УДК 004.056

ДОВЕРИТЕЛЬНАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МУЛЬТИАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ С ДЕЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

И.А. Зикратов[a], Т.В. Зикратова[b], И.С. Лебедев[a]

[a] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), Санкт-Петербург, Россия, petr-ermolaev@hotmail.com

[b] Военный институт (Военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», Санкт-Петербург, Россия, ztv64@mail.ru

Рассмотрены вопросы защиты мультиагентных робототехнических систем от атак со стороны роботов-диверсантов. Проведен анализ функционирования таких систем с децентрализованным управлением. Дано определение вредоносного информационного воздействия (атаки) со стороны робота-диверсанта, осуществляемого в отношении мультиагентной системы роботов. Рассмотрен класс атак, использующих перехват сообщений, формирование и передачу коллективу роботов дезинформации, а также осуществляющих иные действия, эксплуатирующие уязвимости мультиагентных алгоритмов, и не имеющих явно идентифицируемых признаков вторжения роботов-диверсантов. Проведен анализ существующих моделей информационной безопасности мультиагентных информационных систем, основанных на принципах централизованного и децентрализованного управления информационной безопасности. Разработана модель информационной безопасности, в которой роботы-агенты вырабатывают уровни доверия друг к другу на основе анализа событий, происходящих в системе. Идея доверительной модели состоит в анализе каждым роботом переданной информации и выполненных действий других членов коллектива и сопоставлении выбранного ими на *k*-м шаге итерации решения с целевой функцией коллектива. Отличительной особенностью доверительной модели по сравнению с ближайшим аналогом – Buddy Security Model, где осуществляется обмен между агентами токенами безопасности – является учет фактора времени, в течение которого агенты должны своими действиями «доказать» членам коллектива свою полезность в достижении общей цели. Предложены варианты реализации этой модели и способы оценки уровней доверия агентов, исходя из принятой в коллективе политики безопасности.

Ключевые слова: информационная безопасность, коллектив роботов, мультиагентные робототехнические системы, атака, уязвимость, модель информационной безопасности**.**

TRUST MODEL FOR INFORMATION SECURITY OF MULTI-AGENT ROBOTIC SYSTEMS WITH A DECENTRALIZED MANAGEMENT

I.A. Zikratov[a], T.V. Zikratova[b], I.S. Lebedev[a]

[a] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia, zikratov@cit.itmo.ru (igzikratov@yandex.ru)

[b] Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy «Naval Academy», Saint Petersburg, Russia, ztv64@mail.ru

The paper deals with the issues on protection of multi-agent robotic systems against attacks by robots-saboteurs. The operation analysis of such systems with decentralized control is carried out. Concept of harmful information impact (attack) from a robot-saboteur to the multi-agent robotic system is given. The class of attacks is considered using interception of messages, formation and transfer of misinformation to group of robots, and also carrying out other actions with vulnerabilities of multi-agent algorithms without obviously identified signs of invasion of robots-saboteurs. The model of information security is developed, in which robots-agents work out trust levels to each other analyzing the events occurring in the system. The idea of trust model consists in the analysis of transferred information by each robot and the executed actions of other members in a group, comparison of chosen decision on iteration step *k* with objective function of the group. Distinctive feature of the trust model in comparison with the closest analogue - Buddy Security Model in which the exchange between the agents security tokens is done — is involvement of the time factor during which agents have to "prove" by their actions the usefulness in achievement of a common goal to members of the group. Variants of this model realization and ways of an assessment of trust levels for agents in view of the security policy accepted in the group are proposed.

Keywords: information security, group of robots, multi-agent robotic systems, attack, vulnerability, information security model (IT security model).

Введение

Все более значимым направлением развития робототехники является совершенствование теории и практики построения интеллектуальных систем группового управления роботами – так называемых мультиагентных робототехнических систем (МРТС). Наиболее перспективными представляются МРТС, реализующие методы коллективного планирования действий, основанные на принципах децентрализованного управления. Это обусловлено меньшей размерностью решаемых задач, большим радиусом действия, достигаемым за счет рассредоточения роботов по всей рабочей зоне, и более высокой вероятностью выполнения задания, достигаемой за счет возможности перераспределения целей между роботами группы в случае выхода из строя некоторых из них [1].

