ON TRUST IN AUTONOMOUS SHIPPING SYSTEMS OF CRITICAL INFORMATION INFRASTRUCTURE

DOI: 10.36724/2072-8735-2025-19-6-52-59

Leonid A. Baranov,
Russian University of Transport (MIIT), Moscow, Russia,
baranov.miit@gmail.com

Igor F. Mikhalevich,
Russian University of Transport (MIIT), Moscow, Russia,
mif-orel@mail.ru

Manuscript received 30 April 2025;
Accepted 28 May 2025

Keywords: *automated system in a secure design, autonomous shipping, autonomous shipping system, computer based system, critical information infrastructure, critical information infrastructure object, hardware and software platform, information security, import independence, software and hardware complex, technological independence*

The paper considers the problem of ensuring the security of the critical information infrastructure of the Russian Federation in terms of computer based systems (CBSs) of autonomous shipping. These systems still use foreign hardware and software, information and telecommunication technologies, automated (automatic) control and artificial intelligence technologies. Due to supply chain disruptions, unfixable vulnerabilities and undeclared capabilities, trust in foreign tools and technologies has been undermined. Their use in autonomous shipping systems creates additional risks to the security of the critical information infrastructure and national security in general. This study is aimed at reducing these risks through the use of trusted secure hardware and software platforms, software and hardware complexes, tools and technologies in the creation and operation of CBSs of autonomous shipping on inland waterways. The paper implements a systems approach, uses methods of analysis and synthesis of complex systems, information protection, creation of automated systems in a secure design, ensuring the security of the critical information infrastructure, and the theory of law. The article presents the basic configuration of autonomous shipping systems on inland waterways and reflects the features that affect their safety. The composition of typical objects of critical information infrastructure operating as part of autonomous shipping systems on inland waterways is determined, a model of relations between their safety areas is given. The basic principles of creating a trusted environment for the development and implementation of computer based autonomous shipping systems on inland waterways are outlined. The obtained results allow increasing the safety of critical information infrastructure by reducing the risks associated with dependence on imports. The basic principles of creating a trusted environment for the development and implementation of CBSs of autonomous shipping have common features, which allows them to be extended to other types of transport.

Information about authors:
Leonid A. Baranov, *Russian University of Transport (MIIT), Moscow, Russia. ORCID: 0009-0005-1262-8270*
Igor F. Mikhalevich, *Russian University of Transport (MIIT), Moscow, Russia., ORCID: 0000-0001-8712-1005*

Для цитирования:
Баранов Л.А., Михалевич И.Ф. О доверии к системам автономного судоходства критической информационной инфраструктуры // T-Comm: Телекоммуникации и транспорт. 2025. Том 19. №6. С. 52-59.

For citation:
L.A. Baranov, I.F. Mikhalevich"On trust in autonomous shipping systems of critical information infrastructure," *T-Comm*, 2025, vol. 19, no. 6, pp. 52-59.

Introduction

Computer based systems (information, corporate management and technological control, telecommunications, communications, artificial intelligence) of autonomous shipping are part of the critical information infrastructure of the Russian Federation[1] [1-3]. This imposes increased security requirements for the software, hardware and information processing technologies used in them [4-6]. For a long time, a significant part of the tools and technologies used in autonomous shipping systems (ASSs) were supplied from abroad. Their technical support, elimination of vulnerabilities and undeclared capabilities were carried out in the same way. However, in 2022, there were mass terminations of concluded contracts and refusals to conclude new ones. Previously supplied high-tech computer based systems (CBSs) were left without copyright support and technical support. This created new challenges for the Russian Federation associated with the emergence of new types of information security threats in the field of development, creation and use of CBCs [7-9].

In response to the challenges, emergency measures were taken. In March 2022, the obligation to use only trusted hardware, software and technologies, primarily of domestic origin, at significant critical information infrastructure objects was introduced[2]. In November 2023, rules were approved establishing the procedure for using trusted hardware and software platforms, and software and hardware systems at significant critical information infrastructure objects[3]. In February 2024, the National Strategy for the Development of Artificial Intelligence was clarified and significantly supplemented[4, 5]. In June 2024, the Priority Directions of Scientific and Technological Development of the Russian Federation[6] and the List of the Most Important Science-Intensive Technologies[7] were approved.

Technologies for creating trusted secure software, as well as transport technologies for various areas of application, are among the priorities. Technologies for ensuring the security of receiving, storing, transmitting and processing information, as well as technologies for intelligent transport and telecommunication systems, autonomous vehicles are classified as critical. However, the development and implementation of these technologies is hampered by the insufficient development of domestic solutions in the field of hardware and software platforms software and hardware compresses[5], which fully applies to autonomous shipping systems [2, 10].

1 Autonomous shipping systems

Let us define the term "autonomous shipping system". By an autonomous shipping system we mean a “distributed control system that integrates modern information, telematics, telecommunication technologies, artificial intelligence, and is designed for automated search and adoption for implementation of the most effective scenarios for managing a water transport complex, a shipping company, a vessel or a group of vessels, and water infrastructure objects in order to ensure the specified mobility of the population, maximize the use of waterways, improve the safety and efficiency of shipping, transport processes, and comfort for navigators and users of water transport” [11].

