УДК 004.056

ОЦЕНКА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МУЛЬТИАГЕНТНОЙ РОБОТОТЕХНИЧЕСКОЙ СИСТЕМЫ ПРИ ИНФОРМАЦИОННОМ ВОЗДЕЙСТВИИ

И.С. Лебедев[a], Т.В. Зикратова[b], Д.П. Шабанов[a], В.В. Чистов[a]

[a] Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), Санкт-Петербург, Россия, lebedev@cit.ifmo.ru

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

Рассматриваются особенности обеспечения информационной безопасности мультиагентной робототехнической системы с самоорганизующимся поведением. Акцентируется внимание на возможности реализации угроз информационной безопасности на уровне организации взаимодействия между отдельными элементами. Вводятся определения понятий информационного воздействия и дезорганизации мультиагентной робототехнической системы. Для оценки безопасного состояния системы в качестве критерия выбрана вероятность наличия в момент времени Δt требуемого для выполнения поставленной задачи количества элементов мультиагентной робототехнической системы, не подвергающихся информационному воздействию. Предложен метод оценки вероятности нахождения мультиагентной робототехнической системы в безопасном состоянии. В основе метода лежит математический аппарат марковских цепей. Отличие метода состоит в использовании функциональных зависимостей интенсивности информационного воздействия. Метод позволяет выявить требуемые характеристики отдельных элементов на ранних стадиях разработки. Приводятся графики вероятности безопасного состояния системы группы элементов при различных интенсивностях, характеризующих программно-аппаратные возможности выхода элемента из небезопасного состояния, и интенсивностях информационного воздействия со стороны злоумышленника. Моделируется поведения системы в динамике при различных функциональных зависимостях интенсивностей информационного воздействия. Рассматривается пример нахождения группировки из четырех однотипных элементов в безопасном состоянии при атаке тремя дезорганизующими элементами. Раскрывается методика получения числовых значений интенсивностей информационного воздействия в последовательные моменты времени.

Ключевые слова: информационная безопасность, робототехнические системы, самоорганизующееся поведение, информационное воздействие, уязвимость.

INFORMATION SECURITY ASSESSMENT FOR MULTI-AGENT ROBOTIC SYSTEM UNDER THE INFORMATION IMPACT

I.S. Lebedev[a], T.V. Zikratova[b], D.P. Shabanov[a], V.V. Chistov[a]

[a] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia, lebedev@cit.ifmo.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 features of information security guaranteeing of the multi-agent robotic system with self-organizing behavior. The main attention is paid to the possibility of implementing information security threats on the level of interaction between the individual elements. The definitions “information impact” and “disorganization” are introduced for multi-agent robotic system. As a criterion for the system safety state assessment, probability is selected of number of items available at time Δt for required task execution of multi-agent robotic system, not suffering from the effects of the information impact. A method for estimating the probability of the multi-agent robotic system being in a safe state is proposed. The method is based on mathematical apparatus of Markov chains. Its distinction is the usage of functional dependencies for intensity information impact. The method gives the possibility to identify required characteristics of the individual elements in the early stages of development. Graphs of probability for secure system state of group of elements at different intensities of information impact by intruder and intensities are given, characterizing software and hardware capabilities of element output from the unsafe condition. The system behavior is modeled in the dynamics for different functional dependencies of the information impact intensity. An example of group consisting of four identical elements staying in a safe condition and attacking by three disorganizing elements is shown. Technique of obtaining numerical values for the intensities of information impact at successive instants is revealed.

Keywords: information security, robotic systems, self-organizing behavior, information impact, vulnerability.

Введение

В связи с ростом сложности робототехнических систем (РТС) особое внимание уделяется вопросам обеспечения информационной безопасности (ИБ) отдельных устройств, элементов и их групп. Достижения в области искусственного интеллекта, появление ряда перспективных направлений, требующих массовости, масштабирования и самоорганизации отдельных агентов для решения поставленных задач, увеличивает интерес исследователей к самоорганизующимся системам [1, 2].

