The Methodology for Assessing Information Security Risks for Robotic Systems

Alexander Basan
Dept. Information security
Southern Federal University,
Taganrog, Russia
tftrtu @mail.ru

Elena Basan
Dept. Information security
Southern Federal University,
Taganrog, Russia
ebasan@sfedu.ru

***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.**

***Keywords*—attack, robotic system, risk, security, threats**

I. 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, assume that a robotic system is a group of robotic devices, joined to decided one or several similar tasks perform their functions through communication channel or autonomous mode. 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. 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 become a problem. 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. 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]. 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. 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 research lies in the fact that the authors proposed a technique for assessing initial security as well as risk assessment and information security threats. 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:

- Researching for 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 the methodology of assessing the level of degrees of criticality, initial security, degree of difficulty of attack realization, negative consequences of the threat.

The remainder of the paper is structured as follows. Section 2 summarizes related work. Section 3 described analyses of the structural and functional characteristics of robotic systems, Section 4 view aassessment of the level of initial security, in Section 5 is described degree of difficulty of attack realization, in Section 6 represents negative consequences of the threat and Section 7 is conclusion and future work.

II. Related work

The closest methodical document, which describes a process of evaluating the initial security level, is a: 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. 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 based on what the degree of security of a 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 consider 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 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. 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 [9]. For each of the proposed security subsystems, there are specified sections of the standards where the procedure for developing each subsystem [10]. This Framework presents many 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]. In 2008, the NIST Special Publication 800-82 standard was introduced. This standard defines key components are [12]:

- 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 [13]. 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 considers 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).

III. 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. 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]. The robots can be carried out by the group control system of robots (GCSR) [16]. The GCSR solves the problems of forming subgroups and the distribution of tasks between them. There are two main ways to organize robots into group: centralized, decentralized [17]. The action of the robots in group or each subgroup is also planning 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. 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 [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.

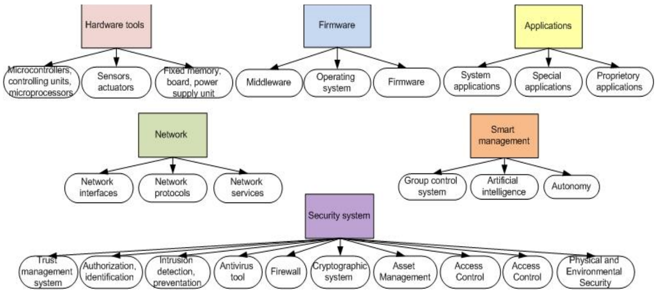

Fig.1. Modular architecture of robotic system.

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 because 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 because 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. We consider each module of the robotic system from the point of view of criticality. We define three degrees of criticality for evaluation:

- High - The implementation of an attack on a particular security attribute will lead to serious consequences such as denial of service, system damage, system destruction, system malfunction, control interception, system destruction, landing system for further research and data collection, as well as entail for itself damage in the field of state security, in the field of defense, political field, economic, man-made consequences.

- Medium - The implementation of an attack on a particular security attribute will lead to minor consequences such as a short-term system shutdown, partial destabilization of the network due to the failure of one or more mobile devices. The introduction of an attacker can lead to disruption of the system’s functioning, as well as to disrupt the process of achieving goals. The application of a destructive effect on the network, and a partial failure of the system, as well as the implementation of the attack, are detrimental in the field of economy, reputation, and political.

- Low - The implementation of an attack on a particular security attribute leads to minimal consequences such as a partial destabilization of the network, short-term interference with data transmission, as well as the implementation of the attack is harmful in the social, reputational and economic fields.

IV. 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. 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 in table 1. 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 assets this it is necessary to determine the reason for assigning a 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. 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: Violation of the hardware performance; Violation of the software; Violation of communication channels; Violation of the navigation system; Negative impact on the robotic IS operator; Impact on data transmission process. The results of the assessment of the impact of factors on the structural and functional characteristics are presented in table 1.

TABLE I. 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.

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. 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.down to the next line. This is the author sequence that will be used in future citations and by indexing services.

TABLE II. 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 application type:			
- industrial,		+	
- household,			+
- social,			+
- medical,		+	
- research,			+
- fighting.		+	
The functioning environment:	+		
- space,		+	
- air,			+
- ground,			+
- underground,		+	
- marine.			
The degree of mobility:			
- stationary,		+	
- mobile.			+
Type of network topology:			+
- star,		+	
- ad-hoc,		+	
- mesh**.**			
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.			+

V. DEGREE OF DIFFICULTY OF ATTACK REALIZATION

In order to determine the degree of difficulty in implementing an attack, it is necessary to understand what goals and opportunities an attacker has. For this, a number of incidents related to the violation of the safety of robotic tools were considered. For example, in 2009 in Iran, the rebels, using a data channel from the UAV to the ground control center, managed to intercept the video data stream from the UAV. At the same time, they used cheap SkyGrabber software, which can be purchased online for as little as $ 25.95.