Autonomous shipping systems are characterized by a complex system of relations and connections of objects, as shown in Figure 1. The objects of autonomous shipping systems are automated corporate management and technological control systems [2, 10], located in the offices of state bodies and water transport organizations, private shipping companies, on infrastructure and ships.

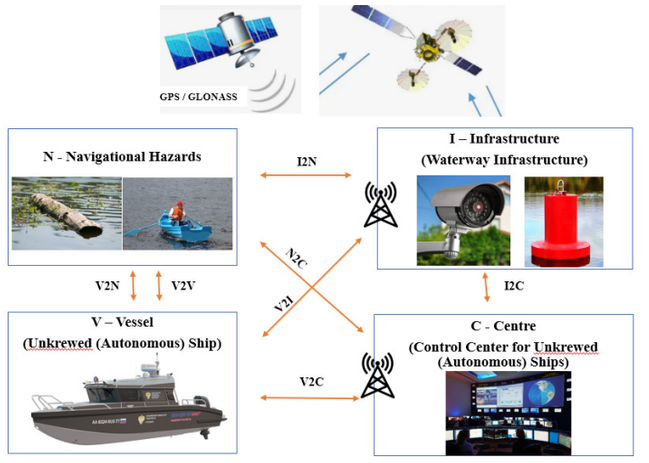

Fig. 1. Basic configuration autonomous shipping systems

The objects may simultaneously include elements of corporate networks, information systems and automated (automatic) control systems. They can process publicly available, confidential and secret information [2, 10]. Reliance on radio channels creates high susceptibility of autonomous shipping systems to the impact of electronic warfare systems, which can disrupt the control of ships [4, 12, 13]. Having a high level of computerization, autonomous shipping systems objects may have a negative impact on other critical information infrastructure objects [1, 14, 15].

Objects of autonomous shipping systems are exposed to high risks of computer attacks (Table 1), which can cause a variety of computer incidents.

[1] Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 No. 187-FZ.
[2] Decree of the President of the Russian Federation of March 30, 2022 No. 166 "On measures to ensure technological independence and security of the critical information infrastructure of the Russian Federation".
[3] Rules for the transition of subjects of the critical information infrastructure of the Russian Federation to the preferential use of trusted software and hardware complexes at significant objects of the critical information infrastructure of the Russian Federation that belong to them (approved by Decree of the Government of the Russian Federation of November 14, 2023 No. 1912).
[4] Decree of the President of the Russian Federation of 15.02.2024 No. 124 "On Amendments to the Decree of the President of the Russian Federation of October 10, 2019 No. 490 "On the Development of Artificial Intelligence in the Russian Federation" and the National Strategy Approved by this Decree.".
[5] National Strategy for the Development of Artificial Intelligence for the Period up to 2030 (approved by the Decree of the President of the Russian Federation of 10.10.2017 No. 490).
[6] Priority areas of scientific and technological development (approved by the Decree of the President of the Russian Federation dated 18.06.2024 No. 529).
[7] List of the most important science-intensive technologies (approved by the Decree of the President of the Russian Federation dated 18.06.2024 No. 529).

Table 1

Statistics of the implementation of computer attacks on objects of the transport complex of the European Union (based on [16])

Types of acts of unlawful interference	Frequency of implementation in year	
	2021	2022
Complex attacks	35%	25%
Ransomware	13%	25%
Data-related attacks	21%	9%
Malware	11%	6%
Denial of service attacks	2%	13%
Phishing	7%	3%
Supply chain attacks	3%	7%
Disruption functioning attacks	4%	4%
Source spoofing	3%	2%
Vulnerability exploitation	4%	1%

In Table 1, complex computer attacks include attacks that have caused not one, but several consequences. These are, for example, attacks with simultaneous substitution of the source and source data of the global navigation satellite system.

In 2023-2024, the overall landscape of computer attacks did not undergo significant changes [17, 18]. In 2024, in the global landscape, the largest number of computer attacks were committed against objects in the public administration (19%), transport (11%) and finance (9%) sectors [17]. The bulk of these attacks were distributed denial of service (DDoS) attacks. Of the total number of computer attacks committed against the transport sector, 21% were DDoS attacks.

However, the most serious consequences are caused by complex computer attacks, examples of which are given in Table 2.

One of the latest public cases is a computer attack on the website of the Taiwanese sea container carrier Wan Hai Lines [9, 10].

As a result of the DDoS attack, the site was down for several days. According to the administration, this act of illegal influence did not have a significant impact on the company's operations, no data leaks were detected and no ransom was paid. However, we note that such events may indicate that attackers are taking the first step in preparing new attacks to penetrate the victim's computer infrastructure with the aim of subsequently stealing or encrypting information, disrupting technological processes, demanding a ransom, etc. [3, 15]. Given that Taiwan's ocean container carrier Wan Hai Lines is the 11th largest in the world, it cannot be ruled out that a complex cyber attack was started on this carrier on April 18, 2025.

