НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2017 Том 17 № 3 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2017 Vol. 17 No 3 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.056

МОДЕЛЬ БЕЗОПАСНОСТИ МОБИЛЬНЫХ МУЛЬТИАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ С КОЛЛЕКТИВНЫМ УПРАВЛЕНИЕМ

И.А. Зикратов[a], И.И. Викснин[a], Т.В. Зикратова[b], А.А. Шлыков[a], Д.И. Медведков[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[b] Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», Пушкин, 197045, Российская Федерация
Адрес для переписки: wixnin@cit.ifmo.ru

Информация о статье
Поступила в редакцию 15.02.17, принята к печати 27.04.17
doi: 10.17586/2226-1494-2017-17-3-439-449
Язык статьи – русский

Ссылка для цитирования: Зикратов И.А., Викснин И.И., Зикратова Т.В., Шлыков А.А., Медведков Д.И. Модель безопасности мобильных мультиагентных робототехнических систем с коллективным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 3. С. 439–449. doi: 10.17586/2226-1494-2017-17-3-439-449

Аннотация

Рассмотрена проблема построения механизмов защиты мультиагентных робототехнических систем от атак со стороны внедренных роботов-диверсантов. Исследован класс так называемых «мягких» атак, использующих перехват сообщений, формирование и передачу коллективу роботов дезинформации, а также осуществляющих иные действия, которые не имеют идентифицируемых признаков вторжения роботов-диверсантов. Предложена теоретическая модель безопасности для мультиагентных робототехнических систем, которая основана на зональной модели безопасности и модели полицейских участков для распределенных вычислительных систем. Основная идея предлагаемой субъектно-объектной модели разграничения доступа состоит в том, что в информационную систему, кроме сущностей субъект и объект, вводится логически самостоятельная сущность – полицейский участок, на которую, в соответствии с концепцией монитора безопасности обращений, возлагаются функции проверки легитимности доступа и (или) целостности транзакций пространственно распределенных в пределах региона субъектов и объектов. Таким образом, изначально гомогенную мультиагентную систему предлагается проектировать как гетерогенную, в которой, кроме агентов-исполнителей, вводятся агенты, предназначенные исключительно для решения задач безопасности: идентификации и аутентификации, разграничения доступа, генерации и распределения ключей и анализа локации местоположения агентов. Для решения последней задачи регион разбивается на несколько зон, для которых вводится зональная и межзональные процедуры безопасности. Работоспособность модели иллюстрируется примером ее использования при построении механизма защиты классической итерационной задачи распределения наряда сил роботов по нескольким целям. При этом показан порядок взаимодействия агентов с полицейскими участками своей зоны, а также реализация межзональной политики безопасности.

Ключевые слова

информационная безопасность, коллектив роботов, мультиагентные робототехнические системы, атака, уязвимость, модель информационной безопасности, распределенные киберфизические системы

SECURITY MODEL OF MOBILE MULTI-AGENT ROBOTIC SYSTEMS WITH COLLECTIVE MANAGEMENT

I.A. Zikratov[a], I.I. Viksnin[a], T.V. Zikratova[b], A.A. Shlykov[a], D.I. Medvedkov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
[b] N.G. Kuznetsov Naval Academy, Pushkin, 197045, Russian Federation
Corresponding author: wixnin@cit.ifmo.ru

Article info
Received 15.02.17, accepted 27.04.17
doi: 10.17586/2226-1494-2017-17-3-439-449
Article in Russian

For citation: Zikratov I.A., Viksnin I.I., Zikratova T.V., Shlykov A.A., Medvedkov D.I. Security model of mobile multi-agent robotic systems with collective management. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 3, pp. 439–449 (in Russian). doi: 10.17586/2226-1494-2017-17-3-439-449

Abstract

The paper deals with creation problem of protection mechanisms for multi-agent robotic systems from attacks by introduced robots-saboteurs. We considered a class of so-called "soft" attacks that involve intercepting of communications, formation

and transmission of misinformation to robots group, as well as performing other actions that do not have identified signs of robots-saboteurs invasion. We proposed theoretical security model for multi-agent robotic systems, based on zone security model and model of police stations for distributed computing systems. The basic idea of the proposed subject-object model of access control, is that a logically self-contained entity, the police station, is introduced in information system, in addition to the entities "subject and object". In accordance with the concept of security monitoring of appeals, it performs the functions of access legitimacy checking and/or integrity of the transactions spatially distributed within a region of subjects and objects. Thus, initially homogeneous multi-agent system is proposed to be designed as heterogeneous, where there are not only agents-executors, but also agents, intended solely for the decision of security problems: identification and authentication, access control, generation, and key distribution and location analysis of agents' position. For the latter problem solution, the region is divided into several zones with introducing of zonal and interzonal security procedures. The performance of the model is illustrated by an example of its usage in the protection mechanism creation for classical iterative task of robot forces distribution for several purposes. We show the order of agents' interaction with the police stations of their zone, as well as implementation of interzonal security policy.

Keywords
information security, robots group, multi-agent robotic systems, attack, vulnerability, information security model, distributed cyber-physical systems

Введение

Развитие телекоммуникационных систем и их интеграция с физическими объектами окружающего мира приводят к появлению новых моделей информационных систем, основанных на парадигме Индустрии 4.0. К таким системам можно отнести мультиагентные киберфизические системы, ярким примером реализации которых являются мультиагентные робототехнические системы (МРТС). Отличительной особенностью МРТС является возможность пространственного перемещения элементов системы в процессе выполнения задачи. Представителями МРТС являются, в частности, коллективы беспилотных летательных аппаратов, наземных беспилотных транспортных средств, беспилотные суда и т.д., действующие совместно для достижения общей цели [1].

В то же время особенности построения и функционирования МРТС, такие как децентрализация управления, пространственная удаленность киберфизических устройств (агентов) и нахождение их вне пределов контролируемой территории, необходимость использования телекоммуникационных технологий для обмена информацией между информационными объектами, ограниченность их представления о системе, а также непредсказуемая динамика внешней среды, делают МРТС максимально уязвимой для специфических угроз, источником которых могут являться физическое внедрение «инородных» агентов (диверсантов) [2–4].

