15. *Yiyang Li, Guanyu Tao, Weinan Zhang, Yong Yu, Jun Wang.* Content Recommendation by Noise Contrastive Transfer Learning of Feature Representation, *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, ACM*, 2017, pp 1657-1665.
16. *Pan S.J., Yang Q.* IEEE Transactions on knowledge and data engineering, *Institute of Electrical and Electronics Engineers, Inc., NY, 2010*, Vol. 22 (10), pp 1345-1359.
17. *Saprykin A.N., Akinina K.D., Saprykina E.N.* Nakhozhdenie optimal'nogo chisla poleznykh osobey v populyatsii i konvergiruemykh pokoleniy geneticheskogo algoritma optimizatsii prostykh mnogoekstremal'nykh funktsiy [Finding the optimal number of useful individuals in the population and converged generations of the genetic algorithm for optimization of simple multi-extreme functions], *Actualscience* [Actualscience], 2016, Vol. 2. No. 11, pp. 168-169.
18. *Zadeh L.A.* Fuzzy sets, *Information and Control*, 1965, Vol. 8, pp. 338.
19. Nechetkie mnozhestva v modelyakh upravleniya i iskusstvennogo intellekta [Fuzzy sets in control and artificial intelligence models], ed. by D.A. Pospelova. Moscow: Nauka, 1986, 312 p.
20. *Kureychik V.M., Danil'chenko V.I.* Klassifikatsiya i analiz metodov resheniya zadachi razmeshcheniya SBIS [Classification and analysis of methods for solving the problem of VLSI placement], *Informatika, vychislitel'naya tekhnika i inzhenernoe obrazovanie* [Computer science, computer engineering and engineering education], 2018, No. 1 (32), pp. 21-40.

Статью рекомендовал к опубликованию д.т.н., профессор А.Н. Целых.

Чернышев Юрий Олегович – Донской государственный технический университет, e-mail: myvnn@list.ru; г. Ростов-на-Дону, Площадь Гагарина, 1; тел.: 88632738510; кафедра автоматизации производственных процессов; д.т.н.; профессор.

Венцов Николай Николаевич – e-mail: vencov@list.ru; тел.: 88632738582; кафедра информационных технологий; к.т.н.

Chernyshev Yury Olegovich – Don State Technical University; e-mail: myvnn@list.ru; 1, Gagarin square, Rostov-on-Don, Russia; phone: +78632738510; the department of automation of productions; dr. of eng. sc.; professor.

Ventsov Nikolay Nikolaevich – e-mail: vencov@list.ru; phone: +78632738582; the department of information technologies; cand. of eng. sc.; associate professor.

УДК 004.056.5 DOI 10.23683/2311-3103-2019-4-68-80

С.А. Хованскоов, В.А. Литвиненко, В.С. Хованскова

МЕТОДИКА ЗАЩИТЫ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ В МНОГОАГЕНТНОЙ СИСТЕМЕ*

Рассматривается организация и защита распределенных вычислений на основе многоагентной системы для решения задач многовариантного моделирование. При моделировании выбор одного из многих вариантов может потребовать перебора огромного множества параметров недоступного для быстродействующей ЭВМ. Длясокращение времени решения таких задач используют распределенные вычисления. Существует множество различных подходов для организации распределенных вычислений в компьютерной сети - технология grid, metacomputing (BOINC, PVM и другие). Основным недостатком большинства существующих подходов является то, что они предназначены для создания централизованных систем распределенных вычислений. Распределенные вычисления организуются на основе многоагентной системы на вычислительных узлах любой компьютерной сети. При использовании в качестве вычислительной среды компьютерную сеть большого масштаба могут возникнуть угрозы безопасности распределенных вычислений со стороны злоумышленников. Одной из таких угроз является получение в процессе вычислений ложного результата злоумышленником. Ложный результат может привести в процессе моделирования к принятию не оптимального, либо неправильного решения. Разработан метод защиты распределенных вычислений на основе много-

* Работа выполнена при поддержке РФФИ (проект № 18–01–00041).

агентной системы от угрозы получения ложного результата. Выполнены оценки степени обеспечения информационной безопасности в многоагентных системах с различной структурой. Проведено сравнение обеспечения информационной безопасности для этих систем.

Распределенные вычисления; многоагентная система; защита результатоввычислений; сокращение времени решения; многовариантное моделирование.

S.A. Khovanskov, V.A. Litvinenko, V.S. Khovanskova

METHODS OF PROTECTION OF DISTRIBUTED COMPUTING IN A MULTI-AGENT SYSTEM

The organization and protection of distributed computing based on a multi-agent system for solving problems of multivariate modeling is considered. When modeling, the choice of one of many options may require a search of a huge set of parameters unavailable for a high-speed computer. Distributed computing is used to reduce the time required to solve such problems. There are many different approaches to the organization of distributed computing in a computer network - grid technology, metacomputing (BOINC, PVM and others). The main disadvantage of most existing approaches is that they are designed to create centralized distributed computing systems. Distributed computing is organized on the basis of a multi-agent system on the computing nodes of any computer network. When used as a computing environment a computer network on a large scale can cause threats to the security of distributed computing from the intruders. One of these threats is getting the calculation about the result by the attacker. A false result can lead in the modeling process to the adoption of not optimal or wrong decision. A method of protection of distributed computing based on a multi-agent system from the threat of false results is developed. The assessment of the degree of information security in multi-agent systems with different structure. Comparison between information securities in these two systems is provided.