The information in Table 2 shows that computer incidents at autonomous shipping systems can cause negative consequences on a national scale. This is due to the interconnectedness of the security areas of autonomous shipping systems[11]. The system of relationships between security areas is three-dimensional.

Figure 2 shows its vertical projection.

Table 2

Computer incidents at water transport objects (based on[8])

Port (company) / country	**The role of the port (company) in the economy**	**Date (period) / method / target of attack**	**Consequences**	**Amount of damage**
Taiwanese Wan Hai Lines / Taiwan	the world's 11th largest containerline	18.04.2025 / DDoS / information theft, advancement through information infrastructure	blocking the site for 2 days	No information available
Croatia	the largest seaport in the country	06.12.2024 / encryption / data theft	theft of accounting documents and personal data	No information available
Nagoya / Japan	10% of Japan's total trade volume, averaging 10,000 units of cargo per day	07.05.2023 / encryption of information of the automated control system by cargo operations / receiving ransom	2 days of downtime at cargo terminals	No information available, national level of danger is recognized
Sydney, Melbourne, Brisbane, Fremantle / Australia	40% of Australia's total cargo volume	11.10.2023 / encryption of ACS information by cargo operations / receiving ransom	3 days of downtime at cargo terminals	No information available, national level of danger is recognized
Durban / South Africa	over 60% of South Africa's cargo turnover, the second largest container port in southern Africa	07.22.2021 / encryption of information of the automated control system of cargo operations / receiving ransom	7 days of downtime at cargo terminals	Ransom over $200,000, incident is considered transnational
Rotterdam / Netherlands	First and second place among European ports in terms of cargo turnover in 2023	2011-2013 / substitution of data on containers with drugs and weapons / smuggling	change of location and delivery time of containers	200,000 euros for countermeasures
Antwerp / Belgium				

[8] Maritime Cyber Attack Database» (MCAD). https://maritimecybersecurity.nl/ (accessed 29.04.2025).

[9] Wan Hai Hit By Cyberattack. The Maritime Executive. April 21, 2025. https://maritime-executive.com/article/wan-hai-hit-by-cyberattack (access date 29.04.2025).

[10] Wan Hai website targeted by hackers. Daily Splash Newsletter. April 21, 2025. https://splash247.com/wan-hai-website-targeted-by-hackers/ (access date 29.04.2025).

[11] List of typical industry-specific critical information infrastructure objects operating in the transport sector (approved by the Ministry of Transport of Russian Federation on 15.05.2023).

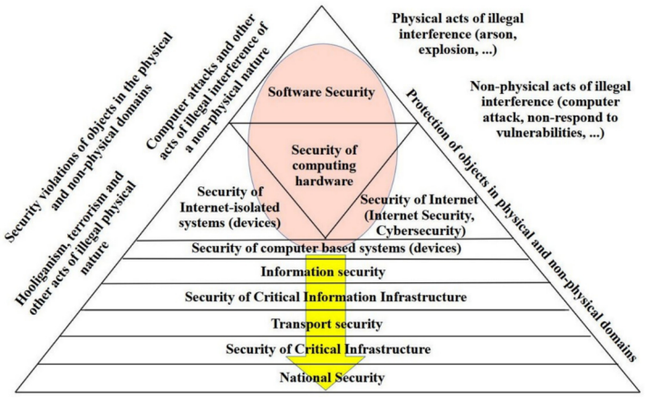

Fig. 2. Communication of security areas of autonomous shipping systems

Each horizontal layer uses its own set of security tools and technologies. The state of each layer located closer to the top of the pyramid can negatively affect the state of the adjacent layer located closer to the base of the pyramid. This corresponds to the "leaky bucket" model. Given this, reliable and complete security measures must be implemented at each layer to achieve security goals. These measures must provide for the neutralization of threats of both physical and non-physical origin. Previous approaches, dividing the spheres of physical and non-physical threats orthogonally, considering them as independent, create significant risks in modern integrated computer based systems of autonomous shipping.

The specified model of relations between the areas of security of autonomous shipping systems integrates Russian approaches to the regulatory framework for protecting computer based systems from acts of illegal interference of a physical (arson, blasting, vandalism, etc.) and non-physical (computer attack, failure to eliminate software and other vulnerabilities, etc.) nature. Its pyramidal form of presentation clearly reflects the complex nature of threats, means and methods of ensuring security, as well as the impact of autonomous shipping systems on the security of critical information infrastructure and national security as a general.

2. Typ al objects of critical information infrastructure of the russian federation in the sphere of sea and river transport

The Ministry of Transport of the Russian Federation has approved the List of typical industry critical information infrastructure objects operating in the transport sector ("List of typical industry-specific critical information infrastructure objects operating in the transport sector", approved by the Ministry of Transport of Russian Federation on 15.05.2023, and "Methodological recommendations for categorization of critical information infrastructure objects operating in the transport sector", approved by the Ministry of Transport of Russian Federation on 24.01.2024) as well as methodological recommendations for categorizing such critical information infrastructure objects (https://mintrans.gov.ru/documents/10/13201?ysclid=lu2cx9gfse525544140 (accessed 24.04.2025). The basic list of typical critical information infrastructure objects in the field of sea and river transport and the critical processes they perform are given in Table 3.