Эти особенности МРТС затрудняют применение известных моделей разграничения доступа на основе дискреционной политики [5], мандатной политики [6] и других видов политик безопасности [7, 8].

Вместе с тем в последние годы с развитием распределенных мультиагентных вычислительных систем (МАС) появились новые модели безопасности, основанные на зональной модели разграничения доступа в распределенных системах [9], модели полицейских участков (Police Office Model, POM), предложенной Ксюдонгом в работе [10], и модели безопасности, основанные на оценке доверия и (или) репутации агентов [11–13], которые хорошо согласуются с принципами построения децентрализованных систем.

Системы доверия и репутации основаны на расчете величины доверия агентов друг к другу, осуществляемой в процессе мониторинга действий агента в системе [14]. Различие в подходах к вычислению уровня доверия обусловлено, как правило, особенностями среды, в которой происходит взаимодействие участников. Это могут быть электронные рынки, пиринговые сети, онлайновые социальные сети, мультиагентные робототехнические системы и т.п. Как следствие, в существующих моделях доверия имеются различные трактовки понятий доверие и репутация, рассматриваются различные субъекты и объекты доверия. При всех достоинствах таких моделей безопасности существенным их недостатком является необходимость в дополнительных затратах ресурсов агентов на выполнение функций безопасности.

POM относится к моделям с так называемым централизованным принципом управления безопасностью. Суть централизованных механизмов информационной безопасности (ИБ) в МАС состоит в том, что МАС разбивается на несколько областей (хостов), в каждом из которых имеется модуль, осуществляющий функции идентификации и аутентификации агентов, а также анализирующий их деятельность. Наличие такого модуля освобождает агентов от выполнения функций безопасности всей системы.

Очевидно, что правила выделения областей и МАС, а также порядок взаимодействия членов коллектива с полицейскими участками имеют существенные особенности при их реализации в МРТС, что обусловлено размещением элементов системы на отдельных физических объектах, которые способны перемещаться в пространстве. На текущий момент применение POM ограничивается использованием в традиционных распределенных компьютерных системах. С учетом развития технологий, входящих в подход «Индустрия 4.0», разработка POM для одной из парадигм данного подхода представляется актуальной задачей. Требуется провести теоретическое обоснование особенностей построения POM для МРТС, с учетом указанных выше особенностей построения и функционирования данного вида телеком-

муникационных систем. Предложены модели РОМ для МРТС и рекомендации для реализации РОМ, обеспечивающих ИБ МРТС.

Принципы работы мультиагентных робототехнических систем с коллективным управлением

Рассмотрим действия МРТС при использовании наиболее распространенной итерационной процедуры оптимизации коллективного решения [15].

Пусть в составе МРТС, действующей в пределах региона H, имеется множество R роботов-агентов. В начале работы всем роботам коллектива поступают исходные данные, необходимые для решения оптимизационной задачи по достижению цели, стоящей перед МРТС. Каждый робот $r \in R$ обладает своим процессорным устройством (ПУ). Процессорное устройство связано с ПУ других роботов по каналам связи, по которым передается информация о текущих состояниях F_i^0 остальных роботов и выбираемых ими в процессе выполнения итерационной процедуры действиях A_j^{k+1}, (k=0,1,2,…).

В каждой итерации ПУ одного из агентов, получающего по очереди право управления, на основе информации о своем состоянии F_j^0, о состоянии части региона h^0, в пределах которого он находится, а также на основе информации, полученной от других агентов на предыдущих шагах итерационной процедуры, вычисляет значение приращения целевого функционала ΔY для всех возможных допустимых действий в текущей ситуации, и в качестве нового действия A_j^{k+1} выбирает то, для которого значение ΔY максимально. Выбрав действие, активный агент посредством каналов связи передает информацию остальным членам коллектива, которые на данной итерации являются пассивными агентами. Поочередно и циклически выполняя указанные процедуры, агенты последовательно получают право на доступ к формированию информационного потока и переводят систему из одного состояния в другое, добиваясь при этом искомого экстремального значения функционала Y. Такой обмен информацией между активными и пассивными агентами, приводящий к изменению состояния системы, будем называть транзакцией.

Исходя из приведенного описания функционирования, МРТС можно представить как систему, обладающую следующими свойствами:

- физической распределенностью элементов системы;
- дискретностью представления данных в цифровых вычислительных устройствах систем управления роботов;
- цикличностью вычислений;
- дискретностью по времени информации;
- наличием активных сущностей (сенсорные устройства, телекоммуникационные технологии и т.д.) для осуществления доступа транзакциям;
- наличием пассивных сущностей (оперативная память агентов, базы данных и т.п.).

Виды атак на МРТС. Постановка задачи

Предпосылками возникновения угроз для МРТС являются:

- пространственная удаленность элементов системы друг от друга и центров управления и мониторинга;
- возможность нахождения всего или части региона, в пределах которого МРТС выполняет задачу, вне границ контролируемой территории;
- использование агентами телекоммуникационных технологий для обмена информацией;
- возможность физического доступа злоумышленников к элементам системы (агентам);
- высокая вероятность попадания агентов в зону неустойчивого приема сигналов из-за естественных или искусственных помех;
- ограниченные возможности бортовых вычислительных систем и средств связи, обусловленные стремлением удешевления стоимости агентов и снижения их массогабаритных характеристик;
- слабая осведомленность агентов о состоянии всей системы.

Перечисленные факторы создают благоприятную среду для внедрения в состав коллектива агентов-диверсантов, наличие которых в системе приводит к появлению вредоносных информационных воздействий (атак), осуществляемых диверсантом на k-й итерации, когда он получает статус активного агента. Под атакой будем понимать выполнение роботами-диверсантами таких транзакций, которые приводят к модификации информации в системе, в результате которой выбранное легитимными агентами новое действие A_j^{k+1} не будет способствовать приращению целевого функционала ΔY МРТС в имеющихся условиях.

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

- перехват диверсантами сообщений агентов с последующей их модификацией и воспроизведением (атаки Man in the Middle);

– формирование и передача диверсантом ложных сведений (дезинформации) о своем состоянии, местоположении и выбранных действиях, направленных на уменьшение приращения целевого функционала ΔY;
– действия роботов-диверсантов, направленные на эксплуатацию уязвимостей алгоритмов коллективного управления, и т.д.