Distributed computing; multi-agent system; protection of computing results; reduction of solution time; multivariate modeling.

Введение. В настоящее время множество задач требуют выполнения большого объёма вычислений за минимальное время. К ним относятся задачи моделирования.

На практике задачи моделирования требуют выбора наилучших решений не по одному, а сразу по нескольким критериям (многокритериальные задачи оптимизации), которые привносят дополнительные и не всегда разрешимые трудности. Если объект и его параметры являются переменными, зависящими от времени, то в этом случае используются более сложные стратегии решения задач моделирования [1–7].

Выбор одного из многих вариантов может потребовать перебора огромного параметров, недоступного даже для самой быстродействующей ЭВМ. Подсчитано, например, что при решении задачи распределения 20 критериев по 10 объектам число возможных вариантов составит 10^8. Даже если расчёт каждого варианта потребует всего 10 арифметических операций, то и тогда общее число расчётных операций достигнет миллиарда, что не может быть выполнено ЭВМ в приемлемые сроки.

Самым популярным решением этой проблемы в настоящее время является использование распределённых вычислений. В качестве вычислительной среды для организации распределенных вычислений была выбрана глобальная компьютерная сеть, обладающая значительными вычислительными ресурсами. Главным недостатком использования глобальной сети являются существующие в ней угрозы информационной безопасности распределенных вычислений [8–10].

Основными причинами уязвимости организуемых распределенных вычислений является наличие центров организации и управления вычислительными процессами в системе. В настоящее время для защиты централизованных систем распределенных вычислений разработаны различные методы обеспечения информационной безопасности, такие как использование балльной оценки доверия, концепция «Полицейского управления», концепция идентификации и игнорирования блокировки хостов и др. [12–19]. Однако эти подходы требуют длительного исследования управляющими центрами результатов работы ограниченного множества компьюте-

ров и накопления полученной информации в своих базах. В случае использования нестабильной вычислительной среды такая защита бесполезна, а, кроме этого, само наличие центров делают систему уязвимой. Для организации распределенных вычислений в нестабильной вычислительной среде в настоящей работе предлагается использовать менее уязвимую децентрализованную распределенную вычислительную систему и разработанный метод защиты распределенных вычислений на основе многоагентной системы от угрозы получения ложного результата.

Постановка задачи. Основными задачами, решаемыми авторами было:

- создать метод, позволяющий свести к минимуму подготовительные этапы для решения любой задачи многовариантного моделирования;
- использовать в качестве вычислительных центров для решения конкретного вычислительного блока узлы обычной масштабируемой компьютерной сети;
- оптимизировать время выполнения задачи за счёт оптимизациивычислительной нагрузки компьютера в соответствии с его вычислительными ресурсами.

В то же время создаваемая система должна быть работоспособной при любом наборе компьютеров, как по количеству, так и по производительности, обладать высокой живучестью – не терять работоспособность и выполнять решение за отведённые под задачу временные ресурсы при динамическом изменении используемой вычислительной среды.

В качестве наиболее перспективного пути организации распределённых вычислений в компьютерной сети было выбрано использование многоагентной системы [11–13].

Многоагентная система. Под многоагентной системой понимаетсямножество агентов, каждый из которых представляет программный модульразмещенный на отдельном компьютере. Все агенты образуют одноранговый набор и работают по одному и тому же алгоритму. Каждый агент выполняет управление своим компьютером и его работа не зависит от других компьютеров. Агент организует выполнение вычислительной нагрузки на своём компьютере, инициирует обмен данными с другими агентами, выполняет обработку полученной от других агентов информации и на её основе принимает решения.

Для реализации и защиты распределенных вычислений в компьютерной сети разработан алгоритм работы агента многоагентной системы, который позволяет организовать распределенную вычислительную систему на основе узлов компьютерной сети [14–16].

Реализация многоагентной системы. Сформулируем требования к алгоритму работы системы:

Система должна быть децентрализованной – каждый агент должен обладать равными правами и иметь возможность обмениваться сообщениями с другими агентами:

- агент должен следить за вычислительными процессами, выполняемыми на управляемом им компьютере;
- агенты должны самостоятельно распределять между собой вычислительную нагрузку;
- каждый агент должен хранить все результаты выполнения большеобъемной задачи;
- многоагентная система должна обеспечивать безопасность распределенных вычислений от угроз со стороны злоумышленников.

Для организации распределенных вычислений в компьютерной сети и реализации требований был разработан алгоритм, содержащий ***ряд правил,*** которые должен выполнять каждый агент.

Многоагентная система представляет собой множество агентов M в виде одинаковых программных модулей агентов $\{m_1,m_2, \ldots, m_n\} \in \mathrm{M}$ [11–16]. Множество M накладывается на множество $\{p_1, p_2, \cdots, p_j\} \in P$ сетевых компьютеров *(P>M)* так, что агент m_i располагается на соответствующем p_i компьютере сети. Каждый модуль агента $m_i \in M$ (агент) управляет ресурсами компьютера p_i и следит за выполняемой на нем нагрузке W_i. Вся многоагентная система M, управляя компьютерами $\{p_1, p_2, \cdots, p_\mathrm{n}\} \in P$, организует систему распределенных вычислений для решения всего множества заданий $\{w_1, w_2, \cdots, w_\mathrm{n}\} \in W$. Множество M является одноранговым набором агентов, работающих по одной программе (рис. 1).

