The Problem of Assessing Information Security Risks for Robotic Systems

E.S. Basan[1], **A.S. Basan**[1]

[1]Southern Federal University, Chehov str. 22, Taganrog, Russia, 347922

Abstract. Today, robotic systems are becoming very popular. They are typically used to monitor critical objects. Human lives often depend on the correct operation of a robotic system. Therefore, risk analysis of a robotic information system is an important task. However, to date there is no standard that describes this process. We conducted a study of existing standards for industrial control system and typical information systems. We have identified one common problem. If the risk assessment process is still described in these documents, then the analysis of initial security is not considered at all. This assessment of the initial level of security, the analysis of structural and functional characteristics is a very important task. If we are not completely knowledgeable about our system, then we may not fully assess the risks. Therefore, an attacker can take advantage of this. This article also discusses security incidents related to robotic systems. We concluded that an attacker may not have special means to attack, and at the same time causes substantial damage to the robotic system. Indeed, the main problem in the analysis of robotic systems is the difference of this type of network from the typical computer networks, which in turn requires the creation of new methods and approaches to the analysis of the security of a network of mobile robots.

1. Introduction

As is well known, the industry associated with robotic systems is actively developing. Automation in production, military areas is becoming a mass phenomenon. Special types of networks are being created; new ways of data processing and decision-making methods are being introduced, as well as artificial intelligence [1]. To date, topics related to the creation of robotic systems are quite relevant. Such systems are created not only for industrial and military purposes, but also for consumer services (such as Smart City, Smart Home) and farms (Smart Farm, Smart Greenhouse). Systems equipped with artificial intelligence, are capable of varying degrees of autonomy, gaining widespread popularity. Unmanned vehicles, surface autonomous vehicles, submarine and air autonomous vehicles, and much more can be attributed to such systems. All systems listed above, ranging from autonomous robots to complex intelligent robotic systems have common features, and especially in terms of information security. In this study, a robotic system is a group of robotic devices, united in the performance of one or several similar tasks perform their functions through communication channel or autonomous mode. Devices can be in any environment (air, underwater, surface, non-deterministic, etc.) and at the same time can be equipped with artificial intelligence, or perform predefined sets of actions. Robots can be both stationary and mobile. Elements of robotic and intelligent systems are used in practice in industrial control system (ICS), in smart home systems or the Internet of things. Due to the fact that these systems are only developing and there are no any information security standards for them, certified security equipment, etc., improving the security of such systems becomes a problem. In addition, most approaches to creating robotic systems are also not standardized. There is a huge range of software and hardware for creating the control mechanisms of the system, a large number of operating system and application software, and solutions can be open or proprietary. Scientists have developed a large number of methods and algorithms for controlling a robotic system [2]. Conducting a security analysis of a robotic system is really becomes a problem. The same applies to the process of selecting current threats and determining the likely intruder. As you know, the process of creating a security system for any information system has a clearly structured algorithm [3]. At the first stage, information security risks are analyzed, protection requirements are defined, and a security policy is built. But in order to analyze the risks or determine the protection requirements, to develop a security policy, you need to clearly understand what you are dealing with. The operator of the information system must clearly know the structure of his system; understand its functionality and capabilities. The owner or operator of an information system relies on two factors: the value of the assets to be protected and the likelihood of an information security threat being realized when assessing risks. Typically, information security risks are associated with a violation of the integrity, confidentiality, accessibility of information that can be presented in the form of electronic resources (databases, web resources, electronic documents, etc.) and information resources on solid media (servers, paper documents, hard drives, etc.) [4]. Accordingly, the implementation of a threat that is associated with risk leads to damage. Unlike a typical information system, a robotic system or an automatic process control system works not only with the processing, storage, transmission, collection of information, but also with the control object. That is, the robotic system has assets not only in the form of information, but also in the form of the object of informatization, which can be the environment, the production process, and humans. Thus, the attacker has more opportunities to influence the system and obtaining benefits can be achieved not only by violating confidentiality, integrity, accessibility of information, but also by disrupting the object [5]. The object in this study means a certain entity that is controlled by a robotic system. The novelty of this study lies in the fact that the authors proposed a technique for assessing initial security; this technique will allow us to assess the initial risks of a robotic system associated with the presence of certain structural and functional characteristics and the capabilities of the intruder. Thus, the main goal of our study is to develop a methodology for assessing information security risks for a robotic system by assessing the initial security. To achieve this goal it is necessary to perform the following tasks:

- Study of the features of robotic systems, and the architecture of robotic systems;
- Structuring and systematization information about robotic systems;
- Determination of indicators to assess the degree of protection of the robotic system;
- Development of methodology of assessing the level of initial security.