Table 3

Typical objects of critical information infrastructure in the field of sea and river transport (based on[9-11])

No.	Typical objects of CII	Critical processes carried out by a typical object of CII
1	Information systems designed to control the activities of sea passenger transport	Control over the activities of sea and inland water passenger transport. Control over the transportation of passengers in sea and coastal waters, carried out according to a schedule or without a schedule. Control over the activities of excursion, cruise or pleasure boats. Control over the transportation of passengers on ferries and water taxis. Control over the transportation of passengers on sea routes on mixed (river - sea) navigation vessels.
2	Information systems providing monitor over the activities of sea and inland cargo transport	Control over the activities of sea and inland freight transport. Control over the transportation of goods in sea and coastal waters, carried out according to a schedule or not according to a schedule. Control over the activities of foreign-going vessels. Control over the activities of coastal vessels. Control over the activities of river vessels.
3	Information systems designed to support shipping in marine and coastal waters, including pilotage of vessels	Ensuring safe shipping in marine and coastal waters. Providing pilotage for vessels.
4	Automated systems designed to manage shipping support activities for shipping on sea and inland waterway transport	Provision of cartographic information. Determining the location of sea and inland waterway vessels. Route control outside the GSM-communication coverage area.
5	Automated systems for managing loading stations in ports	Collection and processing of information on the state of process parameters. Detection, signaling and recording of emergency situations. Access control to the main of warehouse premises. Archiving the history of parameter changes. Formation and issuance of operational and archived data to personnel. Remote control of shut-off and control valves (gate valves). Remote control of pump units. Control of the process of draining/filling of petroleum products: automatic opening/closing of valves in order to ensure the required route of draining/filling. Diagnostics of the state of software and hardware control tools.
6	Automated systems designed to manage emergency rescue and ship-lifting activities in marine transport	Monitoring distress signals from sea and inland waterway vessels. Automation of emergency rescue operations. Carrying out work to lift sea vessels.
7	Automated systems for the control of icebreaking vessels	Monitoring of icebreakers parameters. Display of information on monitored parameters of icebreakers to operators. Provision of vessel pilotage in ice. Providing route planning in ice Provision of rescue operations in ice. Management of distribution of electric power between consumers. Management of technical means and systems of habitability and life support. Management of technical means and systems of fire fighting. Management of technical means and systems of cargo and ballast systems.
8	Integrated systems providing comprehensive automation of the vessel	Ensuring safe navigation of river and sea vessels. Management of dynamic positioning of river and sea vessels. Management of diesel and electric installations of river and sea vessels. Management of distribution of electric power between consumers. Management of technical means and systems of habitability and life support. Management of technical means and systems of fire fighting. Management of technical means and systems of cargo and ballast systems. Management of technical means and systems of ensuring ecological cleanliness and ecological safety of the vessel.
9	Automated systems designed to control conveyors	Control and management of the technological process of cargo handling.
10	Automated systems designed to control a wagon unloading station	Control and management of the technological process of unloading wagons.
11	Automated systems designed to control ship loading machines	Managing the process of loading onto a ship.
12	Automated systems designed to control signaling, centralization and blocking	Ensuring the safety of train and shunting operations during the process of unloading/loading a vessel.
13	Information systems designed for accounting and planning of loading and unloading activities	Accounting and planning of logistics operations of organizations engaged in loading and unloading activities. Accounting for technical maintenance of handling equipment. Accounting for the availability of cargo in warehouses. Control of the availability of handling equipment.Visualization of cargo flow. Exchange of information with other information and automated systems of participants in the transshipment process.
14	Automated systems providing loading and unloading operations	Automation of loading and unloading operations. Weighing of cargos.

The list of typical critical information infrastructure objects is characterized by its evolving nature. Initially, it included 8 types of objects (lines 1-8 in Table 3). In 2024, 6 more types of objects were included in the list (lines 9-14 in Table 3).

Given the rapid development of autonomous shipping systems and intelligent transport systems, the introduction of the concepts of "autonomous vessel", "fully autonomous vessel" and "semi-autonomous vessel" at the legislative level [12, 13], "unmanned vessel" and "unmanned vessels control center" in state standards [14, 15], the list of typical critical information infrastructure objects will continue to expand.

3. asic principles for creating a trusted environment for the development and implementation of autonomous shipping systems

The above circumstances have a significant impact on the creation and implementation of trusted solutions that are acceptable for use in autonomous shipping systems from the standpoint of ensuring national security, critical information infrastructure security, transport and information security.

In relation to computerized autonomous shipping systems, the requirements of trust are inextricably linked with a set of measures to ensure information security based on domestic solutions [6, 19], taking into account domestic experience [20-22], the results of international research [23-26] and foreign practices [27-29].

To create a trusted environment for the development and implementation of automated shipping systems, it is necessary to comply with the basic principles below. This list contains links to sources that provide definitions for previously formulated terms. It also provides definitions and explanations for additional terms that have been formulated again.

