The Estimation of Secure Condition of Multi-Agent Robotic System in Case of Information Influence on the Single Element

Igor' Alekseevich Zikratov, Ilja Sergeevich Lebedev, Viktoria Mihajlovna Korzhuk
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
zikratov@cit.ifmo.ru, lebedev@cit.ifmo.ru, vika@cit.ifmo.ru

Abstract—**The purpose of the work is the development of an approach that uses the instrument of Markov chains estimating the safe condition of multi-agent robotic system undergoing the processes of data influence. Proposed models, methods and approaches are aimed at ensuring the protected state of the multi-agent robotic system in the situation of information impact. It is supposed that the change in the state of objects with information about the target location is described by the rules of group behavior. It is considered that the feature of the simulation is to assess the system state achievements of element affecting the information security accessibility index applied to multi-agent robotic systems. The application possibilities of the scientific tools of Markov process for modeling information influence on the decentralized multi-agent robotic system have been investigated. The formula dependence for the analytical modeling with the purpose of obtaining probabilistic values of the system safe condition is identified. The experiment is aimed at assessing the state of information security robotic system exposed to unauthorized effects giving the opportunity to compare the data. The obtained results can be widely used in solving practical problems associated with the analysis of information security of multi-agent robotic systems with self-organizing behavior.**

I. Introduction

Interest in the feasibility of self-organizing systems which use “natural” algorithms of interaction between the individual elements as well as to the development of teamwork methods and cooperative behavior, where the achievement of the preset goal is possible only by joint actions, necessitates a comprehensive study of models and methods of Swarm intelligence.

Multi-agent robotic system (MARS) is a computational system that acquires and analyzes sensory data or external stimulus and executes behaviors that produce effects in the environment. It decides for itself how to relate sensory data to its behaviors in its efforts to attain certain goals. Such a system is able to deal with unpredictable problems, dynamically changing situations, poorly modeled environments, or conflicting constraints.

The motivation behind the research and development in multi-agent robotic systems comes from the fact that the decentralized multi-robot approach has a number of advantages over traditional single complex robotic systems approaches. Distributed robots can readily exhibit the characteristics of structural flexibility, reliability through redundancy, simple hardware, adaptability, reconfigurability and maintainability. The robots can interact with their local environments in the course of collective problem solving. Responding to different local constraints received from their task environments, they may select and exhibit different behavior patterns, such as avoidance, following, aggregation, dispersion, homing, and wandering. These behaviors are precisely controlled through an array of parameters (such as motion direction, timing, lifespan, age, etc.), which may be carefully predefined or dynamically acquired by the robots based on certain computational mechanisms.

A huge number of projects is devoted to the problems of optimizing behavior in a variety of environments in situation when there is no external management, control or coordination of single elements. However, it should be noted that attention paid to the protected status of multi-agent systems in proposed solutions is not enough, as far as their functioning can occur in environments that have inherent potential of information impact on individual elements and the use of software, hardware and algorithmic vulnerabilities of different levels.

Thus, the development of scientific and methodological apparatus designed to optimize the operation of multi-agent systems defines ensuring of information security (IS) as one of the subtasks. This involves the development and implementation of mechanisms for control and monitoring of the behavior of a plurality of physically independent mobile robots subordinated to the rules defining achievement of the goal.

II. Statement of the Problem

A. *Features of information security assurance of robotic system*

Robotic systems (RS) have specific vulnerabilities that cause the necessity to adapt scientific and methodological apparatus of information security to the functioning conditions.

Specificity of the structure and behavior of multi-agent robotic systems (MARS), which are capable to self-organize (for example swarm robotic system) allow us to identify a precondition number that determine potential vulnerabilities:

- the lack, the insufficiency and the relativity of information about the current state and location of each device;
- comparatively weak intensity of the information exchange between the device and the coordinating center;
- the originally-based autonomy of individual action of RS elements;
- the possibility of action of individual elements of the RS group outside the controlled area;
- the imperfection (or the lack) of mechanisms of element identification and authentication leading to significant delays in detection of intrusion in the RS group;
- limited capability of the tools of detection of the abnormal behavior of the RS elements.