Очевидно, что указанные виды «мягких» атак не имеют четко идентифицируемых признаков, в отличие от так называемых «силовых атак», проводимых путем постановки помех, DDoS-атак, так как роботы, их системы и каналы связи функционируют в штатном режиме, и МРТС не в состоянии выявить факт воздействия атаки и снижения эффективности своих действий. В их основу положено внедрение диверсанта в состав МРТС под видом легитимного агента и генерация в системе различного вида транзакций, которые приводят к снижению эффективности принимаемых агентами решений.

Таким образом, с точки зрения процессов ИБ, трактуемой как состояние защищенности информации в пределах региона H, задача состоит в интеграции в робототехническую систему монитора безопасности, который:

1. имеет механизмы отслеживания текущего местоположения каждого агента;
2. разбивает множество всех доступов T субъектов к объектам на два непересекающихся подмножества T_L и T_N,
   $T = T_L \cup T_N, T_L \cap T_N = \emptyset$,
   где T_L – множество доступов, вызываемых легальными (безопасными) транзакциями; T_N – множество доступов, вызываемых агентами-диверсантами и нарушающих целостность информации в МРТС.

Следовательно, модель безопасности для робототехнических систем должна осуществлять физическую локацию агентов и описывать правила разграничения доступа физически удаленных субъектов к объектам, которые реализуются монитором безопасности региона H и представляют собой формально описанные доступы, принадлежащие множеству T_L.

Модель полицейских участков для мультиагентных робототехнических систем

Исходя из описания функционирования коллектива роботов в каждый фиксированный момент времени, на k-й итерации МРТС можно представить как конечное множество элементов $r \in R$, разделяемых на два подмножества:

1. подмножество субъектов доступа S;
2. подмножество объектов доступа O;
   где $S \cup O = R$.

Под субъектом доступа $s \in S$ в работе понимаются роботы-агенты, получившие на k-й итерации право доступа на запись, которые могут изменять состояние системы, выполняя транзакции в системе посредством своих активных сущностей.

Под объектом доступа $o \in O$ понимается пассивные на k-й итерации агенты, получившие право доступа на чтение данных.

Сформулируем основные положения модели РОМ для МРТС, базирующиеся на основных положениях модели Ксюдонга и зональной модели безопасности распределенных систем.

1. Основные сущности МРТС как объекта защиты:

– множество непересекающихся зон региона $H(h_1, h_2, \dots, h_M)$, в каждой из которых расположен полицейский участок (Police Office, PO);
– множество роботов-агентов $R(r_1, r_2, \dots, r_N)$.

Сегментация региона H на локальные сегменты (зоны) вызвана физической удаленностью элементов МРТС, и может осуществляться несколькими способами (критериями) обособления подмножества субъектов и объектов в локальный сегмент, например [8]:

– группирование некоторого подмножества субъектов доступа на основе их управления одним общим системным процессом;
– локализация некоторого подмножества субъектов и объектов доступа в рамках некоторой технической/физической компоненты МРТС;
– присвоение всем субъектам и объектам некоторого уникального идентификатора (адреса) в едином информационном (адресном) пространстве и разделение этого пространства на области, обособляющие локальные сегменты.

В произвольный момент времени все агенты $r \in R$ размещены в пределах региона H, причем каждый агент зарегистрирован на одном из полицейских участков в соответствии с некоторым правилом f:

$\forall r \in R \ \exists h \in H: r = f(h)$.

Например, если (x_i, y_i) – координаты i-го агента, $(x_j^{\min}, x_j^{\max}, y_j^{\min}, y_j^{\max})$ – координаты j-й зоны и $x_j^{\min} < x_i \le x_j^{\max}$ и $y_j^{\min} < y_i \le y_j^{\max}$, то агент r_i будет зарегистрирован на полицейском участке j-й зоны (рис. 1).

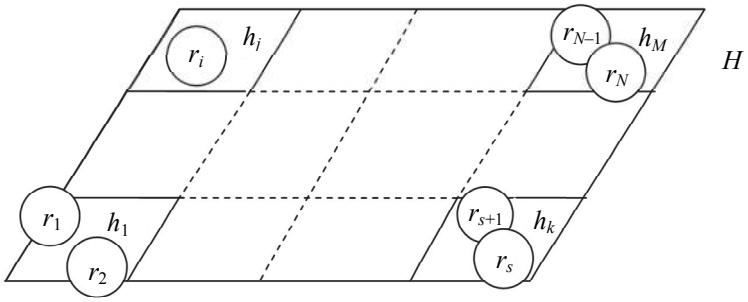

Рис. 1. Разделение региона на участки

2. Каждый робот-агент $r \in R$ концептуально имеет две составные части интерфейса. Открытая часть предназначена для взаимодействия с агентами МРТС в процессе выполнения коллективом поставленной задачи. Закрытая часть предназначена для взаимодействия агента с РО. Для закрытой и открытой частей интерфейса должны использоваться различные каналы связи.

3. В ходе итерационной процедуры роботы-агенты поочередно активизируются, получая статус субъектов доступа. Остальные члены коллектива на данной итерации являются объектами доступа.

4. Внутризональная политика безопасности реализуется РО зонами, которые обеспечивают весь набор функций безопасности (аутентификация, управление доступом и аудит процессов). Полицейским участком зоны назовем системный субъект (процесс), реализующий в отношении объектов зоны $h \in H$ разрешенное множество доступов $T_L(h)$, которое в общем виде является объединением внутризональных доступов, регламентированных правилами (критериями) внутризональной политики, и удаленных доступов агентов зоны к объектам других зон, а также агентов других зон к объектам данной зоны, разрешенных по правилам (критериям, процедурам) межзональной политики безопасности:

$T(h) = T_L^{in}(h) \cup T_L^{out}(h)$,

где $T_L^{in}(h)$ – множество безопасных внутризональных доступов; $T_L^{out}(h) = T_L^{out}(h \rightarrow) \cup T_L^{out}(h \leftarrow)$ – множество безопасных удаленных доступов для зоны $h \in H$, являющееся объединением множества удаленных доступов субъектов зоны h к объектам других зон $T_L^{out}(h \rightarrow)$ и множества удаленных доступов субъектов других зон к объектам зоны h – $T_L^{out}(h \leftarrow)$.