В начале организации распределённых вычислений в компьютерной сети P на $\{p_1, p_2, \cdots, p_\mathrm{n}\} \in P$ находятся управляющие их работой агенты $\{m_1, m_2, \ldots, m_n\} \in M$. На первом этапе агент $m_i \in M$, получает основную информацию для организации распределенных вычислений в множестве M. Она включает в себя вычислительную нагрузку W системы M и указание того, какую часть w_i из общего объема W агент должен выполнить. Для отслеживания процесса выполнения вычислительной нагрузки каждый агент для работы имеет две таблицы: первая таблица W_{nrez} включает в себя все невыполненные задания, а вторая таблица W_{rez} включает выполненные задания с результатами выполнения $\{W_{nrez}, W_{rez}\} \in W$.

На первоначальном этапе организации распределённых вычислений в компьютерной сети $w_i \subseteq W$.

После получения агентом $m_i \in M$ нагрузки и общей информации о системе он инициирует на своем компьютере p_1 вычислительный процесс для выполнения w_{i1}, выполняя действия в соответствии с правилом выполнения вычислительной нагрузки.

Агент состоит из нескольких программных модулей, которые взаимодействуют друг с другом и обеспечивают выполнение распределенных вычислений в глобальной сети (рис. 1).

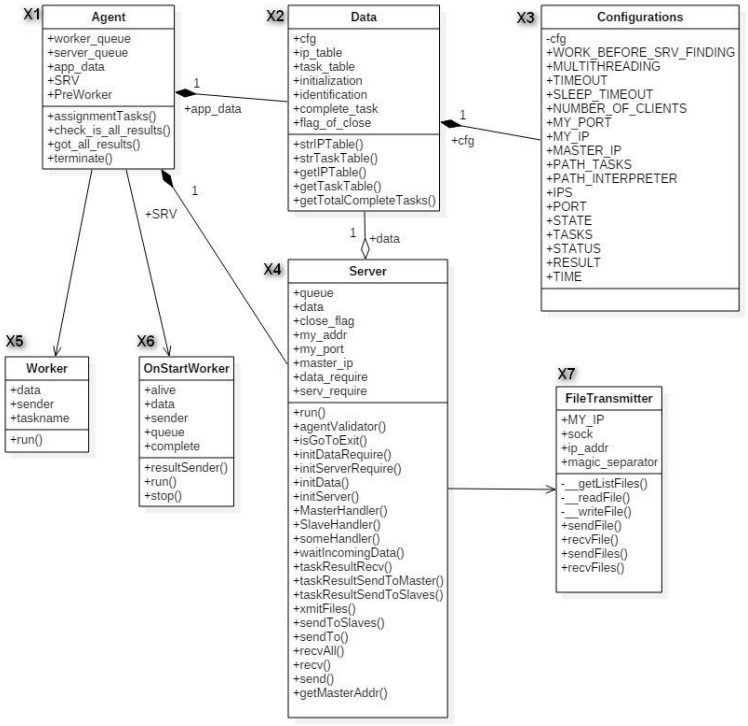

Рис. 1. Структура программы агента многоагентной системы

Угрозы информационной безопасности в многоагентной системе. При организации распределенных вычисление в компьютерной сети большого масштаба велика вероятность нарушения безопасности вычислений со стороны злоумышленников [11–13, 17–21].

Одними из наиболее вероятных нарушений являются следующие:

- ♦ перехват сетевого трафика, содержащего результаты вычислений, и подмена правильных результатов ложными;
- ♦ заражение вычислительного узла вредоносными программами и изменение алгоритма работы программного модуля агента;
- ♦ включение в многоагентную систему одного или нескольких компьютеров с целью нарушения безопасности распределенных вычислений путем подмены результатов вычислений, полученных ими на ложные.

Первый случай, связанный с передачей сетевого трафика от некоторых агентов через компьютер злоумышленника. Перехват трафика с целью получения информации не является серьезной угрозой безопасности распределенных вычислений, поскольку результаты вычислений не являются конфиденциальными данными и создаются только при разовом процессе моделировании.

Во втором и третьем случаях угрозы «нарушения целостности данных» могут привести к формированию неправильных или ложных результатов, что может стать причиной принятия неправильного или неэффективного решения на основании результатов полученных вычислений.

Степень защиты безопасности распределенных вычислений зависит от вида организации многоагентной системы. Существует два варианта организации многоагентной системы: централизованная система и децентрализованная. Каждая из них имеет свои достоинства и недостатки, которые, так или иначе, влияют на безопасность работы системы в сети от угроз типа «нарушение целостности данных».

Защита от угрозы информационной безопасности в многоагентной системе с централизованным управлением. В централизованных многоагентных системах один или несколько агентов выполняют роль центров управления. При централизованной системе организация распределенных вычислений и сбор результатов вычислений выполняется одним агентом. Так проще организовать распределенные вычисления поскольку один центральный агент контролирует весь процесс распределения нагрузки между агентами и собирает результаты.