Разнообразие РТС обусловливает появление различных направлений обеспечения ИБ, использующих как подходы, применяемые в информационно-телекоммуникационных системах и распределенных вычислительных системах [3, 4], так и специфические методы, учитывающие особенности мультиагентных РТС (МРТС) [5–7]. Появление ряда перспективных проектов [1, 2, 6] показывает необходимость осуществления прогнозных оценок и контроля безопасного состояния системы децентрализованных элементов, объединенных необходимостью достижения поставленных целей.

Исходя из сказанного, одним из актуальных направлений является разработка и внедрение научно-методического аппарата теории информационной безопасности, позволяющего осуществлять оценку состояний ИБ МРТС в агрессивной информационной среде.

Особенности обеспечения ИБ мультиагентной робототехнической системы

Особенности структуры и поведения МРТС, обладающим возможностями самоорганизации, например роевых, позволяют выделить ряд предпосылок, определяющих потенциальные уязвимости:
- отсутствие, недостаточность, относительность информации о текущем состоянии, местоположении каждого устройства;
- относительно слабая интенсивность обмена информацией с координирующим центром;
- изначально заложенная автономность действий отдельных элементов МРТС;
- возможность действий отдельных элементов групповой МРТС вне контролируемой зоны;
- несовершенство (или отсутствие) механизмов идентификации и аутентификации элементов, приводящее к значительным задержкам при обнаружении вторжений в группу МРТС;
- ограниченные возможности средств обнаружения аномального поведения элементов МРТС.

Возможность реализации угроз ИБ применительно к МРТС, обладающих возможностями самоорганизации, рассматривается на алгоритмическом, ресурсном уровне и на структурном уровне организации взаимодействия между отдельными элементами [7–9]. Получение аналитических зависимостей, позволяющих идентифицировать аномальную активность или проявление информационных событий, вызываемых злоумышленником, не всегда возможно [4, 5, 9], что, в свою очередь, позволяет выделить ряд категорий потенциальных атак, направленных на нарушение целостности, конфиденциальности и доступности информации:
- сбор информации;
- попытки несанкционированного доступа;
- «отказ» в обслуживании;
- подозрительная активность.

В некоторых случаях нецелесообразно тратить силы на преодоление систем защиты МРТС, достаточно разрушить организационную структуру. Можно, например:
- нарушить взаимодействие между элементами, доступность наиболее важных узлов иерархии группировки, подменить или внедрить отдельных агентов, нарушающих правила группового поведения;
- применить информационное воздействие – процесс, направленный на изменение статуса информационной компоненты в объекте воздействия и осуществляемый в пределах информационной сферы с использованием информационных средств и технологий [10];
- дезорганизовать некоторое количество агентов МРТС (нарушить устойчивость и согласованность алгоритмов и связей, необходимых для совместного функционирования элементов в пространстве и времени [10]), которое не позволит всей группировке достичь поставленной цели.

В связи с этим возникает необходимость оценки влияния информационного воздействия на элементы организационной структуры МРТС с самоорганизующимся поведением.

Целью моделирования является оценка вероятности нахождения системы в состоянии, при котором лица и технические средства, осуществляющие информационное противоборство, не могут контролировать в определенный момент времени критическое количество элементов, необходимое для выполнения поставленной цели. Такое состояние МРТС назовем безопасным состоянием.

Моделирование информационного воздействия

Под МРТС с самоорганизующимся поведением будем понимать систему, состоящую из группы децентрализованных однотипных роботизированных элементов, предназначенных для совместного решения заранее определенных задач, обладающую свойствами автономности, ограниченности представления, масштабируемости [11].

Мультиагентная система O состоит из множества однотипных робототехнических элементов o_i, i=1…n. Каждому элементу o_i соответствует кортеж $h = <h_1, \ldots, h_m>$, определяющий его технические характеристики, зависящие от окружающей среды, информационных воздействий и других технических факторов. Кортеж определяется значениями внутренних и внешних показателей. Внутренние показатели доступны только самому элементу o_i для принятия решения о дальнейшем поведении, внешние используются ближайшими окружающими элементами для коррекции своего состояния. Учитывая, что каждый элемент в самоорганизующейся системе выступает в качестве объекта и субъекта доступа, появление внешнего информационного воздействия, дезорганизующего всю систему, возможно в результате возникновения угроз доступности или модификации информации отдельного элемента.