5. Совокупность взаимодействующих между собой посредством безопасного канала связи РО всех зон $h \in H$ образует монитор безопасности региона *H*. На монитор безопасности региона возлагается реализация межзональной политики безопасности. Канал связи будем называть безопасным, если он удовлетворяет следующим требованиям:

- устойчивостью к несанкционированному раскрытию или модификации передаваемой информации (безопасность связи);
- невозможностью отказов от доставки сообщения, неправильной доставки, доставки ошибочных данных (надежность связи);
- невозможностью изменений в критической информации (имитозащита);
- отсутствием скрытых каналов утечки информации за счет модуляции параметров канала.

Модель графически представлена на рис. 2.

6. Процессы внутризонального доступа субъектов к объектам своей зоны h организуются в три фазы:

- идентификация/аутентификация субъекта (поток *a*, рис. 2) $s \in S$ в зоне $h \in H$ под управлением внутризонального РО и порождение транзакции;
- запрос на доступ $T^{in}(h)$ субъекта s у внутризонального РО (поток *b*, рис. 2) к объектам $o \in O$ зоны *h*;
- получение доступа на осуществление транзакции в случае удовлетворения запрашиваемого доступа зональной политики безопасности (поток *c*, рис. 2). Если доступ признан легитимным, объекты $o \in O$ зоны *h* получают от РО соответствующую квитанцию (поток *d*, рис. 2), и транзакция осуществляется.

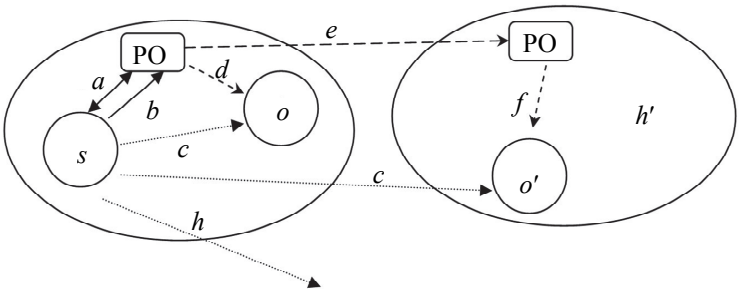

Рис. 2. Графическое представление модели РОМ для мультиагентных робототехнических систем

7. Процессы межзонального доступа субъектов к объектам «чужой» зоны h' организуются следующим образом:

- идентификация/аутентификация субъекта $s \in S$ в зоне $h \in H$ под управлением внутризонального РО (поток *a*, рис. 2) и порождение транзакции;
- запрос на доступ $T_L^{out}(h \rightarrow)$ субъекта *s* у внутризонального РО к объектам $o \in O$ зоны $h' \in H$;
- удаленное вхождение субъекта $s \in S$ в зону $h' \in H$ (поток *e*, рис. 2) под управлением полицейских участков зон h и h';
- получение доступа на осуществление транзакции (поток *b*, рис. 2 в случае удовлетворения запрашиваемого доступа $T_L^{out}(h \rightarrow)$ зональной политики безопасности (поток *c*, рис. 2).

Под удаленным вхождением субъекта $s \in S$ в зоне $h' \in H$ понимается обмен информацией между РО зон h и h' по безопасному каналу связи, в результате которого подтверждается легитимность запроса субъекта *s* на доступ $T_L^{out}(h \rightarrow)$, и объекты $o \in O$ зоны $h' \in H$ получают от РО своей зоны разрешение (поток *f* рис. 2) на доступ $T_L^{out}(h' \leftarrow)$ от субъекта зоны $h \in H$.

Проверим соответствие полученного результата поставленным задачам на примере реализации модели для классической задачи коллектива роботов – распределения роботов-агентов по нескольким целям. Функционирование МРТС при решении этой задачи в самом общем виде выглядит следующим образом.

Пусть имеется *M* целей и коллектив из *N* роботов. На каждую цель должен быть выделен некоторый, заранее известный наряд сил (число роботов, необходимых для выполнения задачи). После того, как какую-нибудь цель выберет необходимое число роботов, она считается обеспеченной. Оставшиеся роботы образуют резервный кластер. Роботу-агенту известны координаты целей, свои координаты и потребный наряд сил для каждой цели. Робот r_j оценивает эффективность своих действий по каждой цели, и сообщает массив своих оценок $D_j = [d_{j1}, \ d_{j2}, \ \ldots, \ d_{jM}]$ остальным членам коллектива. В качестве оценок могут выступать различные показатели, однако авторами рассматриваются оценки, связанные с положительными эффектами выполнения цели (например, остаток энергии после выполнения цели, удовлетворение потребности цели). В процессорном устройстве каждого робота формируется матрица **D** размерностью (*N*, *M*), элементами которой являются d_{jl} – оценки эффективности *j*-го робота для *l*-й цели. После формирования матрицы **D** начинаются итерационные процедуры формирования коллективного плана, в результате которой для каждой цели обеспечивается максимум функционала

$$\mathbf{Y}_c = \sum_{j,l=1}^{N} d_{jl} n_{jl} \rightarrow \max, \qquad (1)$$

при ограничениях

$$\sum_{l=1}^{N} n_{jl} = 1,$$

$$\sum_{j=1}^{N} n_{jl} = n_l^{\max},$$

$$d_{jl} \geq 0,$$

где

$$n_{jl} = \begin{cases} 1, & \text{если } j-\text{й робот выбрал } l-\text{ю цель,} \\ 0, & \text{в противном случае.} \end{cases}$$

Здесь $j = \overline{1,N}$, $l = \overline{1,N}$, а $n_l^{\max}$ – необходимое количество роботов, которые должны выбрать *l*-ю цель.