Его основной задачей является организация распределенных вычислений, которые будут выполняться в компьютерной сети [14]. От его работоспособности зависит безопасность всего процесса распределённых вычислений.

Вместе с этим в компьютерной сети существует высокая вероятность не только нарушения работоспособности управляющего компьютера, но и получения им ложных результатов от других вычислительных узлов.

При организации распределенных вычислений в компьютерной сети такая угроза «нарушения целостности данных» является наиболее существенной и опасной из всех угроз существующих в глобальной сети. Вцентрализованной системе функции безопасности возложены на управляющего агента.

Для защиты результатов распределенной централизованной вычислительной системы от ложных результатов управляющий агент должен проверять все полученные результаты от агентов, но из-за ограниченности его вычислительных ресурсов он не может обеспечить надежную защиту.

В многоагентной системе выбор нового агента – случайный процесс. Поэтому в любой компьютерной сети велика вероятность внедрения в многоагентную систему компьютеров злоумышленников под видом легального агента и нарушения ими

безопасности распределенных вычислений путем замены результатов вычислений на ложные. В централизованной многоагентной системе вероятность необнаружения ложных результатов при большом количестве агентов очень высока.

Защита от угрозы информационной безопасности в предлагаемой децентрализованной многоагентной системе. При организации децентрализованной многоагентной системы для создания системы распределенных вычислений в качестве агента многоагентной системы может быть использован любой компьютер в сети. При этом выбор компьютера, включаемого в многоагентную систему, является случайным процессом [14–16].

Такой способ организации системы может привести к тому, чтопри распределении общей вычислительной нагрузки, между всеми агентамив децентрализованной многоагентнойсистеме, в качестве агента могут быть задействованы компьютеры любых пользователей, в том числе и злоумышленников. Такая децентрализованная многоагентная система является однороднойпоэтому различить компьютеры злоумышленников и обычных пользователей в ней невозможно.

В централизованной многоагентной системе могут быть использованы такие средства защиты как:

- шифрование передаваемой информации;
- определение заранее степени доверенности к используемому вычислительному узлу;
- ограничение количество используемых вычислительных узлов строго определённой группой компьютеров.

Для защиты распределенных вычислений, на основе децентрализованной многоагентной системы, такие средства являютсянеэффективными, поскольку процесс выбора компьютера для создания и расширения многоагентной системы является случайным.

Например, использование шифрования передаваемой информации между агентами не обеспечивает защиту передаваемой информации, поскольку при масштабировании многоагентной системы каждому компьютеру вместе с модулем агента и информацией по вычислительной нагрузке должна быть передана одна и та же информация, в том числе и шифр.

Ограничение количества компьютеров используемых для организации распределенных вычислений узким кругом «доверенных» компьютеров накладывает жесткое ограничение на степень распараллеливания вычислительных процессов, что также может привести к значительному увеличению времени выполнения вычислительной нагрузки.

В качестве защиты от угрозы изменения правильныхрезультатов вычислений на ложные предлагается использовать метод защиты, основанный на проверке правильности выполнения вычислительной нагрузки всеми агентами.

Вычислительный процесс на основе на многоагентной системы организуется таким образом, чтобы результат решения вычислительной нагрузки каждого агента проверялся на правильность другими агентами. Для этого необходимо организовать распределение вычислительной нагрузки так, чтобы вычислительный процесс каждого задания выполнялся не одним, а несколькими агентами. При этом вычислительная нагрузка на многоагентную систему увеличивается, но за счет возможности масштабирования многоагентной системы, это должно незначительно отразиться на быстродействии системы распределенных вычислений, а безопасность распределенных вычислений повысится.

Для реализации предлагаемого метода защиты в создаваемой децентрализованной системе был изменён алгоритм распределения вычислительной нагрузки между агентами. Алгоритм обеспечивает контроль правильности полученных результатов за счёт проверки процессов вычисленийдругими агентами.

Разработанный алгоритм работы агента многоагентной системы позволяет обнаруживать нарушение правильности полученных результатовв следствиипередачи злоумышленниками ложных результатов другим агентам.

Сравнение вероятности необнаружения ложного результата в централизованной и децентрализованной многоагентных системах. Для сравнения степени обеспечения безопасности распределенных вычислений, организованных в централизованной и децентрализованной многоагентных системах, сравнимобеспечиваемую имивероятность необнаружения ложных результатов. Чем меньше эта вероятность, тем более защищенными будут результаты организованных распределенных вычислений.

Сумма вероятностей обнаружения ложных результатов P_{olr} и необнаружения P_{nolr} равна $P_{olr} + P_{nolr} = 1$, поскольку вероятность необнаружения ложных результатовP_{nolr} – это величина, обратная вероятности их обнаружения, которая рассчитывается по формуле

$$P_{nolr} = 1 - P_{olr} = 1 - \frac{(\frac{W}{N})!}{m!*(\frac{W}{N}-m)!} * (\frac{1}{N})^m * (1 - \frac{1}{N})^{\frac{W}{N}-m}. \quad (1)$$

Рассчитаем по формуле (1) вероятность необнаружения ложных результатов при одном злоумышленнике в централизованной многоагентной системе состоящей изразном (от 100 до 10000) количестве агентов *N*. Вероятность необнаружения хотя бы 1, одновременно 2 и 3 ложных результатов при выполнении распределённых вычислений в многоагентной системе отображено на графике (рис. 2).