Изменение состояния ИБ одного элемента влияет на состояние всей системы в целом, так как каждый элемент обладает своими характеристиками, определяющими ИБ работы системы. Переход в небезопасное состояние одного элемента МРТС может оказывать дезорганизующее воздействие на другой

элемент, в зоне доступности которого он находился. В результате образуется цепная реакция, когда каждый элемент будет переходить из безопасного состояния, направленного на выполнение задачи совместно с другими элементами, в небезопасное состояние, оказывающее информационное воздействие на других участников группового поведения.

Если в качестве критерия оценки безопасного состояния системы выбрать вероятность наличия в конкретный момент времени требуемого для выполнения поставленной задачи количества элементов МРТС, не подвергающихся информационному воздействию, то вероятность безопасного состояния будет зависеть от интенсивностей, характеризующих программно-аппаратные возможности выхода элемента из небезопасного состояния, и интенсивностей информационного воздействия со стороны злоумышленника. Таким образом, требуется метод оценки вероятности нахождения МРТС в безопасном состоянии, отличающийся от известных использованием функциональных зависимостей интенсивности информационного воздействия, что позволит выявить требуемые характеристики отдельных элементов на ранних стадиях проектирования.

В МРТС S, состоящей из n однотипных элементов, состояние S_0, S_1, S_2, …, S_n, определяемое количеством подвергающихся информационному воздействию элементов, меняется с течением времени не предсказуемым заранее образом. Для каждого момента времени вероятность любого состояния системы в будущем зависит только от ее состояния в настоящее время и не зависит от того, когда и каким образом система перешла в это состояние.

Переход из конкретного состояния системы определяется интенсивностью, зависящей от программно-аппаратных возможностей выхода элемента из небезопасного состояния, и интенсивностью информационного воздействия со стороны злоумышленника. С учетом этого можно описать состояния всей МРТС, подвергающейся атаке, дезорганизующей структуру:

- S_0 – начальное состояние системы, когда все элементы самоорганизующейся МРТС находятся в безопасном состоянии, отсутствуют внешние информационные воздействия со стороны злоумышленника на потенциально имеющиеся уязвимости организационной структуры;
- S_1 – один элемент МРТС подвергается информационному воздействию;
- S_2 – два элемента МРТС подвергаются информационному воздействию;
- S_n – все элементы МРТС подвергаются информационному воздействию.

Переход из одного состояния в другое определяется, с одной стороны, возможностями злоумышленника, оказывающего информационное воздействие, а с другой – техническими характеристиками, определяемыми ресурсами элемента МРТС, задействованными для обработки. Информационное воздействие может быть осуществлено злоумышленником, например, путем посылки пакетов, использующих уязвимости, активной постановкой помех, что позволяет охарактеризовать события его возникновения интенсивностью. Возвращение элемента МРТС в безопасное состояние можно определить интенсивностью обратного перехода. Формальное представление функционирования такой системы целесообразно описать с использованием аппарата цепей Маркова.

На рис. 1 представлена последовательность состояний S_0, S_1, S_2,…, S_n системы, где $\mu_{j,i}$ – интенсивность, характеризующая программно-аппаратные возможности выхода элемента из небезопасного состояния, $\lambda_{i,j}$ – интенсивность информационного воздействия со стороны злоумышленника.