Несмотря на указанные преимущества, децентрализованный характер построения информационных систем и потенциальная возможность коммуникации агента с любым другим агентом делают мультиагентную среду максимально уязвимой для таких угроз, как несанкционированный перехват сообщений в процессе межагентных коммуникаций, нарушение целостности передаваемых по сети данных, не-

санкционированный доступ к данным, отказ в обслуживании (DDoS-атаки), перехват запросов с последующей их модификацией и воспроизведением и т.д. [2]. Перечисленные особенности, наряду с потенциальной возможностью противоборствующей стороны получить физический доступ к роботу-агенту, также существенно затрудняют использование известных из теории информационной безопасности методов разграничения доступа, основными из которых являются дискреционное и мандатное разграничения, реализуемые в рамках соответствующих моделей [3, 4].

К основным механизмам атак на МРТС, формирующим указанные угрозы, принято относить [5, 6]:

1. атаки на каналы связи;
2. затруднение идентификации и аутентификации агентов в системе;
3. физическое внедрение «инородных» роботов, которыми, в том числе, могут быть захваченные и перепрограммированные злоумышленником «свои» роботы.

Целью настоящей работы является разработка модели информационной безопасности МРТС, позволяющей противостоять атакам третьего вида – физическому внедрению «инородных» роботов (роботов-диверсантов), задачей которых является недопущение или снижение эффективности действий коллектива роботов при децентрализованном управлении.

Функционирование МРТС с децентрализованным планированием действий

Рассмотрим действия МРТС при использовании наиболее распространенной итерационной процедуры оптимизации коллективного решения [7, 8].

В начале работы всем роботам коллектива передаются исходные данные, необходимые для решения оптимизационной задачи по достижению цели, стоящей перед МРТС. Каждый робот R_j ($j = \overline{1,N}$) коллектива обладает своим процессорным устройством (ПУ). Типовая структура МРТС с децентрализованным управлением может быть построена по схеме, представленной на рис. 1.

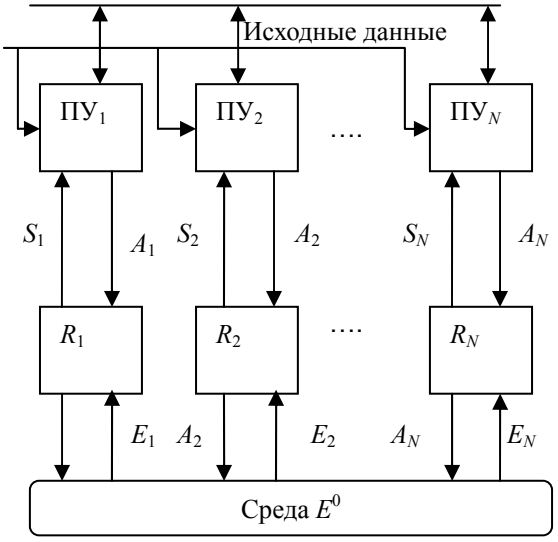

Рис. 1. Децентрализованная система управления в МРТС

В состав ПУ входят следующие блоки: ВБ – вычислительный блок; БПИ – блок передачи информации; БПрИ – блок приема информации; БОТС – блок определения текущего состояния; СБ – сенсорный блок. Процессорное устройство связано с процессорными узлами других роботов каналами связи, по которым передается информация о текущих состояниях S_i^0 остальных роботов и выбираемых ими в процессе выполнения итерационной процедуры действиях A_j^{k+1}, (k=0,1,2,…). Кроме того, ПУ получает информацию о состоянии S_j^0 своего робота и окружающей среды E^0. На основании всей полученной информации ВБ j-го робота 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.