The remainder of the paper is structured as follows. Section 2 summarizes existing related work. Section 3 describes the analysis of the structural and functional characteristics of robotic systems. and Section 5 is conclusion and future work

2. Related work

The closest methodical document, which describes a process of evaluating the initial security level, is: «Method for determining threat to the security information in information systems» by FSTEK [6]. This technique describes the procedure for developing a threat model and an intruder model for a typical information system. A method for assessing initial security is described. The method of assessing the initial security described in the methodology basically uses an analysis of the structural and functional characteristics of the system. The operator can evaluate how much the system is potentially susceptible to attacks, depending on what characteristics the system possesses. If it is necessary to assess the initial security of the robotic system, this method is not suitable for two reasons. Firstly, because the structural and functional characteristics of a typical information system and a robotic system differ significantly. Secondly, it is not completely clear on the basis of what the degree of security of a particular characteristic was determined. FSTEC Order No. 31 «Approval requirements for the provision information security in the industrial control systems (ICS) on critical infrastructure, potentially dangerous objects, and objects posing an increased danger to life and health and for the environment» was published in 2014 [7]. This order addresses issues of ACS TP structuring, and also offers a variety of security subsystem. The standard describes the structural and functional characteristics of process control systems and gives the following levels:

- Operator (dispatch) control level (upper level);
- Automatic control level (middle level);
- Level of input (output) of data of executive devices (lower (field) level).

Despite the fact, that in the order to allocate separately autonomous management level, directly implying the protection of actuators and sensor system in the section, which deals with the protection subsystem, the specific features of the Autonomous level not taken into account. In addition, this document does not take into account that executive mechanisms (which may include sensor nodes, robots) themselves autonomous controls may take decisions or act in a separate group. At the same time, intermediaries between the group of executing devices and the operator (devices at the automatic control level) can often be absent when it comes to a fully distributed system. Currently, group management systems, group intelligence are gaining more and more popularity [8]. These systems will provide greater economic efficiency and eliminate a single point of failure. In the Russian legislation to date there are no regulations governing the security of such systems. One of the important points that are described in the law is those assets that need to be protected in ICS. In the automated control system of the objects of protection are:

- information (data) about the parameters (state) of a controlled (monitored) object or process (input (output) information, control (command) information, control and measurement information, and other critical (technological) information);
- software and hardware complex, including hardware (including workstations, industrial servers, telecommunications equipment, communication channels, programmable logic controllers, actuators), software (including firmware, system-wide, applied), as well as security information.

There are several more problems with applying these requirements to a robotic system. The means of protection that are used on automated systems must be certified, but if we talk about robotic system, it is not always possible to install special software and hardware on robots. There is also no information about choosing the applicable measures of protection, as this procedure depends on what threats are relevant to a target system. Despite the fact that the FSTEC threat database has a fairly large set of threats, the threats associated with mobile robots or robot group management systems or intelligent robot management are not taken into account [9].

In 2008, a safety standard for industrial control systems was issued. National Institute of Standards and Technology represents SP 800-82 Guide to Industrial Control Systems. In addition to this order, there are also foreign standards. For example, is the NIST, the ISO, but these standards are mainly aimed at examining protection systems for the Internet of things. NIST has developed a Framework for Improving Critical Infrastructure Cybersecurity, where represented the necessary security subsystems that should be implemented in information systems [10]. For each of the proposed security subsystems, there are specified sections of the standards where the procedure for developing each subsystem. This Framework presents a large number of requirements, but it is also not clear how to select a specific requirement for the system, how to assess the need to protect one or another component of the system. The organization has established and implemented the processes to identify, assess and manage supply chain risks [11]. The following assets must be considered when assessing risks according to this document:

- Physical devices and systems within the organization.
- Software platforms and applications within the organization.
- Organizational communication and data flows.
- External information systems.
- Resources (e.g., hardware, devices, data, time, personnel, and software).
- Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders.