– “security” [6, 11] of hardware and software platforms and complexes, software, equipment and technologies (further – platforms, complexes, tools and technologies) of computer based autonomous shipping systems;

– “protectionability” [6, 11] of platforms, complexes, tools and technologies of computer based autonomous shipping systems;

– controllability of platforms, complexes, tools and technologies of computer based autonomous shipping systems. This principle establishes the mandatory availability of a complete set of documents for platforms, complexes, tools and technologies, including documentation on the compliance of their components and processes for achieving work results individually and jointly as part of computing systems with security requirements. A computing system is understood to mean a SHC or a set of SHCs that form a single infrastructure for solving problems;

– “completeness” [6, 11, 30] of platforms, complexes, tools and technologies of computer based autonomous shipping systems;

– technological sovereignty in the field of platforms, complexes, tools and technologies of computer based autonomous shipping systems. The principle of technological sovereignty assumes the preferential use of domestic solutions in the platforms, complexes, tools and technologies of computer based autonomous shipping systems, as well as their independence from imports, transfer of information, including technological information, outside the Russian Federation. Technological sovereignty is aimed at ensuring the completeness of platforms, complexes, tools and technologies of automated autonomous shipping systems under any external conditions;

– «industrial level» [6, 11, 30] of platforms, complexes, tools and technologies of computer based autonomous shipping systems;

– “universality” [6, 11, 30] of platforms, complexes, tools and technologies of computer based autonomous shipping systems;

– “guarantees for the development and support” [6, 11, 30] of platforms, complexes, tools and technologies of computer based autonomous shipping systems;

– compatibility of platforms, complexes, tools and technologies of computer based autonomous shipping system;

– flexibility of platforms, complexes, tools and technologies of computer based autonomous shipping systems. Flexibility provides the ability to create a variety of computing system architectures based on components of platforms, complexes, tools and technologies of autonomous shipping systems;

– promptability of platforms, complexes, tools and technologies of computer based autonomous shipping systems. Promptability ensures a reduction in the time required to move from scientific or applied research to the creation of computing systems

– continuity (inheritance) of platforms, complexes, tools and technologies of computer based autonomous shipping systems. The principle of continuity (inheritance) is aimed at ensuring a gradual transition to domestic special software through the consistent replacement of special software operating under the control of operating systems from unfriendly countries (inheritance software);

– integrity of the innovation cycle of platforms, complexes, tools and technologies of computer based autonomous shipping systems;

– “support of competition” [6, 11] in the field of platforms, complexes, tools and technologies of computer based autonomous shipping systems.

The principles considered were developed taking into account the experience of developing and implementing national secure hardware and software platforms for critical information infrastructure [6], the provisions of GOST R 56939-2024, the results of foreign research and practices (zero trust [26, 28, 29], multilevel (echeloned) protection [27, 31], etc.).

Conclusion

The conducted research is aimed at reducing the security risks of critical information infrastructure caused by dependence on import of software and hardware platforms and complexes, software, equipment and technologies of autonomous navigation systems and incomplete consideration of risk factors.

The research uses a systems approach using methods of analysis and synthesis of complex systems, information protection, creation of automated systems in a secure design, ensuring the security of critical information infrastructure, theory of law.

---

[12] Federal Law “Code of Inland Water Transport of the Russian Federation" dated March 03, 2001, No. 24-FL.

[13] Federal Law “Code of Merchant Shipping of the Russian Federation” dated April 30, 1999. No. 81-FL,

[14] GOST R 59298-2021. Unmanned inland navigation vessels. Terms and defini-tions.

[15] GOST R 59284-2020. Unmanned vessels of the technical fleet. General requirements.

The presented basic configuration of autonomous shipping systems takes into account the features affecting their security in the physical and non-physical areas of committing acts of illegal interference. Model of interrelations of security areas Russian approaches to regulatory regulation of the security of computer based systems of autonomous shipping on inland waterways from acts of illegal interference of physical and non-physical nature of origin.

The obtained results make it possible to increase the security of critical information infrastructure through the use of trusted secure platforms, complexes, tools and technologies in the creation and operation of computer based systems for various purposes.

Acknowledgments

The work was carried out using budget funding within the framework of the state assignment dated 20.03.2025 No. 103-00001-25-02.

References

[1] A. P. Nyrkov, K. V. Natashova, S. S. Sokolov, O. N. Gubernators et al., "On the issue of categorization of critical information infrastructure objects of seaports," *Information Technology Security*. 2020. Vol. 27, No. 2, pp. 35-46. DOI 10.26583/bit.2020.1.03. (In Russian)

[2] S. Sokolov, N. Glebov, K. Natashova, O. Gubernatorov, "Categorization of objects of critical information infrastructure of water transport," *E3S Web of Conferences : 2018 International Science Conference on Business Technologies for Sustainable Urban Development, SPbWOSCE 2018*, St. Petersburg, December 10-12, 2018. Vol. 110. St. Petersburg: EDP Sciences, 2019. P. 02003. DOI 10.1051/e3sconf/201911002003.