Анализ возможностей роботов-диверсантов по вредоносному воздействию на МРТС

Под вредоносным информационным воздействием (атакой), осуществляемым роботом-диверсантом на k-й итерации, будем понимать деятельность робота-диверсанта, направленную на реализацию угрозы информационной безопасности в отношении роботов-агентов R_j ($j = \overline{1,N}$) и осуществляемую с использованием информационных средств и технологий, в результате которой выбранное агентами новое действие A_j^{k+1} не будет способствовать приращению целевого функционала ΔY МРТС в имеющихся условиях.

Рассмотрим следующие виды атак на МРТС: перехват сообщений A_j и S_j с последующей их модификацией и воспроизведением; формирование и передача дезинформации диверсантом о своем состоянии и выбранных действиях A_j и S_j; создание помех сенсорным устройствам для оценки состояния внешней среды; действия роботов-диверсантов, направленные на эксплуатацию уязвимостей алгоритмов коллективного управления [9], и т.д. Очевидно, что указанные атаки не имеют четко идентифицируемых признаков, в отличие от атак, проводимых путем постановки помех, DDoS-атак, так как роботы, их системы и каналы связи функционируют в штатном режиме.

В мультиагентных информационных системах для предотвращения атак подобного типа используются: метод защищенных состояний агентов [10]; методы мобильной криптографии [11]; метод Ксюдонга [12]; «товарищеская» модель безопасности (Buddy Security Model, BSM) [13, 14], которые хорошо согласуются с принципами построения децентрализованных систем. В частности, модель взаимной безопасности BSM представляет собой такую систему безопасности, в которой агенты отвечают за безопасность друг друга, отслеживая происходящие в системе события и взаимодействуя между собой и внешней средой. В процессе межагентных коммуникаций агенты системы обмениваются специальными сообщениями – токенами, которые несут в себе секретную информацию о состояниях известным им агентов и о возможных угрозах с их стороны либо со стороны узлов сети. Таким образом, все агенты системы получают информацию о потенциальных угрозах их безопасности. Информируя своих соседей о возможной опасности (например, о появлении «чужого» агента в системе), каждый из агентов несет ответственность за безопасность своего окружения и всей системы в целом. Привлекательность этой модели состоит в отсутствии какого-либо единого центра безопасности, что приводит к невозможности разрушения модели. Однако использование BSM в робототехнических мультиагентных системах несет в себе опасность внедрения робота-диверсанта, так как, в отличие от мультиагентных информационных систем, роботы-агенты в МРТС находятся вне пределов зоны контролируемой территории, где вероятен физический захват агента противником и компрометация токена.

В настоящей работе предлагается модель безопасности МРТС, базирующаяся на принципах модели BSM, но отличающаяся введением показателя «уровень доверия» для каждого робота-агента, что в значительной степени затрудняет эксплуатацию указанной уязвимости.

Доверительная модель информационной безопасности для мультиагентных робототехнических систем

Идея, положенная в основу модели, состоит в следующем.

После запуска итерационного цикла *j*-й робот (робот-объект) ($j = \overline{1,N}$), имеющий текущее состояние S_j^0, получает в активной фазе текущей итерации в свое распоряжение канал связи и доступ к ПУ роботов – членов своего коллектива. На основании имеющейся у него информации о состояниях $S_1^0, S_2^0, \ldots, S_{j-1}^0, S_{j+1}^0, \ldots, S_N^0$ и текущих действиях $A_1^{k+1}, A_2^{k+1}, \ldots, A_{j-1}^{k+1}, A_{j+1}^k, \ldots, A_N^k$ объект вырабатывает действие A_j^{k+1}, при котором значение ΔY максимально, и осуществляет доступ на запись *w* информации о A_j^{k+1} в ПУ роботов-субъектов. Остальные роботы-агенты, получив эту информацию, проверяют:

– полученную информацию на предмет соответствия действительности;
– «полезность» выбранного роботом-объектом действия с точки зрения приращения целевого функционала ΔY.