The document provides references to other standards that allow realized risk assessment: CIS CSC, COBIT 5, ISA 62443-2-1: 2009, ISO / IEC 27001: 201 NIST SP 800-53. Most of these documents are in the public domain, but are paid, which makes it difficult to study. Nevertheless, it can be concluded that when assessing risks, documents do not refer to methods for determining the current threats. Thus, the issues related to the identification of current threats are practically not worked out.

In 2008, the NIST Special Publication 800-82 standard was introduced. This standard defines key components are:

- Control node. The control node consists of measurement sensors, a controller (includes equipment and actuators, such as PLC controllers, valves, switches, levers, motors) and variable systems.
- Human Machine Interface (HMI). Operators and engineers use the HMI to monitor, control and change set points, algorithms, control and set controller parameters.
- Remote diagnosis and support program. Remote diagnostic and support programs are used to prevent, recognize, and correct malfunctions.

This structure is fundamentally different from that presented in the FSTEC. In May 2015, the standard was released in the second version. The document describes the structure of ICS as follows. A typical ICS contains numerous control loops, human interfaces, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. Control loops utilize sensors, actuators, and controllers (e.g., PLCs) to manipulate some controlled process. A sensor is a device that produces a measurement of some physical property and then sends this information as controlled variables to the controller. The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. Actuators such as control valves, breakers, switches, and motors are used to directly manipulate the controlled process based on commands from the controller. As a whole, this document gives a clear understanding of what control systems are, a large number of examples of such systems, their architecture and description are given. This standard can serve as an example for creating a similar document for a robotic system. The document also provides a list of vulnerabilities specific to ICS. In addition, much attention is paid to network protection. Examples of firewall rules and network segmentation options are provided.

Another example is the Robot Security Framework (RSF) [14]. This article describes a security assessment system. Robotic system is divided into 4 components and evaluates the safety of each of them. At the same time, the assessment does not rely at all on the possible threats characteristic of each component of the system, and takes into account only the physical, network, firmware, and application. This Framework also lacks the ability to evaluate the intelligent control system of the robot, evaluate the robot if it is mobile, and the group control system. Authors hereby propose a framework based on four layers that are relevant divide them into aspects considered relevant to be covered. Also they provide relevant criteria applicable for security assessment. For each of these criteria they identify what needs to be assessed (objective), why to address such (rationale) and how to systematize evaluation (method).

3. Analyses of the structural and functional characteristics of robotic systems

The nodes of the robotic system collect information and, if necessary, control a remote object. Robots can be both stationary and mobile. Robots can act as autonomous, or they can be remotely controlled. Robots could be in active mode or in sleep mode if necessary. They can collect data on humidity, temperature, noise, pressure, light, etc., as well as perform previously defined sets of actions. Sensor nodes provide the ability to track various physical processes. A group of nodes can be networked according to the IEEE 802.11n, s standard, which is part of the IEEE 802.11 standards and allows to organize hierarchical wireless Ad-Hoc and mesh networks. In addition, ZigBee, 6LoWPAN, Thread, RPL, BLE, and other protocols support for communication [15]. It should be noted that mobile or stationary nodes can be combined into groups for distribution and collection of information from ground sensors, so that in case of a failure of one of the nodes the network was not disrupted, and the collected data was not lost.

The robots can be carried out by the group control system of robots (GCSR) [16]. Two methods of management strategy can be implemented in GCSR: centralized; decentralized (hybrid). When implementing methods of centralized management or hybrid control system, the group of robots has a “robot leader”. The GCSR solves the problems of forming subgroups and the distribution of tasks between them. The action of the robots in group or each subgroup is also plans to solve different tasks.

In other words, with a centralized strategy, the control system of each robot receives an algorithm of actions of this robot through information channels and implements it. In this case, the control systems of robots actually solve only the local tasks of controlling the parts of the robots; therefore, the main part of the robots group can have simple computing systems. This type of control system is also used in the case of mini- and micro-robots, when the dimensions of the robots don't allow placing a powerful computing complex on it. However, such the control system has a rather low reliability and is used for multiple duplication of the group leader [17].

The decentralized management strategy that leads to distributed group management systems seems more promising. In this case, the group control system is implemented by the dissemination of information among several robots or all robots of a group or subgroup. To date, a large number of different approaches to the creation of such decentralized GCSR have been developed. However, decisions both on the distribution of tasks and the formation of relevant subgroups, and on the management of the actions of robots in all cases are made by the robots themselves [18].