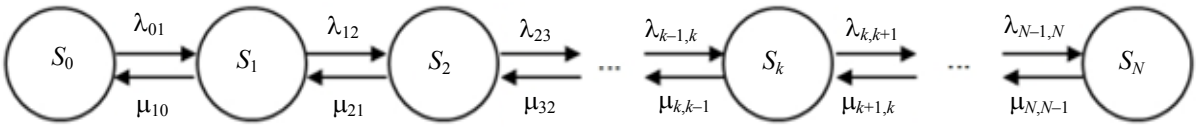


Рис. 1. Граф переходов состояния системы

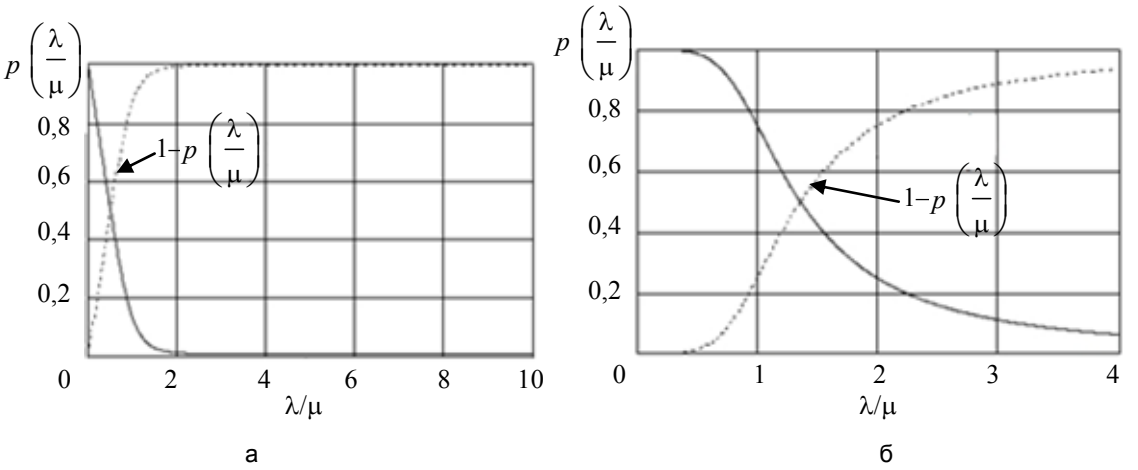
При допущении, что события изменения состояния ИБ двух элементов должны быть разнесены по времени, становится возможным произвести вероятностную оценку нахождения системы в безопасном состоянии на основе марковских процессов гибели и размножения.

Используя систему уравнений Колмогорова, можно вычислить вероятность состояния ИБ, показывающую количество элементов, подвергающихся информационному воздействию S_0, S_1, S_2 [12, 13]:

$$p_0 = \left[1 + \frac{\lambda_{01}}{\mu_{10}} + \frac{\lambda_{01}\lambda_{12}}{\mu_{10}\mu_{21}} + \ldots + \frac{\lambda_{n-1,n}\lambda_{n-2,n-1}\ldots\lambda_{01}}{\mu_{n,n-1}\mu_{n-1,n-2}\ldots\mu_{10}}\right]^{-1}, \; p_1 = \frac{\lambda_{01}}{\mu_{10}} p_0, \; p_2 = \frac{\lambda_{12}}{\mu_{21}} p_1. \quad (1)$$

В случае, когда известны интенсивности $\lambda_{i,j}$ и $\mu_{j,i}$, образуемые информационным воздействием со стороны злоумышленника и техническими факторами, становится возможным определить зависимость вероятности безопасного состояния. Изменения отношения $\frac{\lambda_{i,j}}{\mu_{j,i}}$ отражены на графиках (рис. 2) вероятности безопасного (сплошная линия) и небезопасного (прерывистая линия) состояний системы. На

рис. 2, а, представлены вероятности нахождения системы в состоянии S_0, на рис. 2, б, – вероятности нахождения в группе состояний S_0, S_1, S_2,…, S_k, при $k<n$, когда невозможность функционирования нескольких элементов не является критической для выполнения задач группировки.



а б

Рис. 2. Зависимость вероятности безопасного состояния системы p: вероятность нахождения системы в состоянии S_0 (а); вероятность нахождения в группе состояний S_0, S_1, S_2,…, S_k, при $k<n$ (б)

Модель поведения системы в динамике предполагает, что действия группировки происходят в агрессивной среде. Переходы из состояния в состояние могут происходить в любой момент времени и зависят от возможностей и стратегии применения информационного воздействия со стороны злоумышленника. Количество находящихся под информационным воздействием элементов МРТС может увеличиваться, уменьшаться, а также оставаться неизменным, что оказывает влияние на организационную структуру и вероятность нахождения группировки в безопасном состоянии. Интенсивность переходов из безопасного в небезопасное состояние может подвергаться изменениям в различных точках временной шкалы в зависимости от выбора стратегии информационного воздействия. Исходя из этого, для аналитического моделирования с целью оценки вероятности нахождения системы в безопасном состоянии в момент времени необходимо рассматривать функциональные зависимости интенсивностей переходов $\lambda_i(t)$ и $\mu_j(t)$.