В основу итерационных процедур положен анализ каждым роботом-агентом массива оценок эффективности и выбора «своей» цели, для которой значение оценки эффективности максимально. Затем происходит обмен информацией о выбранных решениях, анализ и «обсуждение» решений, принятых другими роботами, выбор для *l*-й цели агента с максимальным значением d_l, «вычеркивание» из матрицы **D** обеспеченных целей и роботов, выбравших цель в соответствии с функционалом (1). Так как в ПУ всех роботов имеются одинаковые матрицы **D**, то и результаты вычислений будут совпадать. Процедура повторяется до тех пор, пока не будут обеспечены все цели множества *M*.

Очевидно, что деструктивные информационные воздействия внедренных роботов-диверсантов могут заключаться в передаче членам коллектива вектора оценок, содержащих ложную информацию (предоставление членам коллектива завышенных или заниженных показателей эффективности), нарушения правил, принятых при «обсуждении» решений (необоснованные заявления о выборе целей).

Например, диверсант может передавать сообщения, что именно он является агентом, наиболее близко расположенным к цели. В этом случае в состав наряда сил, предназначенных для этой цели, будут включены диверсанты, которые не будут выполнять требующихся от легитимного агента действий в отношении цели [19].

Если роботы выполняют функции ретранслятора сигналов, то возможны атаки Man in the Middle, когда транзакции, осуществляемые удаленными агентами, подвергаются несанкционированной модификации и искажению.

Последствиями проведения всех этих атак может являться недостижение максимума функционалом (1). Основу модели безопасности для такой системы будет составлять монитор безопасности, осуще-

ствляющий физическую локацию субъектов и объектов и описывающий правила разграничения доступа удаленных субъектов к объектам.

Внутризональная политика безопасности, исходя из предложенной модели, реализуется локальным РО. В состав каждого РО входят:

1. агенты-полицейские по числу зон, входящих в состав региона;
2. реестр зон и их координаты;
3. база данных роботов-агентов с их текущими координатами;
4. модуль шифрования данных (при необходимости). Соседние РО связаны между собой безопасными каналами связи.

Логика функционирования такой системы может быть основана на известной логике функционирования системы безопасности мобильных агентов информационных систем, предложенной в работе [9]. Применительно к рассматриваемой модели защищенного коллектива роботов внутризональная логика взаимодействия роботов-агентов с полицейскими участками РО может быть следующей.

Пусть робот-агент r_i, находящийся в зоне h_j, получивший в некоторый k-й дискретный момент времени статус активного агента, на основе информации, полученной от других агентов на предыдущих шагах итерационной процедуры, выбрал в качестве нового действия A_j^{k+1}, для которого значение ΔY максимально. Для осуществления транзакции (передачи роботам-агентам своего решения) агент r_k формирует сообщение c_i^k о выбранном действии A_j^{k+1} для передачи объектам и, используя закрытую часть интерфейса, отправляет запрос a_i^k агенту-полицейскому ap_j зоны h_j на разрешение доступа. Агент-полицейский, получив запрос, осуществляет:

1. процедуры идентификации и аутентификации посредством обращения к базе данных агентов своей зоны;
2. проверку непротиворечивости информации о пространственном положении агента (например, дальность до целей), содержащуюся в сообщении c_i^k, с сообщениями других субъектов и (или) собственной оценкой обстановки. Для этого, исходя из сравнения координат своей зоны с данными, передаваемыми агентами, РО принимает решение, не содержится ли в сообщении дезинформация;
3. генерирование, распределение и передачу агентам по безопасному каналу связи ключей шифрования для предотвращения атаки Man in the Middle.

Если доступ признан легитимным, ap_j разрешает доступ на осуществление транзакции. Для этого он формирует подтверждающую квитанцию d_j^k для агентов своей зоны, и по безопасному каналу связи передает квитанцию e_j^k полицейским участкам остальных зон региона, которые, в свою очередь, формируют квитанции f_j^k для объектов своих зон. В качестве подтверждающей квитанции может служить ключ для дешифрования сообщения или сертификат цифровой подписи. В последнем случае в качестве удостоверяющего центра для агента служит РО своей зоны. Объекты региона, получив сообщение c_i^k, либо осуществляют его обработку, в случае получения подтверждающей квитанции от РО своих зон, либо игнорируют, удалив из оперативной памяти, в случае отсутствия подтверждающей квитанции.

В процессе выполнения задачи каждый робот-агент МРТС мигрирует в пределах региона и посредством телекоммуникационных технологий взаимодействует (осуществляют транзакции) с агентами всех зон региона *H*. При смене агентом зоны выполняется следующая процедура.

Робот-агент r_i, который намеревается мигрировать из зоны h_j в зону h_g, выполняет запрос агенту-полицейскому своей зоны ap_j. Агент-полицейский ap_j после выполнения процедур идентификации и аутентификации проверяет в своем реестре зон существование зоны h_g и, в случае положительного ответа, формирует и выдает роботу-агенту r_i уникальный сертификат, который содержит следующие данные: идентификатор агента, остаток энергоресурса, информацию о точке отправления и выбранном маршруте и время выдачи сертификата. При необходимости осуществляется шифрование данных убывающего робота-агента. После этого агент-полицейский дает разрешение на миграцию r_i. Прибыв в зону h_g, робот-агент предъявляет агенту-полицейскому ap_g этой зоны свой сертификат. Агент-полицейский ap_g на основе информации, содержащейся в предъявленном сертификате, осуществляет проверку в своем реестре зон существования в системе узла зоны h_j и обращается к агенту-полицейскому участка ap_j, из которого мигрировал агент r_i, с запросом на подтверждение существования агента r_i и того факта, что ему было разрешено мигрировать в зону h_g. Если агент ap_j подтверждает запрашиваемые сведения, агент-полицейский ap_g осуществляет расчеты временных и энергетических параметров движения робота-агента из зоны h_j в зону h_g с целью проверки соответствия:

- фактического времени прихода агента и остатка энергоресурса расчетному времени прибытия и остатку энергоресурса, которые могут быть вычислены исходя из времени выхода из зоны убытия и расстояния до него, а также величины остатка энергии в момент убытия робота из зоны пребывания;
- соответствия фактического пути следования пути, заявленному в сертификате.

