

Следует отметить, что, реальные значение приоритетов необходимо выбирать исходя из конкретной задачи, требований стандартов и переназначения КФС. В данной работе эксперименты осуществлялись по показателям Y_{trust} – степень уверенности агента i; Y_{trust} – время отклика агента i.

Под уверенностью агента понимается мера – насколько часто в процессе принятия решения агент меняет свое мнение, которая описана в работе [13]. После определения показателей доверия проводится попытка установления связи и синхронизации цепочки блокчейна с другими агентами. После выполнения данного шага агент обращается к функции getTrust смарт-контракта для того, чтобы проверить, отличается ли его собственное мнение о значении показателя доверия в имеющейся у него версии реестра. В случае если оно отличается, агент инициализирует транзакцию и отправляет свое обновленное мнение при помощи функции vote смарт-контракта.

В рамках эксперимента максимальная дальность беспроводной связи между мобильными агентами ДКФС была ограничена 1 метром. В случае нехватки ресурсов для записи агенты продолжают исследовать среду. На следующем этапе, на основании данных реестра происходит процедура КПР между агентами КФС до тех пор, пока между ними будет достигнут консенсус об агентах, которые являются подозрительными и взаимодействие с которыми необходимо заблокировать.

В качестве механизма смены мнения в данной статье применяется модель большинства, согласно которой агент проверяет имеющуюся у него актуальную версию распределенного реестра и качество признаков каждой альтернативы, затем агент меняет свое мнение на наиболее распространённый вариант по правилу большинства:

$$a_{\hat{q}}, \hat{q} = \arg\max P_q .$$

Таким образом, агент меняет свое мнение на самое распространенное мнение согласно распределенному реестру. После смены мнения агент сообщает о значении доверия T_{direct} прочих агентов и применяется функция isConsensusArchieved, которая позволяет выяснить, достигнут ли консенсус. Подсчитываются голоса и при наличии 80%, проголосовавших за блокировку, консенсус считается достигнутым и взаимодействие с данным агентом блокируется, иначе необходимо перейти заново на стадию исследования среды.

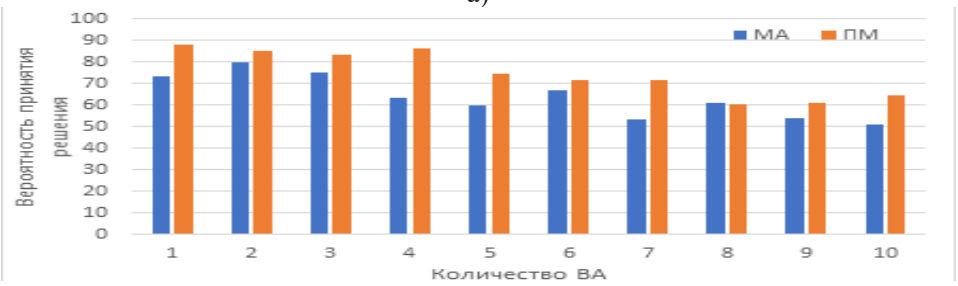
Обсуждение результатов. Для апробации предложенного метода была выполнена его программная реализация на языке программирования C++, при этом использовалась среда имитационного моделирования Contiki's Cooja. В качестве функциональной задачи и метода принятия решения применен метод достижения консенсуса, описанный в [14]. Использованы параметры моделирования, указанные в табл. 1.

Таблица 1. Параметры моделирования
Table 1. Simulation parameters

Наименование параметра/ Parameter name	**Значение/ Meaning**	**Наименование параметра/ Parameter name**	**Значение/ Meaning**
Количество агентов/ Number of agents	20	Количество альтернатив выбора /Number of choice alternatives	2
Количество экспериментов/ Number of experiments	1000	Размер сцены/ Stage size	100 на 100 м.
Количество вредоносных агентов/ Number of malicious agents	0-10	Сложность сцены/ Scene complexity	75%
Кворум достижения консенсуса/ Consensus quorum	16	Распределение цветов на сцене/ Distribution of colors on the stage	40:60

Для проведения исследований был использован сценарий коллективного восприятия с параметрами моделирования, указанными в табл. 1. Моделирование предполагало серию экспериментов из 1000 симуляций для 20 мобильных агентов КФС. Результаты на рис. 3 показывают эффективность предлагаемых решений по сравнению с методом-аналогом, использующим динамический расчет доверия [15]: по показателям среднего затраченного времени на выявление ВА (а) и вероятности принятия правильного решения агентами КФС относительно преобладающего признака среды (б).