Приведённый график (рис. 2) наглядно показывает, что безопасность результатов вычислений в централизованной многоагентной системе низкая и угроза необнаружения ложных результатах при увеличении количества агентов существенна, то есть, $P_{nolr} \approx 1$.

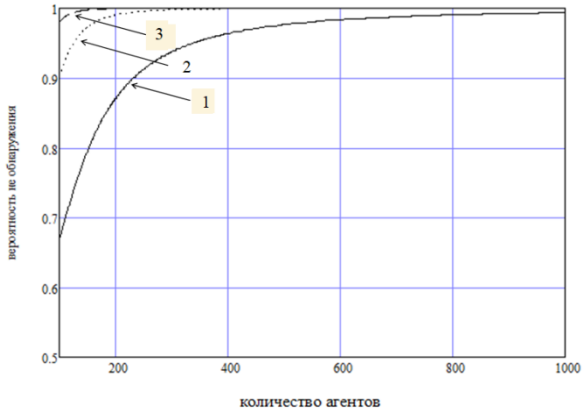

Рис. 2. Вероятности необнаружения одного (1), двух (2) или трех (3) ложных результатов в централизованной многоагентной системе с одним управляющим агентом

Чем больше *N* в многоагентной системе *M*, тем меньше общее время выполнения большеобъемной задачи, а вероятность P_{nolr} необнаружения ложных результатов при $N \to \infty$ $P_{nolr} \to 1$. В централизованной многоагентной системе увеличение количества управляющих агентов снижает вероятность необнаружения ложных результатов (рис. 3).

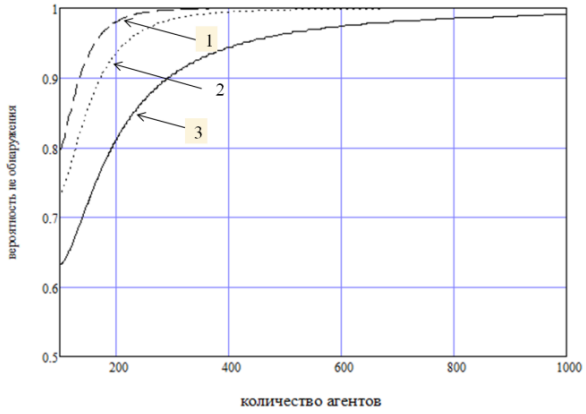

Рис. 3. Вероятность необнаружения ложных результатов в централизованной многоагентной системе с двумя (1), тремя (2), четырьмя (3) управляющими агентами при двух злоумышленниках, вероятность появление ошибки P = 0,6

Из графика (см. рис. 3) можно сделать вывод, что вероятность необнаружения ложных результатов снижается с увеличением количества управляющих агентов, что повышает степень защиты распределенных вычислений.

Однако недостатком увеличения количества управляющих агентов в централизованной многоагентной системе является необходимость усложнения алгоритма взаимодействия управляющих агентов между собой. Это приводит к снижению эффективности применения многоагентной системы для организации распределенных вычислений.

В децентрализованной многоагентной системе порядок организация распределенных вычислений отличается от централизованной, поскольку здесь нет управляющих агентов, которые бы обеспечивали и контролировали организацию распределенных вычислений. С точки зрения обеспечения безопасности результатов распределённых вычислений, основным отличием является организации проверки результатов вычислительного процесса каждого задания. Для того чтобы повысить вероятность обнаружения ложного результата, проверки результатов распределенных вычислений должны выполнять разные агенты.

Это повышает вероятность обнаружения ложных результатов. Если в многоагентную систему попадет злоумышленник и вместо правильных результатов выполнения своей вычислительной нагрузки *Wi* начнёт передавать ложные результаты, то результаты *Wi*, полученные другими агентами, позволят выявить неправильность результатов и, таким образом, обеспечить защиту распределенных вычислений от ложных результатов.

Если в многоагентной системе несколько злоумышленников, то в этом случае возможно необнаружения ложных результатов. Такое нарушение безопасности может произойти только тогда, когда выполнение *Wi* и результаты их проверки будут получены агентами, расположенными на компьютерах злоумышленников.

Рассмотрим для децентрализованной многоагентной системы вероятность нарушение безопасности при параметрах системы аналогичных рассмотренному случаю необнаружения ложных результатов в централизованной многоагентной системе (рис. 2, 3).

График вероятности необнаружения ложных результатов P_{nolr} в децентрализованной многоагентной системе приведен на рис. 4.

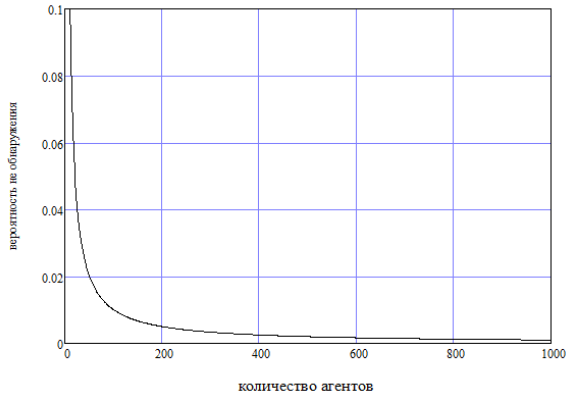

Рис. 4. Вероятность необнаружения ложных результатов в децентрализованной многоагентной системе с двумя злоумышленникамив зависимости от количества агентов в системе M

График построен для различного количества в системе агентов от 5 до 1000. На графике (см. рис. 4) показно, что вероятность необнаружения ложных результатов децентрализованной многоагентной системой значительно меньше, чем в централизованной. При этом, благодаря разработанному методу организации системы распределенных вычислений, вероятность необнаружения в децентрализованной многоагентной системе, в отличие от централизованной, с увеличением количества агентов в системе снижается (рис. 5).