В этом случае система уравнений Колмогорова будет выглядеть следующим образом:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = \mu_1(t)p_1(t) - \lambda_0(t)p_0(t), \\ \quad \ldots \\ \dfrac{dp_i(t)}{dt} = \lambda_{i-1}(t)p_{i-1}(t) + \mu_{i+1}(t)p_{i+1}(t) - (\lambda_i(t) + \mu_i(t))p_i(t), \\ \quad \ldots \\ \dfrac{dp_n(t)}{dt} = \lambda_{n-1}(t)p_{n-1}(t) - \mu_n(t)p_n(t) \end{cases} \qquad (2)$$

при условии $\sum p_i(t) = 1$.

Использование функций $\lambda_i(t)$, описывающей информационное воздействие, и $\mu_j(t)$, характеризующей выход элемента из небезопасного состояния, или их отношения $\dfrac{\lambda_i(t)}{\mu_j(t)}$ в выражении (1) позволяет анализировать вероятностные показатели состояния ИБ системы в динамике для различных моментов t с учетом (2). Например, если элемент мультиагентной системы обладает возможностью фильтрации информационных сообщений, посылаемых в процессе информационного противоборства, то часть из них может не обрабатываться. На графике (рис. 3) представлена смоделированная зависимость нахождения мультиагентной системы однотипных элементов в безопасном состоянии (сплошная линия) и небезопасного (прерывистая линия) для линейного роста с течением времени функции $\lambda_i(t) - \Delta\gamma$, при постоянном $\mu_j(t) = 1$, где $\Delta\gamma$ изменяется случайным образом в интервале от 0 до 0,2, когда безопасное состояние предполагает наличие нескольких работающих элементов мультиагентной РТС. Такие скачки могут образовываться в результате выбора злоумышленником стратегии информационного воздействия на техническую систему, определяющей частоту появления дезорганизующих событий или синергетического эффекта. При известной зависимости функций $\lambda_i(t)$ и $\mu_j(t)$, описывающих события информационных воздействий, можно определить граничные состояния системы и требуемые характеристики средств защиты.

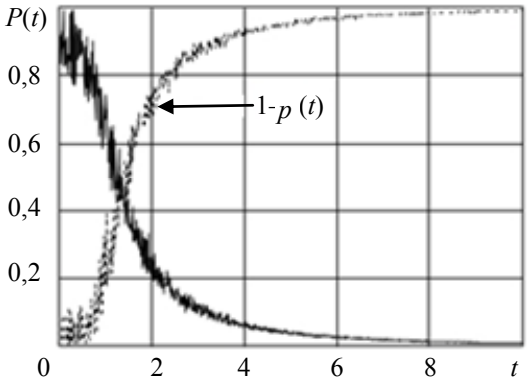


Рис. 3. Зависимость вероятности нахождения системы в безопасном состоянии в моменты времени *t*

Деструктивное воздействие на организацию структуры групповых МРТС может осуществляться как через уязвимости алгоритмов, обеспечивающие движение в направлении к цели [14, 15], так и через алгоритмы, предназначенные для организации группового поведения. Знание структуры МРТС с самоорганизующимся поведением позволяет использовать подход для оценки вероятности безопасного состояния. На рис. 4 показана МРТС, состоящая из четырех однотипных агентов, действия которых синхронизированы по времени таким образом, что в момент времени Δt_1 информацию анализирует элемент с номером 1, Δt_2 – номер 2 и т.д.