The possibility of implementation of information security threats with respect to RS with the capability of self-organization on software, algorithmic and resource level is discussed. Features of swarm RS allow us to identify a number of categories of potential attacks on the integrity, confidentiality and availability of information, for which protection mechanisms are insufficient:

- information gathering;
- unauthorized access attempts;
- denial of service;
- suspicious activity.

The retrieval of analytical dependences enabling to identify abnormal activity or manifestation of informational events requiring attention is not always possible. In this regard there is a need of modeling of the system for the purpose of analysis, state monitoring, detecting of attributes of abnormal behavior of the individual element.

B. *The implementation of attacks on multi-agent robotic system*

The main mechanisms for the implementation of attacks on MRS that realize mentioned threats are:

- attacks on the communication channels;
- the difficulty of identification and authentication of agents in the system;
- the physical implementation of “foreign” robots, which can be captured and reprogrammed by an attacker.

In this paper we consider a model of MARS information security that allow to resist the attacks associated with the physical impact of the implementation of the "foreign" elements, which task is to avoid or reduce the effectiveness of collective action with decentralized management.

The possibility of implementing information security threats in relation to the multi-agent robotic system (MARS) is considered as the entire system as well as a separate element [1 - 3]. Most commonly used type of attack in automated systems is “failure in service”. One of the features of the MARS from the viewpoint of IS is that each element can be simultaneously as an object as well as access subject. Establishment of conditions under which legal agents (other single elements of RS) can not get access to the provided information of a single element of the RS or the access is difficult pose a threat to the availability of MARS information [4, 5]. We assume the safe state of the MARS as a state when the conditions of protection of the confidentiality, availability and integrity for all single elements of the system are complied, allowing acting promptly to ensure the conditions of group behavior.

Most of the existing methods and DDoS-attack (Distributed Denial of Service) detection systems can effectively recognize and fight with escalating attacks aimed at filling the channel capacity and the excess of the normal load of single devices. Though, today the most relevant methods of analysis and detection of DDoS-attacks are those that occur in the low-level mode (Low Rate DoS), which feature is the lack of “overload” of channels and other statistical anomalies.

With respect to the MARS these attacks are possible by impacting on the algorithms of managing and control or environmental condition creation, that do not allow using the functionality providing the rules of collective behavior.

In simplified form we suppose that the change in the state of objects with information about the target location is described by the rules of group behavior [6, 7]. The realization of the rules for a single RS item is based on the system [6]:

$$\begin{cases} \vec{v} = M\vec{v}_1 + T\vec{v}_2, \\ \vec{L} = \vec{v}t, \\ \vec{L} \to \min, \end{cases} \qquad (1)$$

where:

$\vec{v}_1$ - the velocity vector of the target displacement setting (determined by the direction of motion to the target);

$\vec{v}_2$ - the velocity vector of displacement implemented by interaction elements (compliance required intervals and distances);

M and *T* – the coefficients of "influence on the behavior character of the group";

$\vec{v}$ - the velocity vector of displacement depending on the priorities (determined by the coefficients M and T);

$\vec{L}$ - the vector of path to the goal.

In the case of information confrontation attacker tries to impact on group behavior which leads to errors in the formation of vectors v_1 and v_2 of single element that will affect the technical, functional and energy capabilities of the group.

III. The model of the single element

The basis of multi-agent system is the single element. For simplicity we assume that the elements of RS under consideration are the same and homogeneous as in the case of for example swarm systems.

At the end of the targeting process of a group of RS decentralized elements, functioning of the single element is to collect information about the actions of neighboring elements and on the basis of its processing implementation of the rules of group behavior.

In this system, the individual element may be in the following states:

S_0 - RS element performs actions aimed at ensuring the conditions (1);

S_1 - on the RS element receives commands and messages, "consuming" computing resources but not breaking the rules of group behavior. Element is busy because of processing it.

Rules of group behavior are not realized by the device for a some period of time, signals to other elements of the group are not transferred, but the device itself is technically serviceable and "by inertia" can perform actions aimed at ensuring the conditions (1), based on the data obtained at the time prior to the transition to this state;

S_2 - the RS element receives commands, messages, leading to actions that violate the rules of group behavior.

RS element is in a state that actively or passively counteracts to implementation of group behavior rules. A single element can be fixed or carry out the movement not aimed at supporting condition (1) or inhibit movement "divert" the other elements in the opposite direction from the target, transmit false reports that disorganize participants of the collective behavior.