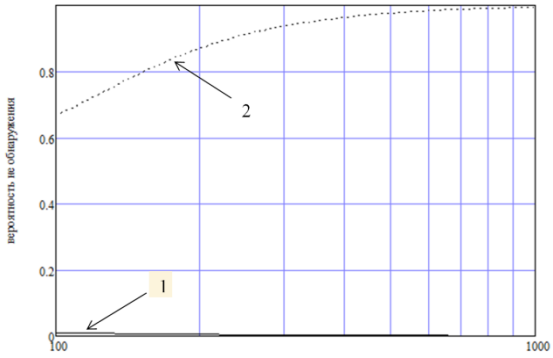

Рис. 5. Вероятность необнаружения ложных результатов в многоагентных системах с разным количеством агентов: 1 – децентрализованной; 2 – централизованной

Данные, полученные при формировании графиков (см. рис. 5) для сравнения вероятностей необнаружения ложных результатов в централизованной и в децентрализованной многоагентных системах показывают, что в децентрализованной системе вероятность необнаружения при увеличении количество агентов системы меньше, чем в централизованной. Для более детального анализа полученных данных для централизованной и децентрализованной системам сформирована табл. 1, содержащая вероятности необнаружения при различных размерах многоагентной системы.

Таблица 1

Количествоагентов	Вероятность необнаружения многоагентной системой		Во сколько раз
	централизованная	децентрализованная	
100	0.671999	0.010000	67,1999
200	0.870534	0.005025	173,2406
300	0.937901	0.003355	279,5532
400	0.963651	0.002518	382,7049
500	0.976402	0.002016	484,3264
600	0.983159	0.001680	585,2137
700	0.988048	0.001440	686,1444
800	0.990265	0.001261	785,3013
900	0.992658	0.001121	885,5112
1000	0.993984	0.001009	985,1179

На основании полученных результатов можно сделать вывод, что при небольшом количестве агентов в многоагентной системе (от 10 до 200 агентов) и количестве 10000 заданий разница в вероятностях необнаружения ложных результатов централизованной и децентрализованной вычислительных систем составляет порядка от 19 до 173 раз, то есть, даже при таком небольшом количестве агентов, децентрализованная система лучше обеспечивает защиту безопасности распределенных вычислительных систем от ложного результата, чем централизованная система.

Заключение. В настоящей работе для организации распределенных вычислений в нестабильной вычислительной среде предложен метод защиты распределенных вычислений от угрозы получения ложного результата на основе многоагентной системы для его использования в децентрализованной распределенной вычислительной системе.

В отличии от известных методов организации централизованных распределенных вычислительных систем, возможности вычислительных мощностей которых весьма ограничены, разработанный метод позволяет организовать распределенные вычисления на любом доступном количестве вычислительных узлов без потери времени на отбор надежных вычислительных узлов, а также позволяет динамически масштабировать вычислительные ресурсы создаваемой системы в процессе выполнения вычислений при изменении используемой вычислительной среды. Программная реализация разработанного метода организации распределенных вычислений на основе многоагентной системы, предназначенных для сокращения времени решения большеобъемных задач, показала свою работоспособность в такой неустойчивой вычислительной среде как глобальная сеть интернет.