а)



б)

Рис. 3. Сравнение предложенного метода (ПМ) с методом-аналогом (МА) по показателю: а) среднего затраченное время для выявления вредоносных агентов; б) вероятности принятия лучшего решения
Fig. 3. Proposed and analogue methods comparison in terms of: a) average time to detect malicious agents; b) probability of making a better decision

Согласно полученным в ходе моделирования данным предложенное решение обеспечивает повышение эффективности по показателю среднего затраченного времени на выявление ВА в среднем на 10,02 %, а по показателю вероятности принятия решения – на 14,15%.

Вывод. В данной статье предложена модель ДВ в ДКФС, основанная на применении технологии распределенного реестра. Экспериментальные результаты показывают, что эффективность предлагаемой модели ДВ агентов в ДКФС по времени обнаружения ВА превосходит метод на основе динамического расчета доверия в среднем на 10,02 %, а по показателю эффективности функционирования агентов КФС – вероятность принятия наилучшего решения – на 14,15%.

Таким образом, можно сделать вывод о том, что выполнение ДВ с помощью распределенного реестра и смарт-контрактов для расчета показателя доверия при выборе альтернативы позволили снизить среднее затраченное время на выявление ВА и улучшить вероятность принятия лучшего решения при выполнении целевых задач агентами КФС.

Практическая значимость предлагаемых решений обусловлена факторами достижения предлагаемых технических решений высоких показателей ИБ ДВ агентов в ДКФС, что позволит повысить отказоустойчивость по сравнению с централизованным управлением. Предлагаемая модель позволит повысить эффективность агентов при реализации ДВ в ДКФС.

Благодарности. Исследование выполнено при финансовой поддержке Минцифры России (грант ИБ, проект № 27/22-к).

Acknowledgments. The study was financially supported by the Russian Ministry of Digital Development (IB grant, project No. 27/22-k).

Библиографический список:

1. Алгулиев Р.М., Имамвердиев Я.Н., Сухостат Л.В. Киберфизические системы: основные понятия и вопросы обеспечения безопасности // Информационные технологии. 2017. Т. 23. № 7. С. 517–528.
2. Lee E.A., Cheng A.M.K. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models // Multidisciplinary Digital Publishing Institute. 2015. V. 15, № 3. C. 4837–4869.
3. Закирова Ю.М., Мышляева А.А., Закиева Е.Ш. Киберфизические системы: возможности и угрозы // Технологические инновации в современном мире. 2019. С. 64–68.
4. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem // C. Trans. Program. Lang. Syst. 1982. V. 4, № 3. P. 382–401.
5. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead // Comput. Networks. Elsevier, 2015. V. 76. P. 146–164.
6. Jøsang A., Keser C., Dimitrakos T. Can We Manage Trust? // Lect. Notes Comput. Sci. Springer, Berlin, Heidelberg, 2005. V. 3477. P. 93–107.
7. Jøsang A., Ismail R., Boyd C. A survey of trust and reputation systems for online service provision // Decis. Support Syst. North-Holland, 2007. V. 43, № 2. P. 618–644.
8. Kaur J. Trust Based Technique for the Multicasting in IoT // Int. J. Emerg. Trends Eng. Res. The World Academy of Research in Science and Engineering, 2020. V. 8, № 8. P. 4574–4579.
9. Kumar A. IOT Security with Blockchain // YMER Digit. Engineering Skill Development, 2021. V. 20, № 11. P. 7–19.
10. Putra G.D. Blockchain for Trust and Reputation Management in Cyber-Physical Systems // Springer Optim. Its Appl. Springer, 2022. V. 194. P. 339–362.
11. Zhou Z. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: integration of blockchain and edge computing // IEEE Trans. Syst. Man, Cybern. Syst. Institute of Electrical and Electronics Engineers Inc. 2020. V. 50, № 1. P. 43–57.
12. Valentini G., Brambilla D., Hamann H.,Dorigo M. Collective perception of environmental features in a robot swarm // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, 2016. V. 9882. P. 65–76.
13. Рябцев С.С. Метод выявления вредоносных роботов на основе данных процесса коллективного принятия решений в роевых робототехнических системах // Системы управления, связи и безопасности. 2021. № 5. С. 224-258.
14. Petrenko V.I., Tebueva F.B., Ryabtsev S.S., Gurchinsky M.M., Struchkov I.V. Consensus achievement method for a robotic swarm about the most frequently feature of an environment // IOP Conference Series: Materials Science and Engineering. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Krasnoyarsk, Russia, 2020. P. 42025.