При отсутствии противоречивых данных агент-полицейский ap_g заносит в свою базу данных агентов робота-агента r_i и предоставляет ему доступ к ресурсам зоны, необходимым для решения стоящей перед МРТС задачи.

Если ap_g не получил соответствующего подтверждения о существовании агента r_i в системе, или если обнаружено несоответствие по одному из пунктов проверки (фактические изменения остатка энергии, скорость и направление следования не соответствуют заявленным в сертификате значениям), агент r_i блокируется, а доступ к ресурсам зоны для него запрещается. Агент-полицейский зоны h_g в этом случае заносит агента r_i в «черный список» и информирует о присутствии «инородного» агента в системе «полицейские участки всех зон».

Предложенная модель, таким образом, позволяет реализовать как внутризональную, так и межзональную политику безопасности описываемой системы. В обоих случаях функция проверки легитимности доступа и (или) целостности транзакций пространственно распределенных в пределах региона субъектов и объектов реализуется посредством РО каждой из сегментированных зон.

Рассмотрим возможную реализацию межзональной политики безопасности и ее сравнение с работоспособностью внутризональной политики без реализации межзональной.

Сравнение работоспособности системы при использовании внутризональной и межзональной политики безопасности

Проведение эксперимента направлено на определение эффективности предложенных механизмов в условиях отсутствия агрессивного информационного воздействия, оказываемого на систему окружающей средой, и наличия скрытого деструктивного информационного воздействия, субъект которого функционирует в рамках рассматриваемой системы и не может быть однозначно идентифицирован классическими методами обеспечения ИБ МРТС.

В качестве сравниваемого подхода рассмотрим коэффициенты доверия/репутации [16], рассчитываемые локально для каждой группы агентов. Для полной потери работоспособности необходимо, чтобы общее количество диверсантов превышало 50% от всего размера роя [20], таким образом, можно говорить об устойчивости данного подхода к возникновению нарушителей ИБ. Однако меньшее число нарушителей также может спровоцировать некоторую потерю работоспособности роя. В качестве решения проблемы может использоваться подход полицейских участков, когда за расчет коэффициентов доверия/репутации отвечает полицейский того участка, на котором находится группа. Расчетные показатели уровней доверия и репутации по каждому из роботов передаются другим полицейским участкам, при возникновении такой необходимости. Таким образом, можно говорить о том, что доверие и репутация перестают рассчитываться локально и становятся глобальным показателем.

Исходя из обозначенных ранее наиболее перспективных видов атак на МРТС, проводимый эксперимент направлен на обоснование алгоритмической осуществимости представленных механизмов. Таким образом, допущением эксперимента является отсутствие моделирования физических особенностей реализации агентов и полицейских участков, а также физического пространства, в котором функционируют роботы. Для проведения эксперимента, исходя из представленных требований, авторами было использовано инструментальное средство имитационного моделирования, подробное описание которого представлено в [20]. Ход эксперимента можно описать следующим образом.

В момент инициализации эксперимента создаются два роя роботов таким образом, что зоны их связи не пересекаются, следовательно, можно говорить о двух изолированных роях. Роботы в роях обладают идентичными характеристиками (дальность действия связи, запас энергии, скорость движения и т.д.), за исключением пространственного расположения и типа поведения (диверсант или обычный робот). Каждая группа знает о наличии двух целей, которых следует достигнуть. Под целью понимается некоторая область пространства, следовательно, степень полноты достижения цели характеризуется количеством функционирующих в штатном режиме роботов, дошедших до цели.

Между роботами проводится аукцион, в ходе которого определяется список роботов, идущих к целям. В качестве оценки, исходя из которой определяются роботы, направленные на выполнение цели, применяется запас энергии, остающийся у робота после выполнения цели. Согласно условиям проведения эксперимента, расход энергии описывается линейной функцией, зависящей только от пройденного расстояния. Исходя из постулата об изолированности агентов, можно утверждать, что количество роботов, достигших целей, будет больше, чем требовалось.

Для сравнения подходов на устойчивость к возникновению скрытого деструктивного информационного воздействия часть агентов роя будет заменена на нарушителей – агентов, ведущих себя как нормальные роботы, но передающих ложную информацию о себе или об окружающей среде.

Предположим, что каждый нарушитель либо фальсифицирует информацию о расстоянии до цели, либо меняет траекторию движения после выбора цели. Остальные члены роя могут обнаружить нарушение при помощи сенсорных устройств. Если нарушение заключается в предоставлении ложной информации о расстоянии до цели, то рейтинг репутации/доверия снижается. Следовательно, агент не будет на-

правлен к цели. Другой тип нарушителей, который предоставляет ложную информацию о траектории движения, может быть обнаружен только при движении роботов роя до цели. В таком случае может отсутствовать возможность сообщить оставшимся членам роя о необходимости направления другого робота к цели.

Авторами работы проводится две серии экспериментов. В каждой серии рассматриваются следующие условия проведения экспериментов:

- размер каждой группы роботов – от 10 до 100 роботов (точное значение определяется случайным образом для каждого эксперимента);
- количество целей – 2;
- общее количество нарушителей – 10% от размера группы;
- необходимое количество обычных роботов для выполнения цели – 10% от числа роботов одного роя.

Для сравнения адекватности применения глобальных и локальных показателей доверия/репутации введем дополнительные условия проведения эксперимента. Предположим, что после достижения первых целей перед группами роботов, располагающимися в местах выполнения целей, ставятся две новые цели (цели второго уровня).

В рамках первой серии экспериментов рассмотрим ситуацию, при которой робот-нарушитель предоставляет неверную информацию относительно стоимости достижения им цели. Таким образом, нарушитель может получить возможность отправиться к цели, не имея для этого объективных предпосылок. Также предположим, что робот-нарушитель осуществляет движение до цели даже без назначения его на эту цель. Исходя из этого предположения и факта определения двух новых целей после достижения начальных, можно говорить о потенциальной успешности выполнения атаки на цели второго уровня. Расположение робота-нарушителя в области цели не учитывается при определении выполнения цели на основе количества числа роботов.

На основе проведенных экспериментов были получены результаты, представленные в табл. 1.