Разработанный метод создания самоорганизующейся децентрализованной вычислительной системы позволяет также обеспечить более высокую степень информационной безопасности вычислительных процессов и результатов вычислений по сравнению с централизованной распределенной вычислительной системой. С использованием разработанной математической модели рассчитана вероятность обнаружение ложного результата распределенных вычислений в централизованной и в предлагаемой децентрализованной вычислительных системах. Сравнение вероятностей обнаружение для этих систем показало, что использование децентрализованной распределенной вычислительной системе на основе многоагентной системы позволяет снизить уязвимость организуемых распределенных вычислений даже при небольшом количестве агентов и обеспечить преимущество использования децентрализованной системы для обеспечения защиты безопасности распределенных вычислительных систем от ложного результата по сравнению с централизованной системо.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Курейчик В.М., Лебедев Б.К., Лебедев О.Б.* Разбиение на основе моделирования адаптивного поведения биологических систем // Нейрокомпьютеры: разработка, применение. – 2010. – № 2. – С. 28-34.
2. *Котенко В.В., Румянцев К.Е., Котенко С.В.* Идентификационный анализ в информационно-телекоммутационных системах: монография. – Ростов-на-Дону: Изд-во ЮФУ, 2014.
3. *Радченко Г.И.* Распределенные вычислительные системы: учеб. пособие. – Челябинск: Фотохудожник, 2012. – 184 с.
4. *Кравченко Ю.А.* Метод построения имитационных моделей принятия решений на основе многоагентных технологий. – Известия ЮФУ. Технические науки. – 2010. – № 7 (108). – С. 119-125.
5. *Таненбаум Э.* Распределенные системы: принципы и парадигмы. – СПб: Питер, 2003. – 877 с.
6. *Лебедев Б.К., Воронин Е.И.* Многоуровневый подход к решению задачи трассировки по всему чипу с использованием модификаций муравьиного алгоритма // Известия ЮФУ. Технические науки. – 2010. – № 7 (120). – С. 73-80.
7. *Чернышев Ю.О., Венцов Н.Н.* К вопросу о построении деревьев Штейнера с различной шириной ветвей для связывания элементов трехмерных СБИС // Известия ЮФУ. Технические науки. – 2009. – № 4 (93). – С. 72-76.
8. *Щеглов К.А., Щеглов А.Ю.* Защита от атак на повышение привилегий // Вестник компьютерных и информационных технологий. – 2015. – № 1. – С. 36-42.
9. *Громов Ю.Ю., Драчев В.О., Иванова О.Г.* Информационная безопасность и защита информации: учеб. пособие. – Ст. Оскол: ТНТ, 2017. – 384 с.
10. *Родичев Ю.А.* Нормативная база и стандарты в области информационной безопасности. – СПб.: Изд-во Питер, 2017. – 256 с.
11. *Емельянов В.В.* Многоагентная модель децентрализованного управления производственными системами // Информационные технологии и вычислительные системы. – 1998. – № 1. – С. 69-77.
12. *Műller J., Fisher K.* Application Impact of Multiagent Systems and Technologies: A Survey // In Agent-Oriented Software Engineering book series. – Springer, 2013. – P. 1-26.
13. *Wooldridge M.* An introduction to multiagent systems. – New Jersey: Wiley, 2012. – 484 p.
14. *Хованских С.А., Норкин О.Р., Парфенова С.С., Хованскова В.С.* Алгоритмическое обеспечение распределённых вычислений с использованием иерархической вычислительной структуры // Информатизация и связь. – 2014. – № 2. – С. 71-74.
15. *Хованских С.А., Литвиненко В.А., Хованскова В.С.* Организация и защита распределенных вычислений на базе многоагентной системы в компьютерной сети с целью сокращения времени решения масштабных задач // Известия ЮФУ. Технические науки. – 2018. – № 4 (198). – С. 198-210.
16. *Хованских С.А., Литвиненко В.А., Хованскова В.С.* Алгоритм организации безопасных распределенных вычислений на основе многоагентной системы // Известия ЮФУ. Технические науки. – 2016. – № 10 (183). – С. 146-158.
17. *Chadha Zrari, Hela Hachicha, Khaled Ghedira.* Agent's security during communication in mobile agents system // 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems Procedia Computer Science. – 2015. – Vol. 60. – P. 17-26.
18. *Sugumaran S., Kumaravelu R.* Distribution of RSA Public Key with Security Device based Identity for Multi-Agent secured Distributed Computing System // IOSR Journal of Computer Engineering. – 2014. – Vol. 14, Issue 4, Ver. VII. – P. 62-66.
19. *Madkour A.M., Eassa F.E., Ali A.M., Qayyum N.U.* Securing Mobile-Agent-Based Systems Against Malicious Hosts // World Applied Sciences Journal. – 2014. – Vol. 29 (2). – P. 287-297.
20. *Muñoz A., Pablo A., Maña A.* Multiagent Systems Protection // Advances in Software Engineering. – 2011. – Article ID 281517. – 9 p. – Doi: 10.1155/2011/281517.
21. *Beydoun G. Low G. Mouratidis H. and Hendersonsellers B.* A security-Aware Metamodel for MultiAgent System (MAS) // Information and software technology. – 2009. – Vol. 51, No. 5. – P. 832-845.