In 2011, Iran planted on its territory the American secret UAV RQ-170 Sentinel, using such vulnerability as GPS-spoofing. As a result of these actions, the UAV automatically, guided by the global navigation system, began returning home. Since the true signal of the satellites was drowned out by a false one, the RQ-170 took the Iranian airfield, taking it as its “home” one.

In 2013, Sami Kamkar used the Aircrack-ng utility to hack the AR.Drone UAV wireless network, on the base of the Raspberry Pi, a Wi-Fi transmitter and receiver. The attacker explained that the quadcopters on the network could be detected thanks to the peculiarities of their MAC address. Special software monitors the MAC addresses of Wi-Fi networks in the signal coverage area, and then blocks them using its UAV and disconnects from the IOS or Android device from which it was controlled. After that, the hacker can control the direction, speed, and altitude of the flight of the UAV, as well as receive an image from the cameras.

In 2014, in the sky over the Crimea, the Russian military managed to seize control of the American MQ-5B Hunter UAV. Specialists from the University of Washington managed to carry out a successful attack on the medical robot Raven II, which is analogous to the robot Da Vinci. At the first stage of the experiment, data packets addressed to the Raven II robot were intercepted, which made it possible to change their sequence during transmission. The robot manipulator began to produce chaotic movements and ceased to obey the doctor’s management. As a result, the specialists managed to get full control over the actions of the Raven II, and the impact on the robot turned out to be so serious that the robot surgeon did not even react to the command to reboot the system and continued to perform the actions imposed on it.

As from the incidents presented above, it is clear that to cause damage for the robotic system is easy, even using publicly available software. Thus, Figure 2 (a) shows the result of determining which goals an attacker most often pursues. pursues. From this diagram, many incidents in the area of the violation of the security of robotic systems are connected with the conduct of terrorist acts. Such statistics say that first the interests of the state and civilians may be affected.

It is necessary to pay more attention to the security of robotic systems, since so much depends on it. According to the analysis, the attacker does not always need to develop a means to attack himself or use special technical means. Figure 2 (b) presents a diagram showing the results of the analysis of indentations associated with robotic systems to determine the capabilities of the intruder. From the diagram, most of the incidents were carried out using software that is freely available. To assess the complexity of the attack, we introduce two evaluation criteria. Tools for conducting an attack (T):

- The attack is implemented by standard software tools available on the Internet, which do not require additional refinement, and use skills.

- The attack is implemented by standard software available on the Internet, requiring additional refinement, and special skills of use.

- The attack is implemented by software and hardware available in the consumer market for purchase, not requiring additional refinement, and skills of use.

- The attack is implemented by software and hardware available in the consumer market for purchase, while requiring additional refinement, and special skills of use.

- The attack is carried out using specially developed software tools.

- The attack is carried out using specially developed software and hardware.

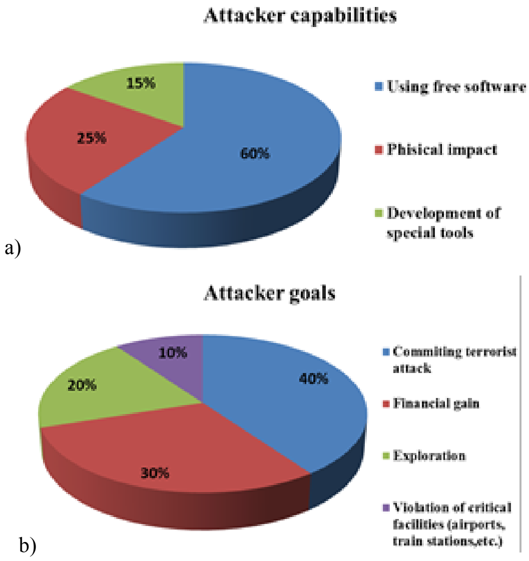

Figure 2. Statistical analysis of the (a) objectives pursued by the intruder (b) the capabilities of the intruder during attacks on robotic systems.

Staged implementation of the attack (S).

- The attack is implemented by remote access.

- The attack is implemented through direct physical access.

- The attack is implemented by directly affecting the structural and functional characteristics.