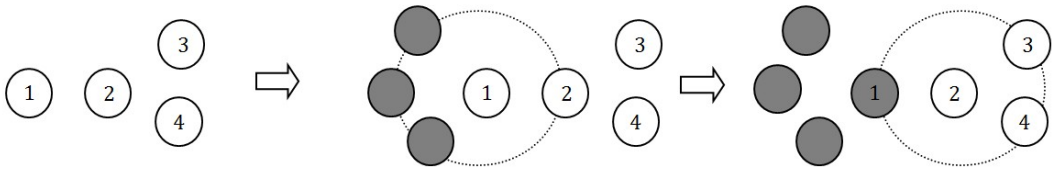


Рис. 4. Состояния группировки: безопасное состояние (а); появление дезорганизующих объектов (б); воздействие дезорганизующих объектов на элемент (в)

На рис. 4, а, группировка находится в безопасном состоянии S_0. На рис. 4, б, в зоне видимости первого элемента появились три объекта, оказывающие на него дезорганизующее информационное воздействие. Если интенсивности информационного воздействия со стороны каждого элемента одинаковы, в приводимом примере для перехода S_0–S_1 графа (рис. 1) значения λ_{01}=3, μ_{10} =1. Для ситуации, изображенной на рис. 4, в, переход S_1–S_2 характеризуется значениями λ_{02}=1, μ_{20} =2. Аналогичным образом рассматриваются остальные переходы. Возможны и другие случаи, зависящие от архитектуры взаимодействия и от расположений элементов, оказывающих деструктивное информационное воздействие, однако, если известна структура мультиагентной РТС и интенсивности переходов из состояния в состояние, то можно получить аналитическое выражение (2) для исследования вероятностей безопасного состояния. Для простейшего случая на рис. 5 дана аналитическая зависимость вероятности нахождения системы в состояниях S_1, …, S_5 группировки из 9 элементов при постоянном отношении интенсивностей информационного воздействия и выхода элемента из небезопасного состояния $\dfrac{\lambda_i(t)}{\mu_j(t)} = 1$.

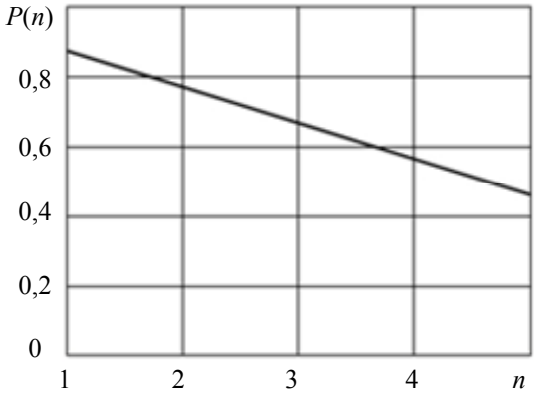


Рис. 1. Вероятность нахождения системы в состояниях S_1,…S_5

Изменение значений интенсивностей позволяет прогнозировать вероятность перехода из небезопасного в безопасное состояние в условиях агрессивной информационной среды. В случае предполагаемого роста интенсивности информационного воздействия со стороны злоумышленника на отдельные узлы архитектуры взаимодействия элементов появляется возможность определять комплекс мероприятий (разработка систем защиты, увеличение производительности и т.д.), обеспечивающих рост интенсивности выхода элемента из небезопасного состояния.

Заключение

В работе показан метод оценки безопасного состояния МРТС, подвергающейся информационному воздействию, направленному на дезорганизацию структуры, на основе подхода, использующего аппарат марковских цепей. Исследовано применение аппарата марковских цепей для моделирования процессов информационного воздействия на организационную структуру децентрализованной МРТС. Приведены формульные зависимости аналитического моделирования с целью получения вероятностных значений нахождения системы в безопасном состоянии.

Новизной подхода является описание вероятности состояний информационной безопасности МРТС с самоорганизующимся поведением, подвергающейся атаке, направленной на дезорганизацию структуры, через характеристики интенсивностей изменения состояний, зависящих от процессов информационного воздействия, что позволяет выявить требуемые характеристики отдельных элементов на ранних стадиях проектирования.

Метод может быть использован для вычисления прогнозных значений вероятностных показателей состояний информационной безопасности МРТС с самоорганизующимся поведением, находящейся в агрессивной информационной среде.