In contrast to the robotic structure, which is presented in the work of the Robotic security framework, we offer the following architecture of the robotic system, as shown in Figure 1. The main differences are that we separately distinguish such subsystems as: smart management and security system. This is very important when assessing threats and vulnerabilities, since these subsystems are significantly different from others. In addition, in the hardware system, we single out separately computing mechanisms, a sensory system and actuators, and auxiliary hardware [19]. In the case of a robotic system, it is not entirely correct to consider hardware as a single subsystem. This is due to the fact that the influence of the sensory system and computing by the attacker mechanisms or aggressive environments may vary and lead to different outcomes, and therefore leads to various risks. We define 10 security subsystems for a robotic system. These subsystems are suitable precisely for that part of the system where robots are represented. In our classification, there are no protection subsystems associated with the operator and the human factor. But we added such a subsystem as trust management, in our opinion this is a very important and basic subsystem. This is due to the fact that robots are often in an untrusted and uncertain environment and can be captured. Therefore, it is very important that robots communicate only with trusted agents.

4. Assessment of the level of initial security

When identifying information security threats at the stage of creating an information system (IS) in the case when information protection measures are not implemented or their sufficiency and effectiveness are not assessed, the assessment of the possibility of realizing a threat, which is characterized by how likely it is. Robotic IS with given structural and functional characteristics and features of functioning, is carried out relative to the level of initial security of IS (Kirichek et al., 2014). The level of initial security is understood to be the security of the IS, due to the structural and functional characteristics set in the design and the conditions of its operation. The level of initial security is determined based on the analysis of design structural and functional characteristics.

During the creation of a robotic IS, the level of its initial security is determined as follows, as described below. Robotic IS has a high level of initial security, if at least 80% of IS characteristics correspond to the "high" level, and the rest - to the average level.IS has an average level of initial security, if the conditions under at least 90% of the characteristics of the IS correspond to a level no lower than "medium", and the rest - to a low level of security.IS has a low level of project security, if the conditions in "high" level and "medium" level are not met.

Methodology for determining information security threats in information systems of the FSTEC (Federal Service for Technical and Export Control) of Russia 2015, applicable, in particular, to mobile robotic complexes. In addition, it is necessary to determine how to assess the impact of certain factors on the structural and functional characteristics of the information system and its operating conditions, such as physical influence or the effect on the communication channels of a robot.

To determine which level of protection a particular characteristic has, it is necessary to determine the reason for assigning a particular characteristic to each level. This can be done in an expert way, but in this study, it was proposed to use the evaluation of factors. A set of factors that affect IS security was developed. These factors were chosen based on what effect an attacker could have on a particular structural-functional characteristic. In determining the level of initial security for each of the characteristics, it was assessed whether the attacker could disrupt the functioning of a particular characteristic according to these factors:

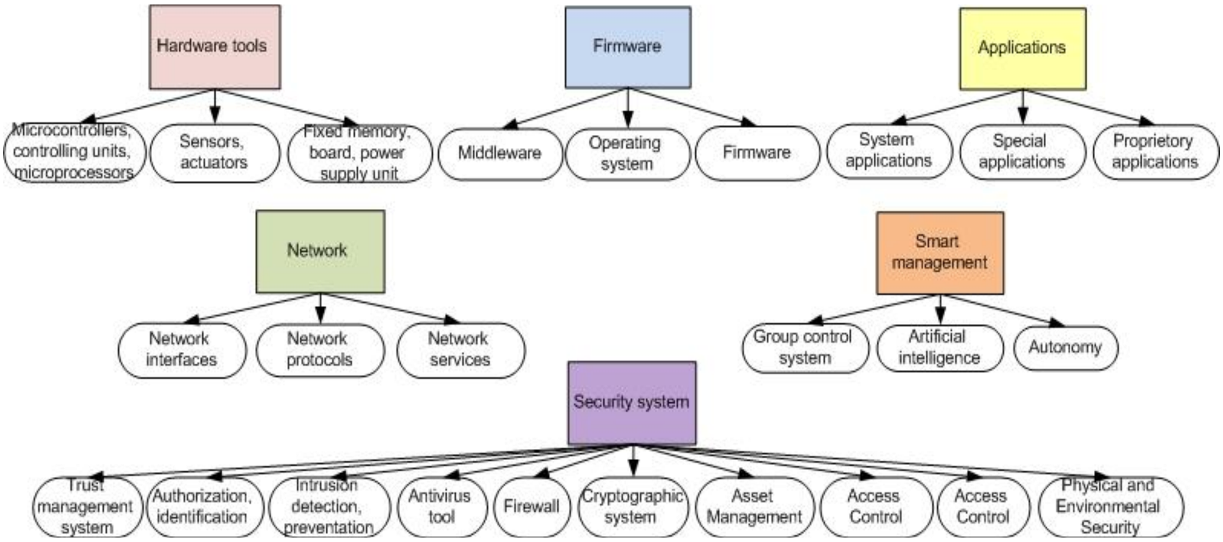

Figure 1. Modular architecture of robotic system.

- Violation of the hardware performance. If a negative impact can be observed both on the part of the intruder and on the part of external factors (environment, man-made disasters, etc.) on the hardware component of the mobile robots IS, then this factor should consider when assessing the possibility of implementing this impact.
- Violation of the software. If a negative impact of the intruder on the IS software of mobile robots may be observed by using special tools and necessary knowledge, then this factor should be taken into account when assessing the possibility of realizing this impact.
- Violation of communication channels. If, as part of the assessment of this factor for the structural and functional characteristics, an adverse impact of the intruder on the communication channels of mobile robots may be observed by using special tools and the necessary knowledge, then this factor should be taken into account when assessing the possibility of realizing this impact.
- Violation of the navigation system. If, as part of the assessment of this factor for the structural-functional characteristics, there is a negative impact of the intruder on the navigation system of mobile robots, through the use of special tools and necessary skills, then this factor should be taken into account when assessing the possibility of realizing this effect.
- Negative impact on the robotic IS operator. If, as part of the assessment of this factor for the structural-functional characteristics, there is a negative impact on the part of the intruder on the operator operating the IS of mobile robots by applying destructive actions against him, then this factor should be taken into account when assessing the possibility of realizing this impact.
- Impact on data transmission process. If, as part of the assessment of this factor for the structural-functional characteristics, there is a negative impact on the data transfer standards from the offender using special tools and the necessary skills, then this factor should be taken into account when assessing the possibility of realizing this impact.

The results of the assessment of the impact of factors on the structural and functional characteristics are presented in table 1.

The result of the analysis of the structural and functional characteristics of the robotic IS, the conditions of its operation, as well as the effects of various factors on each of the security levels of the robotic complexes, is table 2.

As an example, we define the level of initial security for one of the structural and functional characteristic, for stationary and mobile robots.

- Violation of the hardware performance. A stationary robot does not move, and is therefore less susceptible to this factor, due to the inaccessibility of the intruder to the hardware.
- Violation of the software. Stationary robots, like mobile robots use practically the same software, therefore both types of robots are subject to this factor.

- Malfunction of communication channels. Communication channels can be implemented both wirelessly and wired, respectively, the impact on the communication channels stationary robots is minimized.
- Violation of the navigation system. Stationary robots may not use a navigation system, but there are a number of stationary robots (Raven II, Da Vinci), which need to determine the exact location in space of their mechanical parts, respectively, this effect can affect both types of robots.
- Impact on the robotic IS operator. In the case of mobile robots with sufficient autonomy, the role of an individual as an operator in the management of robotic IS is reduced. Therefore, on mobile robots, the influence of this factor is less common.
- Impact on data transmission standards. Transmission standards can be implemented both wirelessly and wired, respectively, the impact on communication channels of stationary robots is minimized.

Table 1. Description of the levels of design security of IS.

The level of design security of the information system	Description
High	The level of the project security of the “High” information system will correspond to a value below 50% of the factors affecting the structural and functional characteristics of the IS of mobile robots and the conditions of its operation.
Medium	The level of design protection of the “Medium” information system will correspond to the range from 50 to 70% of the factors affecting the structural and functional characteristics of the mobile robots IS and its operating conditions.
Low	The level of design protection of the “Low” information system will correspond to the range from 70 to 100% of the factors affecting the structural and functional characteristics of the IS of mobile robots and their operating conditions.