REFERENCES

1. *Kureychik V.M., Lebedev B.K., Lebedev O.B.* Razbienie na osnove modelirovaniya adaptivnogo povedeniya biologicheskikh sistem [Division on the basis of modeling of adaptive behavior of biological systems], *Neyrokomp'yutery: razrabotka, primenenie* [Neurocomputers: development, application], 2010, No. 2, pp. 28-34.
2. *Kotenko V.V., Rumyantsev K.E., Kotenko S.V.* Identifikatsionnyy analiz v informatsionno-telekommutatsionnykh sistemakh: monografiya [Identification analysis in information and telecommunication systems: monograph]. Rostov-on-Don: Izd-vo YuFU, 2014.
3. *Radchenko G.I.* Raspredelennye vychislitel'nye sistemy: ucheb. posobie [Distributed computing systems: a textbook]. Chelyabinsk: Fotokhudozhnik, 2012, 184 p.
4. *Kravchenko Yu.A.* Metod postroeniya imitatsionnykh modeley prinyatiya resheniy na osnove mnogoagentnykh tekhnologiy [Method of construction of simulation models of decision-making based on multi-agent technologies], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2010, No. 7 (108), pp. 119-125.
5. *Tanenbaum E.* Raspredelennye sistemy: printsipy i paradigm [Distributed systems: principles and paradigms]. Saint Petersburg: Piter, 2003, 877 p.
6. *Lebedev B.K., Voronin E.I.* Mnogourovnevyy podkhod k resheniyu zadachi trassirovki po vsemu chipu s ispol'zovaniem modifikatsiy murav'inogo algoritma [Multi-level approach to solving the problem of tracing across the chip using modifications of the ant algorithm], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2010, No. 7 (120), pp. 73-80.
7. *Chernyshev Yu.O., Ventsov N.N.* K voprosu o postroenii derev'ev SHteynera s razlichnoy shirinoy vetvey dlya svyazyvaniya elementov trekhmernykh SBIS [On the construction of Steiner trees with different branch widths for linking elements of three-dimensional VLSI], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, No. 4 (93), pp. 72-76.
8. *Shcheglov K.A., Shcheglov A.Yu.* Zashchita ot atak na povyshenie privilegiy [Protection against attacks to increase privileges], *Vestnik komp'yuternykh i informatsionnykh tekhnologiy* [Bulletin of computer and information technologies], 2015, No. 1, pp. 36-42.
9. *Gromov Yu.Yu., Drachev V.O., Ivanova O.G*. Informatsionnaya bezopasnost' i zashchita informatsii: ucheb. posobie [Information security and data protection: a training manual]. St. Oskol: TNT, 2017, 384p.
10. *Rodichev Yu.A.* Normativnaya baza i standarty v oblasti informatsionnoy bezopasnosti [Regulatory framework and standards in the field of information security]. Saint Petersburg: Izd-vo Piter, 2017, 256 p.
11. *Emel'yanov V.V.* Mnogoagentnaya model' detsentralizovannogo upravleniya proizvodstvennymi sistemami [Multi-agent model of decentralized management of production systems], *Informatsionnye tekhnologii i vychislitel'nye sistemy* [Information technologies and computer systems], 1998, No. 1, pp. 69-77.
12. *Műller J., Fisher K.* Application Impact of Multiagent Systems and Technologies: A Survey, *In Agent-Oriented Software Engineering book series*. Springer, 2013, pp. 1-26.
13. *Wooldridge M.* An introduction to multiagent systems. New Jersey: Wiley, 2012, 484 p.
14. *Khovanskov S.A., Norkin O.R., Parfenova S.S., Khovanskova V.S.* Algoritmicheskoe obespechenie raspredelennykh vychisleniy s ispol'zovaniem ierarkhicheskoy vychislitel'noy struktury [Algorithmic support of distributed computing using hierarchical computational structure], *Informatizatsiya i svyaz'* [Informatization and communication], 2014, No. 2, pp. 71-74.
15. *Khovanskov S.A., Litvinenko V.A., Khovanskova V.S.* Organizatsiya i zashchita raspredelennykh vychisleniy na baze mnogoagentnoy sistemy v komp'yuternoy seti s tsel'yu sokrashcheniya vremeni resheniya masshtabnykh zadach [Organization and protection of distributed computing based on a multi-agent system in a computer network in order to reduce the time of solving large-scale tasks], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2018, No. 4 (198), pp. 198-210.
16. *Khovanskov S.A., Litvinenko V.A., Khovanskova V.S.* Algoritm organizatsii bezopasnykh raspredelennykh vychisleniy na osnove mnogoagentnoy sistemy [Algorithm of organization of secure distributed computing based on multi-agent system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 10 (183), pp. 146-158.

17. *Chadha Zrari, Hela Hachicha, Khaled Ghedira.* Agent's security during communication in mobile agents system, *19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems Procedia Computer Science*, 2015, Vol. 60, pp. 17-26.
18. *Sugumaran S., Kumaravelu R.* Distribution of RSA Public Key with Security Device based Identity for Multi-Agent secured Distributed Computing System, *IOSR Journal of Computer Engineering*, 2014, Vol. 14, Issue 4, Ver. VII, pp. 62-66.
19. *Madkour A.M., Eassa F.E., Ali A.M., Qayyum N.U.* Securing Mobile-Agent-Based Systems Against Malicious Hosts, *World Applied Sciences Journal*, 2014, Vol. 29 (2), pp. 287-297.
20. *Muñoz A., Pablo A., Maña A.* Multiagent Systems Protection, *Advances in Software Engineering*, 2011, Article ID 281517, 9 p. Doi: 10.1155/2011/281517.
21. *Beydoun G. Low G. Mouratidis H. and Hendersonsellers B.* A security-Aware Metamodel for MultiAgent System (MAS), *Information and software technology*, 2009, Vol. 51, No. 5, pp. 832-845.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.О. Чернышев.

Хованскoв Сергей Андреевич – Южный федеральный университет; e-mail: sah59@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634676616; кафедра информационной безопасности телекоммуникационных систем; доцент.

Хованскова Вера Сергеевна – e-mail: bepok2010@gmail.com; кафедра информационной безопасности телекоммуникационных систем; аспирантка.

Литвиненко Василий Афанасьевич – e-mail: litv_va@mail.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634371651; кафедра систем автоматизированного проектирования; доцент.

Khovanskov Sergey Andreevich – Southern Federal University; e-mail: sah59@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634676616; the department of information security of telecommunication systems; associate professor.

Khovanskova Vera Sergeevna – e-mail: bepok2010@gmail.com; the department of information security of telecommunication systems; postgraduate student.

Litvinenko Vasily Avanasjevich – e-mail: litv_va@mail.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +78634371651; the department of computer aided design; associate professor.