References

1. Luo R.C., Chou Y.T., Liao C.T., Lai C.C., Tsai A.C. NCCU security warrior: An intelligent security robot system. *IECON Proceedings (Industrial Electronics Conference)*. Taipei, Taiwan, 2007, art. no. 4460380, pp. 2960–2965. doi: 10.1109/IECON.2007.4460380
2. Flann N.S., Moore K.L., Ma L. A small mobile robot for security and inspection operations. *Control Engineering Practice,* 2002, vol. 10, no. 11, pp. 1265–1270.
3. Peters J.F. Approximation spaces for hierarchical intelligent behavioral system models. *Advances in Soft Computing*, 2005, no. 28, pp. 13–30.
4. Krautsevich L., Lazouski A., Martinelli F., Yautsiukhin A. Risk-aware usage decision making in highly dynamic systems. *Proc. of the 5th International Conference on Internet Monitoring and Protection, ICIMP 2010*. Barcelona, Spain, 2010, art. no. 5476893, pp. 29–34. doi: 10.1109/ICIMP.2010.13
5. Prabhakar M., Singh J.N., Mahadevan G. Nash equilibrium and Marcov chains to enhance game theoretic approach for vanet security. *International Conference on Advances in Computing, ICAdC 2012*. Bangalore, Karnataka, India, 2013, vol. 174 AISC, pp. 191–199. doi:10.1007/978-81-322-0740-5_24
6. Wyglinski A.M., Huang X., Padir T., Lai L., Eisenbarth T.R., Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors. *IEEE Micro*, 2013, vol. 33, no. 1, art. no. 6504448, pp. 80–86.
7. 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.
8. 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.
9. Dey G.K., Hossen R., Noor M.S., Ahmmed K.T. Distance controlled rescue and security mobile robot. *Proc. of the International Conference on Informatics, Electronics and Vision, ICIEV 2013.* Dhaka, Bangladesh, 2013, art. no. 6572602, pp. 1–6. doi: 10.1109/ICIEV.2013.6572602
10. Komov S.A. et. al. *Terminy i opredeleniya v oblasti informatsionnoi bezopasnosti* [Terms and definitions in the field of information security]. Moscow, AS-Trast Publ., 2009, 304 p.
11. Mondada F., Gambardella L.M., Floreano D., Nolfi S., Deneubourg J.-L., Dorigo M. The cooperation of swarm-bots: Physical interactions in collective robotics. *IEEE Robotics & Automation Magazine*, 2005, vol. 12, no. 2, pp. 21–28.
12. Ventsel' E.S., Ovcharov L.A. *Teoriya sluchainykh protsessov i ee inzhenernye prilozheniya* [Theory of stochastic processes and its application to engineering]. Moscow, Vysshaya Shkola Publ., 2000, 383 p.
13. *GOST R 51901.15-2005 (MEK 61165:1995) Menedzhment riska. Primenenie markovskikh metodov.* [State Standard 51901.15-2005 (IEC 61165:1995). Risk management. Application of Markov techniques]. Moscow, Standartinform Publ., 2005. 20 p. (In Russian)
14. Sridhar P., Sheikh-Bahaei S., Xia S., Jamshidi Mo. Multi agent simulation using discrete event and soft-computing methodologies. *Proc. of the IEEE International Conference on Systems, Man and Cybernetics,* 2003, no. 2, pp. 1711–1716.
15. Kirikova E.P., Pavlovsky V.E. Modelirovanie upravlyaemogo adaptivnogo povedeniya gomogennoi gruppy robotov [Modeling of controlled adaptive behavior of robots homogeneous group]. *Iskusstvennyi intellect* [Artificial intelligence], *2002,* no. 4, pp. 596–605. (In Russ.)

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

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

Шабанов Денис Павлович – аспирант, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), Санкт-Петербург, Россия, den_shabanov@yandex.ru

Чистов Виктор Владимирович – магистрант, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), Санкт-Петербург, Россия, chistov_vic@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

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

Denis P. Shabanov – student, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia, den_shabanov@yandex.ru

Viktor V. Chistov – student, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia, chistov_vic@mail.ru

Принято к печати 06.11.13
Accepted 06.11.13