[3] I. F. Mikhalevich, "Conceptual problems of transportation security of intelligent water transportation systems," *Dependability* 2024, no. 2, pp. 72-87. https://doi.org/10.21683/1729-2646-2024-24-2-72-87. (In Russian)

[4] A. P. Nyrkov, S. S. Sokolov, O. M. Alimov et al., "Optimal Identification for Objects in Problems on Recognition by Unmanned Underwater Vehicles," *Automatic Control and Computer Sciences*. 2020. Vol. 54, No. 8, pp. 958-963. DOI 10.3103/S0146411620080234.

[5] A. P. Nyrkov, S. V. Smolentsev, A. A. Butsanets, S. F. Shakhnov et al., "Algorithm for analyzing the automatic identification system data to identify typical scenarios for vessel divergence and testing the systems of autonomous shipping," *T-Comm*. 2024. Vol. 18, No. 3, pp. 50-59. DOI: 10.36724/2072-8735-2024-18-3-50-59.

[6] I. F. Zikhalevich, "Methodological foundations of creation of national protected hardware-software platforms for critical information infrastructures," *T-Comm*, 2018, vol. 12, no.3, pp. 75-81. (In Russian)

[7] A. P. Nyrkov, E. S. Yumasheva, A. V. Kirikov, "Optimization of the process of penetration testing in the automated control system of technological processes using machine learning algorithms," *Bulletin of the Admiral S. O. Makarov State University of Maritime and Inland Shipping*. 2024. Vol. 16, No. 3, pp. 456-466. (In Russian)

[8] I. F. Mikhalevich, A. P. Ryjov, "Assessment of the sustainability of the development of the critical infrastructures on the basis of information security evaluation and monitoring technology," *T-Comm*, 2018, vol. 12, no.5, pp. 71-76. DOI 10.24411/2072-8735-2018-10089.

[9] S. S. Sokolov, O. N. Gubernatorov, T. P. Knysh, "Methods and means of automated detection of a security violator at a transport infrastructure facility (using a seaport as an example)," *Automation and modeling in design and management*. 2023. No. 1 (19), pp. 12-20. DOI 10.30987/2658-6436-2023-1-12-20. (In Russian)

[10] I. F. Mikhalevich, "Problems of Ensuring the Security of Autonomous Shipping on Inland Waterways," Moscow: Goryachaya Liniya – Telecom, 2024. 336 p. (In Russian)

[11] I. F. Mikhalevich, "Problemic Issues of Deploying Cooperative Intelligent Transport Systems during of Digital Transformation," *2021 Systems of Signals Generating and Processing in the Field of on Board Communications*, Conference Proceedings, Moscow, March 16-18, 2021. Moscow, P. 9415999. DOI 10.1109/IEEECONF51389.2021.9415999.

[12] A. Androjna, M. Perkovič, "Impact of Spoofing of Navigation Systems on Maritime Situational Awareness", *Transactions on Maritime Science*. Split, Croatia, 2021, no. 10(2), pp. 361-373. doi: 10.7225/toms.v10.n02.w08.

[13] Y. Jo, O. Choi, J. You, Y. Cha, D. H. Lee, "Cyberattack Models for Ship Equipment based on the MITRE ATT&CK Framework," *Sensors*, 22(5), 1860. (2022, February 26). DOI: 10.3390/s22051860.

[14] A. O. Kalashnikov, I. F. Mikhalevich, "About the single system of protection classes elements of critical information infrastructure by the criteria of importance and information security," *International Journal of Engineering and Technology(UAE)*. 2018. Vol. 7, No. 2, pp. 247-250. DOI 10.14419/ijet.v7i2.23.11952.

[15] I. F. Mikhalevich, "Critical Infrastructure Security: Alignment of Views," *2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019,* Moscow, March 20-21, 2019. Moscow, P. 8706821. DOI 10.1109/SOSG.2019.8706821.

[16] Threat Landscape Transport Sector. ENISA, March 21, 2023. URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (access date 26.04.2025).

[17] ENISA Threat Landscape 2024. Published September 19, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (access date 26.04.2025).

[18] Threat landscape for industrial automation systems. Q2 2024. URL: https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/ (access date 26.04.2025).

[19] D. P. Zegzhda, A.M. Ivashko, "Technology of creating secure information processing systems based on a domestic protected operating system," *Problems of information security. Computer systems*. 1999. No. 2, pp. 59-64. (In Russian)

[20] P. D. Zegzhda, N. V. Gololobov, D. P. Zegzhda, "Set-theoretic model of data poisoning attack techniques in artificial intelligence systems," *Problems of information security. Computer systems*. 2023. No. S2 (55), pp. 120-129. DOI 10.48612/jisp/9agd-pe6p-b82a. (In Russian)

[21] D. P. Zegzhda, A. M. Ivashko, "On the creation of protected information processing systems," *Problems of information security. Computer systems*. 1999. No. 1, pp. 99-107. (In Russian)

[22] A. V. Barabanov, A. S. Markov, V. L. Tsirlov, "On the taxonomy of information security of software supply chains," *Information Technology Security*. 2019. Vol. 26, No. 3, pp. 68-79. DOI: 10.26583/bit.2019.3.06. (In Russian)

[23] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J. -M. Lee, D. -S. Kim, "Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach," *Electronics*, 2024, 13, 276. URL: https://doi.org/10.3390/electronics13020276.