- The attack is implemented by indirectly affecting the structural and functional characteristics (impact on environmental parameters, etc.)

- The attack is carried out by acting on one structural - functional characteristic through another structural and functional characteristic (multi-stage attack).

VI. Negative consequences of the threat

Next, you need to determine what consequences may occur as a result of a particular attack. The following types of damage are usually highlighted as one of the manifestations of damage. We define the following types of damage and the degree of their influence on the consequences that occur because of the implementation of the attack:

- Economic,
- Social,
- Political,
- Reputational,
- Ecological,
- Technogenic,
- In the field of defense,
- State security.

At the same time, for each type of damper, three degrees are determined: low, medium, high. This characterization should be evaluated by the system owner.

In addition, the damage can be estimated considering the value of the assets that the system owner has. We propose to add to the standard set of resources an entity controlled by an information system, or a product that is the result of work. Adding this entity is important, because an attacker can, for example, act on environmental parameters and introduce a system that measures. And vice versa, the results of an attack can affect the system that measures the environment, an attacker can spoof data or block a network. In this case, the management entity will be violated:

- information;

- software and hardware (including automated workstations, servers, including industrial, machine storage media, telecommunications equipment and communication lines, information display tools, programmable logic controllers, production, technological equipment (executive devices);

- software;

- information security tools;

- supporting systems;

- the entity that is controlled by the information system, or the product that is the result of the information system (temperature, production results, gas supply, etc.).

For each asset, three levels of value are also determined: high, medium, low.

VII. Conclusion and future work

As a result, having determined the values of the previous evaluation criteria, we can determine the degree of danger of the realization of the threat for each potentially dangerous threat (PDT):

$$PDT = (dd*va*dc + T*S)/ds$$

where dd - degree of damage, va- value of assets, dc - degrees of criticality, ds- design security

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, many 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.

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. 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.

ACKNOWLEDGMENT

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".

REFERENCES

[1] D. Avery, “The Evolution of Flight Management Systems,” IEEE Software, vol. 28, no. 1, pp. 11-13, 2011. DOI: 10.1109/MS.2011.17.

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

[3] U. P. D. Ani, H. M. He and A. Tiwari, “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective,” Journal of Cyber Security Technology, vol. 1, no. 1, pp. 32-74, 2016. DOI: 10.1080/23742917.2016.1252211.

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

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

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

[7] K. Faizal and P.L. Palaniappan, “Risk Assessment and Management in Supply Chain,” Global Journal of Researches in Engineering: G Industrial Engineering, vol. 14, no. 2, pp. 19-30, 2014.

[8] M. Hagele, “Robots conquer the world,” IEEE Robotics & Automation Magazine, vol. 23, no. 1, pp. 118-120, 2016. DOI: 10.1109/MRA.2015.2512741.

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

[10] H. Holm, M. Karresand, A. Vidström and E.A. Westring, “Virtual Industrial Control System Testbed,” Swedish Defence Research Agency, Stockholm, Sweden, 2015.

[11] R.V. Kirichek and A.E. Kucheryavy, “Flying sensor networks,” Electrosvyaz, vol. 11, pp. 2-5, 2014.

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

[13] R. Mitchel, I.R. Chen, “Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications,” IEEE transactions on systems, man, and cybernetics: systems, vol. 44, no. 5, pp. 2168-2216, 2014.

[14] “National Institute of Standards and Technology,” Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, pp. 1-48, 2018.

[15] V. Pshikhopov, M. Medvedev, A. Kolesnikov, A. Fedorenko and R. Gurenko, “Decentralized control of a group of homogeneous vehicles in obstructed environment,” Journal of Control Science and Engineering, vol. 2016, no. 7192371, pp. 1-9, 2016. DOI: 10.1155/ 2016/7192371.

[16] V. Pshikhopov and A. Al, “Hybrid motion control of a mobile robot in dynamic environments,” Proceedings of the IEEE International Conference on Mechatronics, Istanbul, Turkey, pp. 540-545, 2011. DOI: 10.1109/ICMECH.2011.5971345.

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

[18] G. Phillips-Wren, “Ai Tools in Decision Making Support Systems: a Review,” International Journal of Artificial Intelligence Tools, vol. 21, no. 2, pp. 1-13, 2012. DOI: 10.1142/S0218213012400052.

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

[20] Y.A. Kropotov, A.Y. Proskuryakov, A.A. Belov, “Method for forecasting changes in time series parameters in digital information management systems,” Computer Optics, vol. 42, no. 6, pp. 1093-1100, 2018. DOI: 10.18287/2412-6179-2018-42-6-1093-1100.