After analyzing the influence of factors on the structural and functional characteristics of robotic IS, we find that mobile robots are subject to a greater number of factors than stationary ones. And using our table, we determine that mobile robots have a “LOW” design security level, as corresponds to the range from 70 to 100% of factors affecting the structural and functional characteristics of mobile robot ISs and its operating conditions, while stationary robots have a design security level “MEDIUM” as it corresponds to the range from 50 to 70% of the factors affecting the structural and functional characteristics of the IC of mobile robots and the conditions of its operation.

5. Conclusion and future work

In conclusion, it should be noted that robotic systems differ significantly in their design and functionality from the process control system, the Internet of things, etc. They are usually equipped with an intelligent control system and decision-making, which imposes additional security requirements. Often robotic systems are mobile, and can be located outside the controlled area. In addition, a large number of threats arise in connection with the use of wireless communication channels. This article attempted to structure information about robotic systems, collected the maximum amount of information from open sources, and carried out its classification. An analysis of potential offenders, their goals and capabilities revealed several important points. Due to the peculiarities of the operation and the conditions for the creation of robotic systems, they are very vulnerable to attacks by the intruder. Robots have limited computing and energy resources, and the use of software and hardware protection tools is not at all possible. Thus, research and development in this area is very relevant and necessary.

Table 2. Indicators characterizing the design security of the information system.

Structural and functional characteristics of the information system, the conditions of its operation	The level of design security of the information system		
	High	Medium	Low
The way of movement:			
- wheel,			+
- tracked,			+
- walking,			+
- air,		+	
- floating.		+	
The application type:			
- industrial,		+	
- household,			+
- social,			+
- medical,		+	
- research,			+
- fighting.		+	
The functioning environment:			
- space,	+		
- air,		+	
- ground,			+
- underground,			+
- marine.		+	
The separation of functions for managing an			
information system:		+	
- without separation,		+	
- the allocation of jobs for administration in a			+
separate domain,		+	
- use of various network addresses,			
- the use of dedicated channels for			
administration.			
The degree of mobility:			
- stationary,		+	
- mobile.			+
The way of management:			
- operator management,			+
- semi-automatic control,			+
- autonomous control,		+	
- group management.		+	
The conditions of operation:			
- deterministic (certain),		+	
- non-deterministic (undefined).			+
The type of navigation:			
- global,	+		
- local,		+	
- personal.			+

In future work, we plan to supplement the risk assessment process with a set of threats that are specific to the robotic system. In previous works, we gave examples and bases of such threats. In future work, we plan to supplement the risk assessment process with a set of threats that are specific to the robotic system [20]. In previous works, we gave examples and bases of such threats. And we also plan to automate the process of determining current threats for given conditions. To solve this problem, we plan to use machine learning methods. Today, many industrial enterprises and critical facilities are automated. In addition, the economic effect of using automated systems has already been proven in practice.

The system under development will be implemented in the form of a set of databases where information about already known and new vulnerabilities and threats specific to robotic systems will be stored. In order for this resource to be used not only by information security professionals, but also by business owners, as well as other full-time employees and engineers with access to robotic systems, a set of services is offered that automate the search for threats and vulnerabilities for a particular system. Today, there are security scanners, security analyzers, but they work for a long time and require the skills to configure and use. Thanks to the methods for analyzing the security of robotic systems based on machine learning technologies to predict the behavior of the system. As well as methods of analysis of robotic systems structural and functional characteristics. It is assumed that the user will only need to install a mobile application or connect to a web service, and answer a few questions; the rest of the work will be done for him. As a result, the user of robotic systems will be able to conclude how much his system is susceptible to attacks by an attacker, as well as take measures to increase the level of security of his system.

6. Acknowledgments

This work was supported by the RFBR grant 18-07-00212 "Development of a method and decision protocol for detecting anomalous node behavior in group control systems for autonomous mobile robots".

7. References

[1] Avery, D. The Evolution of Flight Management Systems // IEEE Software. – 2011. – Vol. 28(1). – P. 11-13. DOI: 10.1109/MS.2011.17.

[2] Amullen, E.M. Model-based resilient control for a multi-agent system against Denial of Service attacks / E.M. Amullen, S. Shetty, L.H. Keel // World Automation Congress (WAC). – 2016. – P. 1-6. DOI: 10.1109/WAC.2016.7582963.