[24] C. I. Nwakanma, L. A. C. Ahakonye, J. N. Njoku, J. C. Odirichukwu, S. A. Okolie, C. Uzondu, C.C. Ndubuisi Nweke, D. -S. Kim, "Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review," *Appl. Sci.* 2023, 13, 1252. doi.org/10.3390/app13031252.

[25] V. Bolbot, A. Sandru, T. Saarniniemi, O. Puolakka, P Kujala, O.A. Valdez Banda, "Small Unmanned Surface Vessels – A Review and Critical Analysis of Relations to Safety and Safety Assurance of Larger Autonomous Ships," *J. Mar. Sci. Eng*. 2023, 11, 2387. URL: doi.org/10.3390/jmse11122387.

[26] F. Raheman, "From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security," *Journal of Computer and Communications*, 2024, no. 12, pp. 252-282. URL: doi: 10.4236/jcc.2024.123016.

[27] M. Fabro, E. Gorski, N. Spiers, J. Diedrich, D. Kuipers, "Recommended practice: improving industrial control system

cybersecurity with defense-in-depth strategies," *DHS Industrial Control Systems Cyber Emergency Response Team*, 2016. URL: https://www.hsdl.org/c/view?docid=797585 (access date 29.04.2025).

[28] Zero Trust Strategy and Roadmap. US Department of Defense Releases Nov. 22, 2022 URL: https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/ (access date 29.04.2025).

[29] Zero Trust. Maturity Model. April 2023. Version 2.0. Cybersecurity and Infrastructure Security Agency. Cybersecurity Division. URL: https://www.cisa.gov/sites/default/files/2023-04/CISA Zero Trust Maturity Model Version 2_508c.pdf (access date 29.04.2025).

[30] A. N. Nazarov, I. F. Mikhalevich, "Methodology development and implementation of protected hardware and software platform based on the existing," *2018 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, March 14-15, 2018. Moscow: Institute of Electrical and Electronics Engineers Inc., 2018. P. 8350623-5. DOI 10.1109/SOSG.2018.8350623.

[31] A. Amro, V. Gkioulos, "Cyber risk management for autonomous passenger ships using threat informed defense-in-depth," *Int. J. Inf. Secur.* No. 22, pp. 249-288. 2023. https://doi.org/10.1007/s10207-022-00638-y.

О ДОВЕРИИ К СИСТЕМАМ АВТОНОМНОГО СУДОХОДСТВА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Баранов Леонид Аврамович, *Российский университет транспорта (МИИТ), Москва, Россия,* ***baranov.miit@gmail.com***

Михалевич Игорь Феодосьевич, *Российский университет транспорта (МИИТ), Москва, Россия,* ***mif-orel@mail.ru***

Аннотация

В работе рассмотрена проблема обеспечения безопасности критической информационной инфраструктуры Российской Федерации (КИИ) в части компьютеризированных систем автономного судоходства. В этих системах по-прежнему используются зарубежные аппаратные и программные средства, информационные и телекоммуникационные технологии, технологии автоматизированного (автоматического) управления и искусственного интеллекта. В связи с нарушениями цепочек поставок, не устраняемыми уязвимостями и недекларированными возможностями доверие к зарубежным средствам и технологиям подорвано. Их использование в системах автономного судоходства создает дополнительные риски безопасности КИИ и национальной безопасности в целом. Настоящее исследование направлено на снижение указанных рисков за счет использования при создании и эксплуатации компьютеризированных систем автономного судоходства на внутренних водных путях доверенных защищенных аппаратно-программных платформ, программно-аппаратных комплексов, средств и технологий. В работе реализован системный подход, использованы методы анализа и синтеза сложных систем, защиты информации, создания автоматизированных систем в защищенном исполнении, обеспечения безопасности критической информационной инфраструктуры, теории права. В статье приведены базовая конфигурация систем автономного судоходства на внутренних водных путях и отражены особенности, влияющие на их безопасность. Определен состав типовых объектов КИИ, функционирующих в составе систем автономного судоходства на внутренних водных путях, приведена модель отношений областей их безопасности. Изложены базовые принципы создания доверенной среды разработки и реализации компьютеризированных систем автономного судоходства на внутренних водных путях. Полученные результаты позволяют повысить безопасность КИИ за счет снижения рисков, связанных с зависимостью от импорта. Базовые принципы создания доверенной среды разработки и реализации компьютеризированных систем автономного судоходства обладают признаками общности, что позволяет распространить их на другие виды транспорта.

Ключевые слова: *автоматизированная система в защищенном исполнении, автономное судоходство, аппаратно-программная платформа, импортонезависимость, информационная безопасность, компьютеризированная система, критическая информационная инфраструктура, объект критической информационной инфраструктуры, система автономного судоходства, программно-аппаратный комплекс, технологическая независимость*

Литература

1. *Ныpков А. П., Наташова К. В., Соколов С. С., Губернаторов О. Н.* и др. К вопросу о категорировании объектов критической информационной инфраструктуры морских портов // Безопасность информационных технологий. 2020. Т. 27, № 2. С. 35-46. DOI 10.26583/bit.2020.1.03.