Let us consider the features of the simulation, the purpose of which is to assess the system state achievements of element affecting the IS accessibility index applied to MARS.

Assuming that the transition of RS element from S_i to S_j is characterized by a Poisson process with intensities $\lambda_{ij}(t)$ or $\mu_{ji}(t)$, we represent the graph of its states shown in Fig. 1.

Using this graph the state of information security for a single RS element can be described by the Kolmogorov equation system:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = \mu_{10}(t)p_1(t) - \lambda_{01}(t)p_0(t), \\ \dfrac{dp_1(t)}{dt} = \lambda_{01}(t)p_0(t) + \mu_{21}(t)p_2(t) - \\ \qquad -(\lambda_{12}(t) + \mu_{10}(t))p_1(t), \\ \dfrac{dp_2(t)}{dt} = \lambda_{12}(t)p_1(t) - \mu_{21}(t)p_2(t). \end{cases} \qquad (2)$$

The lack of information from any RS element in the required moment of time means the impossibility of making optimal actions to achieve the goal by the group [8, 9].

The degree of influence of the state S_1 to purpose achievement depends on the dynamics of the environment change and the length of stay in it by single RS element. While the information impacting aimed at increasing the intensity of the system is in state S_1 and S_2, different processes that prevent the fulfillment of the group goal may appear.

The transition of any RS element in the state S_1 and/or S_2 impacts on the whole system.

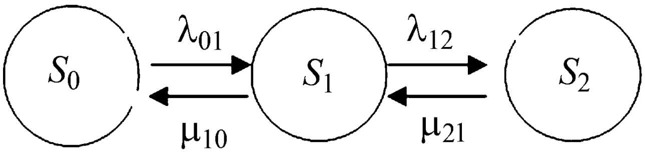

Fig.1. Graph of the states of RS element

As follows from (2), the safety state assessment for various kinds of information impact on the RS element can be made in accordance with the values of the probabilities of being in states S_1 and S_2. For the S_2 this value will take the form (for the stationary states) [10]

$$p_2 = \frac{\lambda_{12}}{\mu_{21}} \frac{\lambda_{01}}{\mu_{10}} p_0 \ . \tag{3}$$

The probability of finding the system in state S_1 or S_2:

$$p_1 + p_2 = \frac{\lambda_{01}}{\mu_{10}} p_0 (1 + \frac{\lambda_{12}}{\mu_{21}}) \ . \tag{4}$$

Taking into account the conditions of stationary of Markov processes of birth and death which include graph of state presented on fig. 1 [10],

$$\frac{\lambda_{ij}}{\mu_{ji}} \le x < 1 \ , \tag{5}$$

the plots of the dependence of the probability of finding the system in a safe condition (p = 1 - p_2) from the intensity ratio of the transition   for different probabilities   of finding the system in the initial state are shown in Fig. 2 and Fig.3.

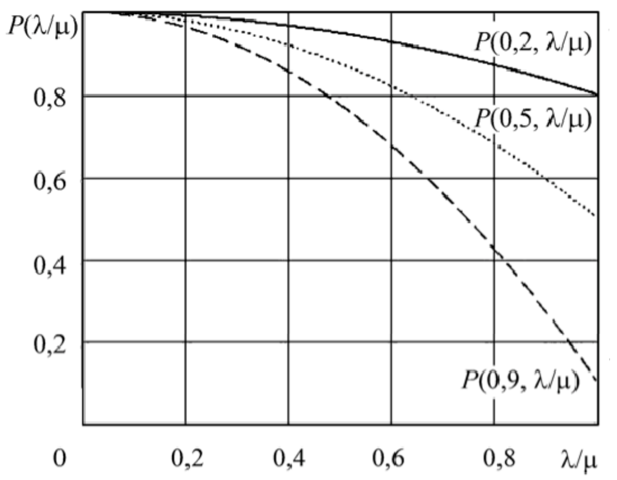

Fig.2. Graphics of the probability of finding the system in a safe state for the ratio (3).

In the shown graphs the single element is in the condition $0 < \frac{\lambda_{ij}}{\mu_{ji}} < 1$ when the system tends to a state S_0. At the same time (in the simulation of processes under the information impact) condition (5) can be broken subject to condition (1) in order to put the system into the extreme state with purpose of disorganization of element action.