Показатель	**Цели первого уровня**	**Цели второго уровня**
	Значение, %	Значение, %
Среднее необходимое количество роботов для достижения цели (от общего числа роботов, задействованных на данном уровне)	5	5
Количество обнаруженных нарушителей (от общего числа нарушителей, функционирующих на данном этапе)	100	30,4
Количество экспериментов с невыполненными целями (минимум одна цель не выполнена)	0	75,3
Среднее количество недостающих для выполнения целей роботов (от общей необходимости)	0	69,3

Таблица 1. Результаты проведения первой серии экспериментов

Как видно из табл. 1, цели второго уровня остаются невыполненными в большинстве случаев, так как дошедшие до целей первого уровня роботы не позволяют провести адекватную оценку своих действий при помощи показателей доверия и репутации. Неверное представление об уровнях доверия и репутации приводит к тому, что около 70% роботов-нарушителей остаются не идентифицированными.

Для решения этой проблемы используем понятие полицейских участков. В предлагаемых экспериментах полицейские используются в качестве элементов, определяющих значения доверия и репутации для каждого робота, находящегося в их зоне ответственности. После определения плана выполнения цели и обнаружения нарушителей роботы начинают движение, в ходе которого меняют свою принадлежность к тому или иному полицейскому участку. Полицейский, в зону ответственности которого вошел робот, запрашивает информацию о его доверии и репутации у полицейского, осуществившего расчет этих данных на первом этапе. Даже при условии предоставления верной информации роботом-нарушителем на втором этапе выполнения эксперимента полицейский не будет учитывать его при определении планов по выполнению целей. Результаты проведения второй серии экспериментов представлены в табл. 2.

По результатам второй серии экспериментов можно говорить о том, что угроза участия в планах по выполнению целей роботов-нарушителей нейтрализована. Следовательно, будут выполнены все цели при использовании полицейских.

Исходя из проведенных экспериментов, можно говорить об успешности применения подхода, основанного на полицейских участках для реализации межзональной политики ИБ с целью обеспечения ИБ для решения классической итерационной задачи распределения наряда сил роботов по нескольким целям. При его использовании можно не только минимизировать ущерб от реализации угрозы, но и полностью нейтрализовать возможную угрозу. Таким образом, доказана работоспособность предлагаемой модели

для обеспечения ИБ МРТС при выполнении базовой функции каждой МРТС – перемещение в пространстве. Кроме того, возможно использование полицейских не только в качестве элементов, обеспечивающих ИБ, но и в качестве элементов, согласующих планы по выполнению целей, что приведет к уменьшению суммарных затрат роботов на выполнение поставленных целей.

Показатель	Цели первого уровня	Цели второго уровня
	Значение, %	Значение, %
Среднее необходимое количество роботов для достижения цели (от общего числа роботов, задействованных на данном уровне)	5	5
Количество обнаруженных нарушителей (от общего числа нарушителей, функционирующих на данном этапе)	100	100
Количество экспериментов с невыполненными целями (минимум одна цель не выполнена)	0	0
Среднее количество недостающих для выполнения целей роботов (от общей необходимости)	0	0

Таблица 2. Результаты проведения второй серии экспериментов

Заключение

Предложена теоретическая модель безопасности для мультиагентных робототехнических систем, которая основана на зональной модели безопасности и модели полицейских участков для распределенных вычислительных систем. Данная модель, в отличие от известных моделей разграничения доступа, позволяет осуществить физическую локацию агентов и описать правила разграничения доступа физически удаленных субъектов к объектам, которые реализуются внутризональными и межзональными мониторами безопасности. Такая организация управлением доступом позволила решить задачу реализации механизма отслеживания текущего местоположения каждого субъекта и объекта системы, а также осуществить разбиение множество доступов субъектов к объектам на множество легальных (безопасных) доступов и доступов, нарушающих целостность работы системы.

Работоспособность модели продемонстрирована посредством ее использования при построении механизма защиты классической итерационной задачи распределения роботов по нескольким целям. Предложенная модель позволила реализовать механизм защиты мультиагентных робототехнических систем от так называемых «мягких» атак, представляющих основную угрозу для системы в силу отсутствия четко идентифицируемых признаков и возможности реализации в процессе штатной работы системы без риска их оперативного обнаружения.

Литература

1. Neeran K.M., Tripathi A.R. Security in the Ajanta MobileAgent system. Technical Report. University of Minnesota, 1999. 28 p.
2. Higgins F., Tomlinson A., Martin K.M. Threats to the swarm: security considerations for swarm robotics // International Journal on Advances in Security. 2009. V. 2. N 2&3. P. 288–297.
3. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5 (87). С. 149–154.
4. Исакеев Д.Г., Зикратова Т.В., Лебедев И.С., Шабанов Д.П. Оценка безопасного состояния мультиагентной робототехнической системы при информационном воздействии на отдельный элемент // Вестник компьютерных и информационных технологий. 2015. № 1 (127). С. 43–49.
5. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in operating systems // Communication of the ACM. 1976. V. 19. N 8. P. 461–471. doi: 10.1145/360303.360333
6. Bell D.E., LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. MTR-2997 Rev.1. 134 p.
7. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks // Computer Communications. 2013. V. 36. N 12. P. 1284–1297. doi: 10.1016/j.comcom.2013.04.007
8. Gorodetski V., Kotenko I., Karsaev O. Multi-agent technologies