Если *i*-й робот (робот-субъект) ($i \neq j$) в результате проверки получил положительное заключение, он повышает уровень доверия для *j*-го робота. Под доверием в данном случае понимается состояние субъекта, характеризующееся готовностью взаимодействовать путем получения и передачи определенных прав и информации иным субъектам. Если результат «проверки» оказался отрицательным (робот-объект передал неверную информацию или выбрал нерациональное действие), уровень доверия робота-объекта для *i*-го робота-субъекта уменьшается. В результате, после нескольких итераций в процессе принятия решения на *l*-м шаге, каждый робот при выборе нового действия A_j^{l+1} будет в первую очередь учитывать информацию от членов коллектива с высоким уровнем доверия, и только затем – с низким.

Таким образом, низкий уровень доверия не позволит диверсанту оказывать деструктивного воздействия на принятие агентами решения даже при наличии токена. Из этого следует, что действия диверсанта по повышению уровня доверия предполагают участие робота в достижении цели МРТС, что, в свою очередь, противоречит логике его использования с точки зрения противника.

Реализация доверительной модели информационной безопасности

Введем следующие обозначения: $A = \{A_1, A_2, \ldots, A_n\}$ – множество возможных действий робота-объекта в отношении функционала МРТС; $S = \{s_1, s_2, \ldots, s_m\}$ – множество состояний устройств коммуникации робота-субъекта; $V = \{F, T\}$ – множество значений результатов проверки действий робота-объекта: *F* – ложь, *T* – истина; r_l^m – значение уровня доверия *l*-го робота-объекта для *m*-го робота-субъекта, $l \neq m$.

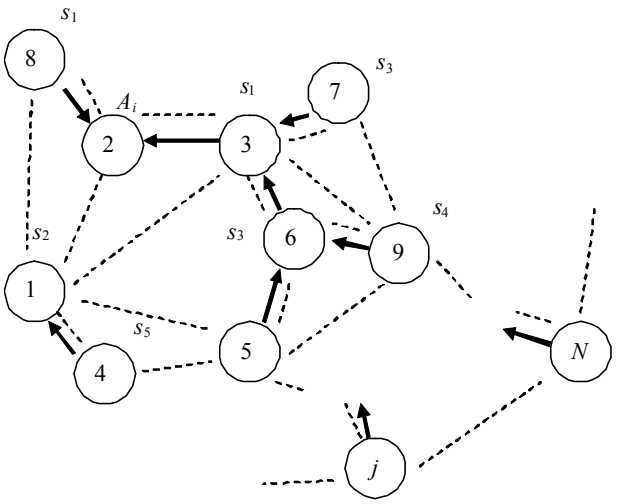

Рис. 2. Взаимодействие роботов-агентов в доверительной модели

Реализацию доверительной модели удобно рассмотреть на примере (рис. 2). На рис. 2 представлен фрагмент группировки из *N* роботов-агентов. Стрелками обозначены межагентные связи, осуществляемые посредством СБ, например, визуальная связь, пунктирными линиями – радиосвязь, осуществляемая БПрИ и БПИ. Рассмотрим возможные способы реализации доверительной модели.

1. Пусть на *k*-м шаге итерационного цикла действие A_i выполнил робот № 2. О выполненном действии робот-объект известил сообщением вида $2A_i$, где цифра означает идентификационный номер объекта. Из рисунка видно, что в зоне радиосвязи робота № 2 оказались роботы №№ 1, 3 и 8, которые и «услышали» сообщение от робота-объекта о выбранном им для реализации действии. Кроме того, субъекты № 3 и № 8 «видят» робота-объекта и, соответственно, выполняемое им действие, о котором было получено сообщение. Следовательно, множество *S* состояний роботов-субъектов №№ 1, 3 и 8 можно описать двумя состояниями:

– состояние s_1 – «слышу и вижу объект» – для субъектов № 3, 8;
– состояние s_2 – «слышу и не вижу объект» – для субъекта № 2.