One of the weakest points of this approach is that it is necessary to know the functional dependence of the intensities of transitions [11, 12]. Transition intensities $\lambda_{ij}(t)$, $\mu_{ji}(t)$ and the ratio $\frac{\lambda_{ij}}{\mu_{ji}}$ for a single RS element are determined by initially given technical characteristics, associated with computing speed of on-board control device, time of access to resources, speed of information exchange between the various components.

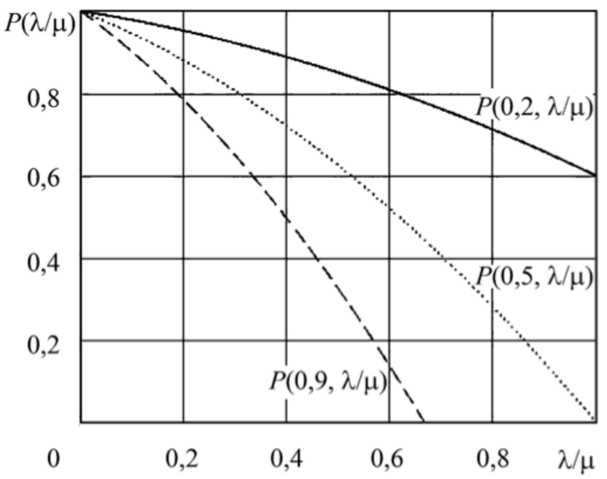

Fig.3. Graphics of the probability of finding the system in a safe state for the ratio (4)

Having information about different modes we can find ranges of ratio $\frac{\lambda_{ij}}{\mu_{ji}}$. If the transition intensities $\lambda_{ij}(t)$, $\mu_{ji}(t)$ are known excess of the defined limits can be interpreted as an indirect indicator displaying information impact [13].

The obtained dependences allow us to estimate the potential effects of information impact on one or several elements of RS. To carry out computational experiments let consider the simplest multi-agent robotic system composed of the similar elements.

Let there be a conventional multi-agent system with self-organizing behavior – a group of the similar items [14,15]. Performance of the tasks is engaged by simultaneously n RS elements. Each of these items can be replaced by k items. Suppose that the probability of a safe system state is defined by the formula

$$P = (1-(1-p)^k)^n \tag{6}$$

where p is the probability of finding the RTS element in a safe state.

Using the ratio (5) and (6) with condition of particular interest of the state S_2 for a single RS element we can obtain the formula

$$P = \left(1 - \left(1 - \frac{\lambda_{12}}{\mu_{21}} \frac{\lambda_{01}}{\mu_{10}} p_0\right)^k\right)^n \ . \tag{7}$$

If it is required to analyze of location of the individual item in the state S_1 or S_2, then

$$P = \left(1 - \left(1 - \frac{\lambda_{01}}{\mu_{10}} p_0 \left(1 + \frac{\lambda_{12}}{\mu_{21}}\right)\right)^k\right)^n . \qquad (8)$$

The derived formulas allow us to evaluate the finding of the multi-agent robotic system, which has the plurality of similar elements in unsafe condition depending on the ratio of the transitions intensities $\frac{\lambda_{ij}}{\mu_{ji}}$ defined by the condition (5).

Fig.4 and Fig.5 show plots of the probability of finding the system in a safe state (1 – *P*, depending on the ratio of transition intensity with regard to condition (5) of the five elements of the same type where each of these is reserved by three element (solid line), and a system of eight elements reserved by five elements (dashed line).

The obtained dependences can be used for example to select different software and hardware configurations for single items of robotic system based on information impact intensity providing the change of PS element state or justification of the structure and quantitative composition of the MARS.