[3] Ani, U.P.D. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective / U.P.D. Ani, H.M. He, A. Tiwari // Journal of Cyber Security Technology. – 2016. – Vol. 1(1). – P. 32-74. DOI: 10.1080/23742917.2016.1252211.

[4] Basan, E. Overview of Information Issues for a Robotic System / E. Basan, A. Basan, A. Grutsynin // Proceedings of 19th Interantional Conference on Communication Technology (IEEE ICCT). – 2019. – P. 1275-1280.

[5] Basan, A. Analysis of ways to secure group control for autonomous mobile robots / A. Basan, E. Basan, O. Makarevich // Proceedings of the 10th International Conference on Security of Information and Networks. – 2017. – P. 134-139.

[6] Basan, A.S. Analysis and implementation of threats for mobile robot management systems / A.S. Basan, E.S. Basan, A.A. Stepenkin // Proceedings of the XIII Russian Scientific-practical Conference Mathematical Methods and Information Technology means. – 2017. – P. 20-23.

[7] Faizal, K. Risk Assessment and Management in Supply Chain / K. Faizal, PL.K. Palaniappan // Global Journal of Researches in Engineering: G Industrial Engineering. – 2014. Vol. 14(2). – P. 19-30.

[8] Hagele, M. Robots conquer the world // IEEE Robotics & Automation Magazine. – 2016. – Vol. 23(1). – P. 118-120. DOI:10.1109/MRA.2015.2512741.

[9] Hoang, T. Supernodes-based solution for terrestrial segment of flying ubiquitous sensor network under intentional electromagnetic interference / T. Hoang, R. Kirichek, A. Paramonov, A. Koucheryavy // Proceedings of the ruSMART: Conference on Internet of Things Smart Spaces and NEW2AN: International Conference on Next Generation Wired/Wireless Networking. – 2016. – P. 351-359.

[10] Holm, H. Virtual Industrial Control System Testbed / H. Holm, M. Karresand, A. Vidström,

E.A. Westring // Swedish Defence Research Agency – Stockholm, Sweden, 2015.

[11] Kirichek, R.V. Flying sensor networks / R.V. Kirichek, A.E. Kucheryavy // Electrosvyaz. – 2014. – Vol. 11. – P. 2-5.

[12] Liang, L. The state of the art of risk assessment and management for information systems / L. Liang, W. Ren, J. Song, H. Hu // Proceedings of 9th International Conference on Information Assurance and Security (IAS). – 2013. – P. 43-56. DOI: 10.1109/ISIAS.2013.6947735.

[13] Mitchell, R. Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications / R. Mitchell, I. Chen // IEEE transactions on systems, man, and cybernetics: systems. – 2014. – Vol. 44(5). – P. 2168-2216.

[14] Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 // National Institute of Standards and Technology. – 2018. – P. 1-48.

[15] Pshikhopov, V. Decentralized control of a group of homogeneous vehicles in obstructed environment / V. Pshikhopov, M. Medvedev, A. Kolesnikov, A. Fedorenko, R. Gurenko // Journal of Control Science and Engineering. – 2016. – Vol. 7192371. – P. 1-9. DOI: 10.1155/2016/7192371.

[16] Pshikhopov, V. Hybrid motion control of a mobile robot in dynamic environments / V. Pshikhopov, A. Ali // Proceedings of the IEEE International Conference on Mechatronics. – 2011. – P. 540-545. DOI: 10.1109/ICMECH.2011.5971345.

[17] Pshikhopov, V.K. Control system design for autonomous underwater vehicle / V.K. Pshikhopov, M.Y. Medvedev, A.R. Gaiduk, B.V. Gurenko // Proceedings of the Robotics Symposium and Competition (LARS/LARC). – 2013. – P. 77-82. DOI: 10.1109/LARS. 2013.61.

[18] Phillips-Wren, G. Ai Tools in Decision Making Support Systems: a Review // International Journal of Artificial Intelligence Tools. – 2012. – Vol. 21(2). – P. 1-13. DOI: 10.1142/S0218213012400052.

[19] Ruiz, J.F. A security engineering process for systems of systems using security patterns / J.F. Ruiz, C. Rudolph, A. Maña, M. Arjona // Proceedings of IEEE International Systems Conference. – 2014. – P. 1-8. DOI: 10.1109/SysCon.2014.6819228.