Очевидно, что выполняемое роботом-объектом № 2 действие A_i может соответствовать либо не соответствовать переданному сообщению по каналу БПрИ. В первом случае роботы-субъекты №№ 3 и 8, визуально наблюдающие посредством своих СБ объект и выполняемые им действия A_i, имеют основания повысить свое доверие к объекту № 2 на величину $\Delta r_2^3 = \Delta r_2^8$, так как сообщение об этом действии не является дезинформацией. Робот-субъект № 1 также получил информацию о действии A_i от объекта № 2, однако подтверждения или опровержения ее по каналу СБ получить не может. Следовательно, изменение доверия Δr_2^1 к объекту № 2 со стороны субъекта № 1 будет иметь меньшую величину, чем для субъектов №№ 3 и 8 $\left(\Delta r_2^1 < \Delta r_2^{3,8}\right)$.

Таким образом, при указанном способе реализации оценку уровня доверия робота-объекта осуществили только «очевидцы», т.е. те роботы-субъекты, которые находились в зоне визуальной и (или) радиосвязи с объектом. Для остальных членов коллектива доверие к роботу № 2 осталась неизменной.

2. Рассмотрим ситуацию, описанную выше. Получив сообщение от робота-объекта, роботы-субъекты, имеющие состояния s_1 и s_2 (роботы-«очевидцы») передают сообщения вида: $numberA_i s_k^j v$, где *number* – номер робота-объекта; A_i – переданное объектом сообщение; s_k^j – состояние *j*-го робота-субъекта; v – результат проверки истинности сообщения объекта ($v \in$ V). Тогда для рассматриваемого примера сообщения от роботов-субъектов будут иметь следующий вид: робот № 1 – $2A_i s_2^1 T$; робот № 3 – $2A_i s_1^3 T$; робот № 8 – $2A_i s_1^8 T$. Эти сообщения будут приняты роботами №№ 4, 5, 6, 7 и 9. Очевидно, что в зависимости от положения агентов на местности состав принятых ими сообщений различен. Тогда множество состояний *S* можно представить следующими состояниями агентов:

– состояние s_1 – «слышу и вижу объект» – для субъектов №№ 3 и 8;
– состояние s_2 – «слышу и не вижу объект» – для субъекта № 2;
– состояние s_3 – «слышу и вижу субъект s_1» – для субъектов №№ 6 и 7;
– состояние s_4 – «слышу и не вижу субъект s_1» – для субъекта № 9;
– состояние s_5 – «слышу и вижу субъект s_2» – для субъекта № 4;
– состояние s_6 – «слышу и не вижу субъект s_2» – для субъекта № 5.

Очевидно, что субъекты, имеющие разные состояния $s_1, s_2, \ldots, s_6$, имеют различные возможности по оценке доверия объекта в зависимости от их возможности по проверке истинности сообщения о дей-

ствиях объекта. Для субъектов, находящихся в состояниях $s_1, s_2, \ldots, s_6$, можно ввести фиксированную шкалу приращения уровня доверия *n*-го объекта:

$\Delta r_{s_1}^n > \Delta r_{s_2}^n > \ldots > \Delta r_{s_6}^n$.

В этом случае задача субъектов МРТС, получивших одно или несколько сообщений от других субъектов, сводится к определению своего состояния и, в соответствии с этим состоянием, изменению уровня доверия к объекту. В случае, когда в принятом сообщении параметр *v* имеет значение *T* (респондент не опровергает сообщение объекта), происходит увеличение уровня доверия на величину $\Delta r_{s_i}^n$. Если параметр имеет значение *F* (респондент обнаруживает, что выполненное объектом действие не соответствует информации в сообщении) – уровень доверия уменьшается на соответствующую величину.

Следует отметить, что поступление от разных источников противоречивой информации об объекте может быть следствием воздействия случайных факторов (условия радиосвязи, случайные ошибки, неисправность канала связи и т.д.) либо преднамеренного искажения информации одним из респондентов. Возможная реакция робота-субъекта, принявшего такую информацию, может определяться принятой в МРТС политикой безопасности (игнорирование сообщений, понижение рейтинга респондентам и т.д.).

Таким образом, второй способ позволяет большему числу субъектов оценить уровень доверия к объекту, но это приводит к увеличению интенсивности обмена сообщениями.