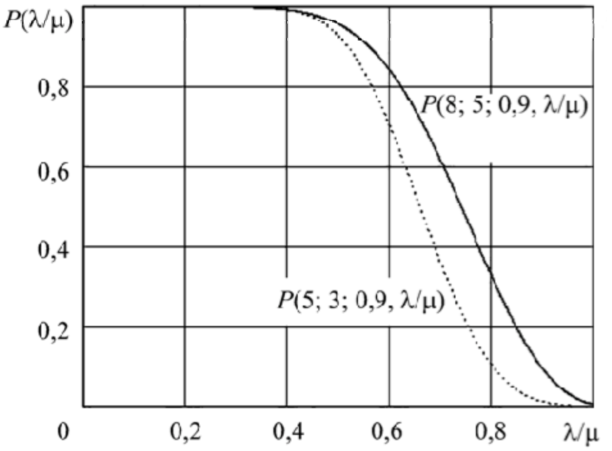

Fig.4. Probabilities of finding the system in a safe state (1 - *P*) for the conditions (7)

Fig. 6 and Fig.7 show graphics allowing assessing two multi-agent systems with identical elements (see Fig.4 and Fig.5) depending on changes in the intensities of transitions $\frac{\lambda_{ij}}{\mu_{ji}}$ and taking into account the conditions of stationary.

The graph shows the ranges of investigated states when one is preferable to the other architecture.

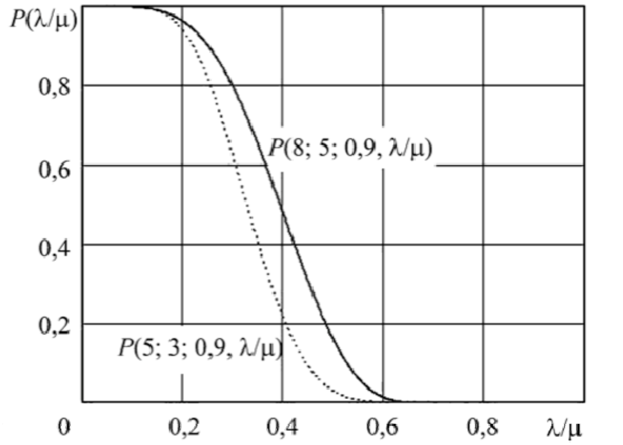

Fig.5. Probabilities of finding the system in a safe state (1 - *P*) for the conditions (8)

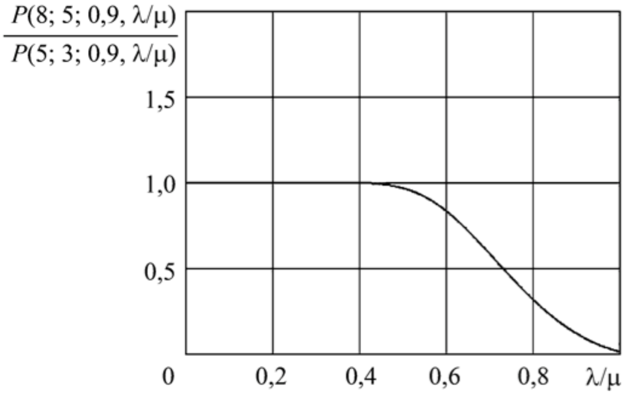

Fig.6. Graph 1 for comparison of architectures

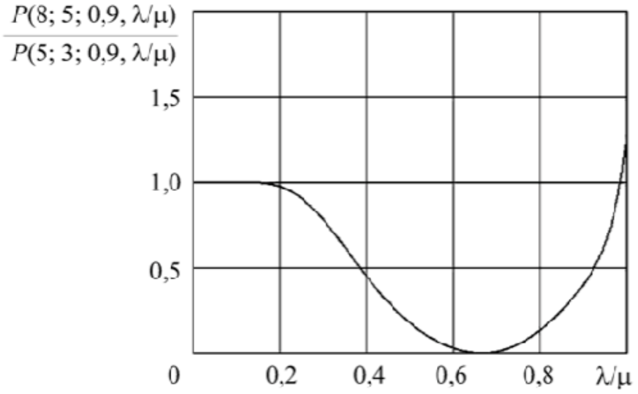

Fig.7. Graph 2 for comparison of architectures

IV. Conclusion

This paper describes the approach to the assessment of the potential impact on the multi-agent robotic system with self-organizing behavior based on scientific and methodological apparatus of Markov chains. Proposed models, methods and approaches are aimed at ensuring the protected state of the multi-agent robotic system in the situation of information impact.