15. Garagad V., Iyer N. Secure IoT Interactions using Dynamic Trust Assessment // 2022 IEEE 7th International conference for Convergence in Technology (I2CT). 2022. P. 1-8

References:

1. Alguliyev R.M., Imamverdiyev Ya.N., Sukhostat L.V. Cyber-Physical Systems: Basic Concepts and Security Issues. *Information technologies*. 2017; 23(7): 517–528. (In Russ)
2. Lee E.A., Cheng A.M.K. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. *Multidisciplinary Digital Publishing Institute.* 2015; 15(3): 4837–4869.
3. Zakirove Yu.M., Myshlyaeva A.A.Zakieva, E.S. Cyber-Physical Systems: Opportunities and Threats // *Technological innovation in the modern world*, 2019, 64–68. (In Russ)
4. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem. *C. Trans. Program. Lang. Syst.* 1982; 4(3): 382–401.
5. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Networks. Elsevier*, 2015; 76: 146–164.
6. Jøsang A., Keser C., Dimitrakos T. Can We Manage Trust? *Lect. Notes Comput. Sci. Springer*, Berlin, Heidelberg, 2005; 3477: 93–107.
7. Jøsang A., Ismail R., Boyd C. A survey of trust and reputation systems for online service provisionю. *Decis. Support Syst. North-Holland*, 2007; 43(2): 618–644.
8. Kaur J. Trust Based Technique for the Multicasting in IoT. *Int. J. Emerg. Trends Eng. Res. The World Academy of Research in Science and Engineering*, 2020; 8(8): 4574–4579.
9. Kumar A. IOT Security with Blockchain.*YMER Digit. Engineering Skill Development*, 2021; 20(11): 7–19.
10. Putra G.D. Blockchain for Trust and Reputation Management in Cyber-Physical Systems. *Springer Optim. Its Appl. Springer,* 2022; 194: 339–362.
11. Zhou Z. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: integration of blockchain and edge computing. *IEEE Trans. Syst. Man, Cybern. Syst. Institute of Electrical and Electronics Engineers Inc.,* 2020; 50(1): 43–57.
12. Valentini G., Brambilla D., Hamann H.,Dorigo M. Collective perception of environmental features in a robot swarm. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag*, 2016; 9882: 65–76.
13. Ryabtsev S. S. A method for detecting Byzantine robots based on data from the collective decision-making process in swarm robotic systems. *Systems of Control, Communication and Security*, 2022; 3: 105-137. (In Russ)
14. Petrenko V.I., Tebueva F.B., Ryabtsev S.S., Gurchinsky M.M., Struchkov I.V. Consensus achievement method for a robotic swarm about the most frequently feature of an environment. *IOP Conference Series: Materials Science and Engineering. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations*. Krasnoyarsk, Russia, 2020; 42025.
15. Garagad V., Iyer N. Secure IoT Interactions using Dynamic Trust Assessment. *2022 IEEE 7th International conference for Convergence in Technology (I2CT),* 2022; 1-8

Сведения об авторах:

Петренко Вячеслав Иванович, кандидат технических наук, доцент, заведующий кафедрой организации и технологии защиты информации Института цифрового развития, vipetrenko@ncfu.ru.

Тебуева Фариза Биляловна, доктор физико-математических наук, доцент, заведующая кафедрой компьютерной безопасности Института цифрового развития, ftebueva@ncfu.ru. ORCID 0000-0002-7373-4692

Стручков Игорь Владиславович, инженер-исследователь кафедры организации и технологии защиты информации Института цифрового развития, selentar@bk.ru.

Рябцев Сергей Сергеевич, старший преподаватель кафедры компьютерной безопасности Института цифрового развития, nalfartorn@yandex.ru.

Information about the authors:

Vyacheslav I. Petrenko, Cand. Sci. (Eng), Assoc. Prof., Head of the Department of Organization and Technology of Information Security, vipetrenko@ncfu.ru.

Fariza B. Tebueva, Dr. Sci.(Physics and Mathematics), Assoc. Prof., Head of the Department of Computer Security, ftebueva@ncfu.ru. ORCID 0000-0002-7373-4692

Igor .V. Struchkov, Research Engineer, Department of Organization and Technology of Information Security, selentar@bk.ru.

Sergey S. Ryabtsev, Senior Lecturer of the Department of Computer Security, nalfartorn@yandex.ru.

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 26.04.2023.

Одобрена после рецензирования/ Reviced 18.05.2023.

Принята в печать/ Accepted for publication 18.05.2023.