Выявление атак на уязвимости алгоритмов коллективного управления МРТС

Предложенные способы реализации доверительной модели позволяют противостоять таким атакам, как перехват сообщений A_j и S_j с последующей их модификацией и воспроизведением, а также формирование и передача дезинформации диверсантом о своем состоянии и выбранных действиях A_j и S_j, которые, в конечном счете, приводят к приращению целевого функционала ΔY для всех возможных допустимых действий в текущей ситуации. Вместе с тем, ряд алгоритмов коллективного управления мультиагентными системами предусматривает процедуру выбора «лидера» – члена коллектива роботов, на которого могут возлагаться специфические задачи, действия которого в значительной степени будут определять успешность решения задач, стоящих перед коллективом. Типичным примером такой задачи является задача управления группой роботов в режиме «ведущий–ведомый» [15], когда процедура выбора действия A_j^{k+1}, способствующего максимуму приращения целевого функционала ΔY МРТС, делегируется «лидеру», а роль остальных агентов сводится к выбору оптимального пути следования за ведущим.

Очевидно, что приобретение статуса «лидера» роботом-диверсантом позволит ему, при наличии токена, управлять ведомым коллективом роботов в интересах противоборствующей стороны. Подобная атака может осуществляться не только «лидером», но и группой диверсантов, осуществляющих действия, не соответствующие целевой установке МРТС. При этом МРТС будет функционировать в штатном режиме, и единственным признаком, позволяющим обнаружить атаку, может быть оценка приращения целевого функционала ΔY на каждой итерации, осуществляемая членами коллектива. Для этого роботы-субъекты, получив на *l*-м шаге информацию от объекта о выбранном действии A_j^{l+1}, осуществляют пересчет приращения целевого функционала ΔY_{i+1}. Если окажется, что $\Delta Y_{i+1} < \Delta Y_i$, субъект уменьшает уровень доверия к *n*-му объекту на величину $\Delta r_{Y_i}^n$, иначе – увеличивает. Итоговая оценка уровня доверия *n*-го объекта на *l*-м шаге итерационного процесса, вычисляемая субъектом с состоянием s_i, равна

$$\Delta\eta^n = \alpha\Delta r_{S_i}^n + \beta\Delta r_{Y_i}^n,$$

где α и β – два параметра, которые задают вес параметру истинности сообщения от объекта и «полезности» выбранного им действия в зависимости от принятой в МРТС политики безопасности.

Заключение

Разработанная модель представляет собой модель информационной безопасности децентрализованной мультиагентной робототехнической системы, в которой разграничение доступа агентов к коллективу осуществляется на основе показателя уровня доверия по отношению друг к другу, вырабатываемого членами коллектива в процессе их взаимодействия при достижении целевого функционала.

Достоинством такого подхода является отсутствие выделенного центра управления безопасностью МРТС, который часто является целью атак злоумышленников. Основным отличием доверительной модели от известных является учет фактора времени, в течение которого агенту необходимо достичь такого уровня доверия со стороны членов коллектива, который позволит эффективно участвовать в процессе функционирования МРТС. Для повышения уровня доверия агенту необходимо выполнять не только рациональные (с точки зрения других членов коллектива) действия, но и функции по обеспечению информационной безопасности. Недостатком децентрализованной модели информационной безопасности являются определенные затраты канальных и вычислительных ресурсов членами МРТС. Оценка эффективности полученных решений будет осуществляться по результатам численного эксперимента, который в настоящее время готовится авторами, и будет представлена в одной из следующих статей.