The presented approach allows to:

- get a probabilistic results of assessment of information impact on the swarms robotic system without a detailed analysis of the properties of a particular algorithm;
- assess the boundary state of the system if it is possible to define functional dependencies of the intensity of the transition of functions $\lambda_i(t)$ and $\mu_j(t)$ from characteristics of information impact processes (in order to make recommendations to the required tactical-technical characteristics of protection tools);
- determine confidence limits and threshold values of probability indicators of the system state based on results of simulation (for the detection of abnormal activity).

Because of the complexity of the implementation of protection systems for MARS with decentralized behavior, it is necessary to use the methods of external monitoring of the information security state and systems with different trust models.

Modeling and simulation of multi-agent robotic system state based on Markov processes allows analyzing the security events. The obtained results can be widely used in solving practical problems associated with the analysis of information security of multi-agent robotic systems with self-organizing behavior.

Acknowledgment

We would like to thank our colleagues who helps us to realize the idea of the article, our postgraduate student for translating the text into English and special thanks to 17th FRUCT Conference organizers for the great possibility of publishing, presentation of our results and getting incomparable experience.

References

[1] R.C. Luo, Y.T. Chou, C. T. Liao, C.C. Lai, A.C Tsai, NCCU Security Warrior: An Intelligent Security Robot System, *IECON Proceedings (Industrial Electronics Conference)*, 2007, pp.2960-2965.

[2] N.S. Flann, K.L. Moore, L.A. Ma, Small Mobile Robot for Security and Inspection Operations, *Control Engineering Practice*, 2012 vol. 10 (11), pp.1265-1270

[3] I.A. Zikratov, E.V. Kozlova, T.V. Zikratova, Analysis of Vulnerabilities of the Robotic Complexes with Swarm Intelligence, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics,* vol. 5(87), pp.149-154.

[4] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, K. Venkatasubramanian, Security of Autonomous Systems Employing Embedded Computing and sensors, *IEEE Micro*, 2013 vol. 33(1), pp.80-86.

[5] E.N. Koval, I.S. Lebedev, General Model of Security of the Robotic Systems, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2013 vol. 4(86), pp.153–159

[6] Dey G.K., Hossen R., Noor M.S., Ahmmed K.T. Distance Controlled Rescue and Security Mobile Robot // Electronics and Vision: International Conference on Informatics 2013, ICIEV. 2013, art. No. 6572602.

[7] F. Mondada, L. M. Gambardella, D. Floreano, S. Nolfi, J.-L. Deneubourg, M. Dorigo, SWARM-BOTS: Physical Interactions in Collective Robotics, *IEEE Robotics & Automation Magazine*, June 2005, vol. 12, pp.21-28.

[8] GOST R 51901.15-2005 (IEC 61165: 1995). Risk management. Application of Markov methods.

[9] P. Sridhar, S. Sheikh-Bahaei, S. Xia, M. Jamshidi, Multi-agent Simulation Using Discrete Event and Soft-computing Methodologies, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, 2003, vol. 2, pp.1711-1716.

[10] E.S. Wentzel, L.A. Ovcharov, *Theory of Random Processes and Its Engineering Application*. Moscow: High School., 2000.

[11] I.A. Zikratov, T.V. Zikratova, I.S. Lebedev, Trust Model of Information Security of Multi-Agent Robotic Systems with Decentralized Control, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, vol. 2 (90), pp.47-53.

[12] I.S. Lebedev, T.V. Zikratova, D.P. Shabanov, V.V. Chistov, Assessment of the State of Information Security of Multi-Agent Robotic Systems under the Information Impact, *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014 vol. 2(90), pp.53-59.

[13] I.A. Zikratov, I.S. Lebedev, E.V. Kuzmich, A. Gurtov, Securing Swarm Intellect Robots with a Police Office Model, *Application of Information and Communication technologies - AICT 2014*, 2014, pp.32-37.

[14] J. F. Peters, Approximation Spaces for Hierarchical Intelligent Behavioral System Models, *Advances in Soft Computing*, 2005, vol. 28 pp.13-30.

[15] I.A. Zikratov, E.V. Kuzmich, T.V. Zikratova, Simulation of Attacks on Robotic Systems with Swarm Intelligence, *Proceedings of the I International Scientific and Practical Conference "Information security in the Strategy Kazakhstan-2050"*, 2013, pp.308-313.