References

1. Neeran K.M., Tripathi A.R. *Security in the Ajanta MobileAgent system*. Technical Report. University of Minnesota, 1999, 28 p.
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, no. 2&3, pp. 288–297.
3. Zikratov I.A., Kozlova E.V., Zikratova T.V. Vulnerability analysis of robotic systems with swarm intelligence. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 5, pp. 149–154. (In Russian)
4. Isakeev D.G., Zikratova T.V., Lebedev I.S., Shabanov D.P. The estimation of secure condition of multi-agent robotic system in case of information influence on the single component. *Herald of Computer and Information Technologies*, 2015, no. 1, pp. 43–49. (In Russian)
5. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in operating systems. *Communication of the ACM*, 1976, vol. 19, no. 8, pp. 461–471. doi: 10.1145/360303.360333
6. Bell D.E., LaPadula L.J. *Secure Computer Systems: Unified Exposition and Multics Interpretation*. Bedford, Mass., MITRE Corp., 1976, 134 p.
7. Garcia-Morchon O., Kuptsov D., Gurtov A., Wehrle K. Cooperative security in distributed networks. *Computer Communications*, 2013, vol. 36, no. 12, pp. 1284–1297. doi: 10.1016/j.comcom.2013.04.007
8. Gorodetski V., Kotenko I., Karsaev O. Multi-agent technologies for computer network security: Attack

for computer network security: Attack simulation, intrusion detection and intrusion detection learning // Computer systems science and engineering. 2003. N 4. P. 191–200.
9. Гайдамакин Н.А. Зональная модель разграничения доступа в распределенных компьютерных системах // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2002. № 12. С. 15–22.
10. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts // Proc. 4th Int. Conf. on High Performance Computing in the Asia-Pacific Region. 2000. V. 2. P. 1165–1166.
11. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies // Applied Artificial Intelligence. 2000. V. 14. N 8. P. 825–848. doi: 10.1080/08839510050127579
12. Golbeck J., Parsia B., Hendler J. Trust networks on the semantic web // Lecture Notes in Artificial Intelligence. 2003. V. 2782. P. 238–249.
13. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems // Knowledge Engineering Review. 2004. V. 19. N 1. P. 1–25. doi: 10.1017/S0269888904000116
14. Carter J., Bitting E., Ghorbani A.A. Reputation formalization for an information-sharing multi-agent system // Computational Intelligence. 2002. V. 18. N 2. P. 515–534.
15. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с.
16. 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. № 2 (90). С. 47–52.
17. Коваль Е.Н., Лебедев И.С. Общая модель безопасности робототехнических систем // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 4(86). С. 153–154.
18. Sander T., Tschudin Ch.F. Protecting mobile agents against malicious hosts / In: G. Vigna (ed.) Mobile Agents and Security. LNCS, Springer, 1998. P. 44–60.
19. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Известия Томского политехнического университета. 2013. Т. 322. № 5. С. 104–108.
20. Viksnin I.I., Iureva R.A., Komarov I.I., Drannik A.L. Assessment of stability of algorithms based on trust and reputation model // Proc. 18th Conference FRUCT-ISPIT. St. Petersburg, Russia, 2016. P. 364–369. doi: 10.1109/FRUCT-ISPIT.2016.7561551

simulation, intrusion detection and intrusion detection learning. *Computer Systems Science and Engineering*, 2003, no. 4, pp. 191–200.
9. Gaidamakin N.A. Zone access control model in distributed computer systems. *Nauchno-Tekhnicheskaya Informatsiya. Seriya 2: Informatsionnye Protsessy i Sistemy*, 2002, no. 12, pp. 15–22. (In Russian)
10. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts. *Proc. 4th Int. Conf. on High Performance Computing in the Asia-Pacific Region*, 2000, vol. 2, pp. 1165–1166.
11. Schillo M., Funk P., Rovatsos M. Using trust for detecting deceitful agents in artificial societies. *Applied Artificial Intelligence*, 2000, vol. 14, no. 8, pp. 825–848. doi: 10.1080/08839510050127579
12. Golbeck J., Parsia B., Hendler J. Trust networks on the semantic web. *Lecture Notes in Artificial Intelligence*, 2003, vol. 2782, pp. 238–249.
13. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems. *Knowledge Engineering Review*, 2004, vol. 19, no. 1, pp. 1–25. doi: 10.1017/S0269888904000116
14. Carter J., Bitting E., Ghorbani A.A. Reputation formalization for an information-sharing multi-agent system. *Computational Intelligence*, 2002, vol. 18, no. 2, pp. 515–534.
15. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Models and Algorithms of the Collective Control of Robots Group*. Moscow, FIZMATLIT Publ., 2009, 280 p. (In Russian)
16. Zikratov I.A., Zikratova T.V., Lebedev I.S. Trust model for information security of multi-agent robotic systems with a decentralized management. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 2, pp. 47–52. (In Russian)
17. Koval E.N., Lebedev I.N. General model of robotic systems information security. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 4, pp. 153–154. (In Russian)
18. Sander T., Tschudin Ch.F. Protecting mobile agents against malicious hosts / In: G. Vigna (ed.) *Mobile Agents and Security*. LNCS, Springer, 1998, pp. 44–60.
19. Beshta A.A., Kirpo M.A. Construction of object trust model in the automated information system for preventing destructive influence on the system. *Bulletin of the Tomsk Polytechnic University*, 2013, vol. 322, no. 5, pp. 104–108. (In Russian)
20. Viksnin I.I., Iureva R.A., Komarov I.I., Drannik A.L. Assessment of stability of algorithms based on trust and reputation model. *Proc. 18th Conference FRUCT-ISPIT*. St. Petersburg, Russia, 2016, pp. 364–369. doi: 10.1109/FRUCT-ISPIT.2016.7561551

Авторы

Зикратов Игорь Алексеевич – доктор технических наук, профессор, заведующий кафедрой, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, igzikratov@yandex.ru

Викснин Илья Игоревич – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, wixnin@cit.ifmo.ru

Зикратова Татьяна Викторовна – преподаватель, Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», Пушкин, 197045, Российская Федерация, ztv64@mail.ru

Шлыков Андрей Александрович – студент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, andrew.shlykov@ya.ru

Медведков Дмитрий Игоревич – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, dmitrymedvedkov12@gmail.com

Authors

Igor A. Zikratov – D.Sc, Professor, Head of Chair, ITMO University, Saint Petersburg, 197101, Russian Federation, igzikratov@yandex.ru

Ilya I. Viksnin – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, wixnin@cit.ifmo.ru

Tatiana V. Zikratova – lecturer, N.G. Kuznetsov Naval Academy, Pushkin, 197045, Russian Federation, ztv64@mail.ru

Andrey A. Shlykov – student, ITMO University, Saint Petersburg, 197101, Russian Federation, andrew.shlykov@ya.ru

Dmitriy I. Medvedkov – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, dmitrymedvedkov12@gmail.com