References

1. Brambilla M., Ferrante E., Birattari M., Dorigo M. Swarm robotics: a review from the swarm engineering perspective. *Swarm Intelligence*, 2013, vol. 7, no. 1, pp. 1–41. doi: 10.1007/s11721-012-0075-2
2. Masloboev A.V., Putilov V.A. Razrabotka i realizatsiya mekhanizmov upravleniya informatsionnoi bezopasnost'yu mobil'nykh agentov v raspredelennykh mul'tiagentnykh informatsionnykh sistemakh [Development and implementation of mobile agent security control mechanisms in the distributed multi-agent information systems]. *Proceedings of the MSTU*, 2010, vol. 13, no. 4-2, pp. 1015–1032.
3. Bell D.E., LaPadula L.J. *Secure computer systems: Unified exposition and multics interpretation*. Bedford, Mass.: MITRE Corp., 1976, 134 p.
4. Harrison M., Ruzzo W., Ullman J. Protection in operating systems. *Communication of the ACM*, 1976, vol. 19, no. 8, pp. 461–471. doi: 10.1145/360303.360333
5. 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.
6. Koval E.N., Lebedev I.S. Obshchaya model' bezopasnosti robototekhnicheskikh sistem [General model of robotic systems information security]. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 4 (86), pp. 153–154.
7. Kalyaev I.A., Gaiduk A.R., Kapustyan S.G. *Modeli i algoritmy kollektivnogo upravleniya v gruppakh robotov* [Models and algorithms of the collective control of robots group]. Moscow, FIZMATLIT Publ., 2009, 280 p.
8. Kalyaev I.A., Lokhin V.M., Makarov I.M. et. al. *Intellektual'nye roboty* [Intelligent Robots] Ed. E.I. Yurevich. Moscow, Mashinostroenie Publ., 2007, 360 p.
9. Zikratov I.A., Kozlova E.V., Zikratova T.V. Analiz uyazvimostei robototekhnicheskikh kompleksov s roevym intellektom [Vulnerability analysis of robotic systems with swarm intelligence]. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013, no. 5 (87), pp. 149–154.
10. Neeran K.M., Tripathi A.R. *Security in the Ajanta Mobile Agent System*. Technical Report, Department of Computer Science, University of Minnesota, 1999, 28 p.
11. Sander T., Tschudin Ch.F. Protecting mobile agents against malicious hosts. *Mobile Agents and Security, Ser. Lecture Notes in Computer Science*, 1998, vol. 1419, pp. 44–60.
12. Xudong G., Yiling Ya., Yinyuan Y. POM-a mobile agent security model against malicious hosts. *Proc. of the 4th International Conference on High Performance Computing in the Asia-Pacific Region*, 2000, vol. 2 (14-17), pp. 1165–1166.
13. Page J., Zaslavsky A., Indrawan M. A buddy model of security for mobile agent communities operating in pervasive scenarios. *Proceedings of 2nd Australasian Information Security Workshop (AISW2004)*. ACS Dunedin, New Zealand, 2004, vol. 32, pp. 17–25.
14. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities. *Proc. of the 1st International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004)*, 2004, pp. 85–101.
15. Kremlev A.S., Kolyubin S.A., Vrazhevsky S.A. Avtonomnaya mul'tiagentnaya sistema dlya resheniya zadach monitoringa mestnosti [Autonomous multi-agent "robot-guide" system to solve area monitoring problems]. *Izv. vuzov. Priborostroenie,* 2013, vol. 56, no. 4, pp. 61–65.

Зикратов Игорь Алексеевич – доктор технических наук, профессор, зав. кафедрой, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), Санкт-Петербург, Россия, zikratov@cit.itmo.ru

Зикратова Татьяна Викторовна – преподаватель, Военный институт (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», Санкт-Петербург, Россия, ztv64@mail.ru

Лебедев Илья Сергеевич – доктор технических наук, доцент, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), Санкт-Петербург, Россия, lebedev@cit.ifmo.ru

Igor A. Zikratov – D.Sc., Professor, Department head, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia, zikratov@cit.itmo.ru (igzikratov@yandex.ru)

Tatyana V. Zikratova – tutor, Military Institute (Naval Polytechnic) Military Educational and Scientific Center of the Navy "Naval Academy", Saint Petersburg, Russia, ztv64@mail.ru

Ilya S. Lebedev – D.Sc., Associate professor, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics(ITMO University),, Saint Petersburg, Russia, lebedev@cit.ifmo.ru

Принято к печати 24.12.13
Accepted 24.12.13