2. *Sokolov S. S., Glebov N., Natashova K., Gubernatorov O.* Categorization of objects of critical information infrastructure of water transport // E3S Web of Conferences : 2018 International Science Conference on Business Technologies for Sustainable Urban Development, SPbWOSCE 2018, St. Petersburg, 10-12 декабря 2018 года. Vol. 110. St. Petersburg: EDP Sciences, 2019. - P. 02003. - DOI 10.1051/e3sconf/201911002003.

3. *Михалевич И. Ф.* Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем // Надежность. 2024. Т. 24, № 2. С. 72-87. DOI 10.21683/1729-2646-2024-24-2-72-87.

4. Nyrkov *A. P., Sokolov S. S., Alimov O. M. et al.* Optimal Identification for Objects in Problems on Recognition by Unmanned Underwater Vehicles / A. P. Nyrkov // Automatic Control and Computer Sciences. 2020. Vol. 54, No. 8. P. 958-963. DOI 10.3103/S0146411620080234.

5. *Nyrkov A. P., Smolentsev S. V., Butsanets A. A., Shakhnov S. F.* et al. Algorithm for analyzing the automatic identification system data to identify typical scenarios for vessel divergence and testing the systems of autonomous shipping // T-Comm. 2024. Vol. 18, No. 3. P. 50-59. DOI: 10.36724/2072-8735-2024-18-3-50-59.
6. *Михалевич И. Ф.* Методологические основы создания национальных защищенных аппаратно-программных платформ для критических информационных инфраструктур // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12, № 3. С. 75-81. DOI 10.24411/2072-8735-2018-10056.
7. *Ныркov А. П., Юмашева Е. С., Кириков А. В.* Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2024. Т. 16, № 3. С. 456-466.
8. Mikhalevich I. F., Ryjov A. P. Assessment of the sustainability of the development of the critical infrastructures on the basis of information security evaluation and monitoring technology // T-Comm: Телекоммуникации и транспорт. 2018, vol. 12, no.5, pp. 71-76. DOI 10.24411/2072-8735-2018-10089.
9. *Соколов С. С., Губернаторов О. Н., Кныш Т. П.* Методы и средства автоматизированного обнаружения нарушителя безопасности на объекте транспортной инфраструктуры (на примере морского порта) // Автоматизация и моделирование в проектировании и управлении. 2023. № 1(19). С. 12-20. DOI 10.30987/2658-6436-2023-1-12-20.
10. *Михалевич И. Ф.* Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях (монография). М.: Горячая линия – Телеком", 2024. 336 с.
11. *Mikhalevich I. F.* Problemic Issues of Deploying Cooperative Intelligent Transport Systems during of Digital Transformation // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings, Moscow, March 16-18, 2021. Moscow, 2021. P. 9415999. DOI 10.1109/IEEECONF51389.2021.9415999.
12. *Androjna A. and Perkovic M.* Impact of Spoofing of Navigation Systems on Maritime Situational Awareness // Transactions on Maritime Science. Split, Croatia, no. 10(2), 2021, pp. 361-373. doi: 10.7225/toms.v10.n02.w08.
13. *Jo,Y., Choi O., You J., Cha Y., Lee D.H.* Cyberattack Models for Ship Equipment based on the MITRE ATT&CK Framework // Sensors, 22(5), (2022, February 26). 1860. DOI: 10.3390/s22051860.
14. *Kalashnikov A. O., Mikhalevich I. F.* About the single system of protection classes elements of critical information infrastructure by the criteria of importance and information security // International Journal of Engineering and Technology(UAE). 2018. Vol. 7, No. 2, pp. 247-250. DOI 10.14419/ijet.v7i2.23.11952.
15. *Mikhalevich I. F.* Critical Infrastructure Security: Alignment of Views // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019, Moscow, March 20-21, 2019. Moscow, 2019. P. 8706821. DOI 10.1109/SOSG.2019.8706821.
16. Threat Landscape Transport Sector. ENISA, March 21, 2023. URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (дата обращения 26.04.2025).
17. ENISA Threat Landscape 2024. Published September 19, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата обращения 26.04.2025).
18. Threat landscape for industrial automation systems. Q2 2024. URL: https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/ (дата обращения 26.04.2025).
19. *Зегжда Д.П., Ивашко А.М.* Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы // Проблемы информационной безопасности. Компьютерные системы. 1999. № 2. С. 59-64.
20. *Зегжда П.Д., Гололобов Н. В., Зегжда Д. П.* Теоретико-множественная модель техник атак отравления данных в системах искусственного интеллекта // Проблемы информационной безопасности. Компьютерные системы. 2023. № S2(55). С. 120-129. DOI 10.48612/jisp/9agd-pe6p-b82a.
21. *Зегжда Д.П., Ивашко А.М.* К созданию защищенных систем обработки информации // Проблемы информационной безопасности. Компьютерные системы. 1999. № 1. С. 99-107.
22. *Барабанов А.В., Марков А.С. Цирлов В.Л.* О систематике информационной безопасности цепей поставки программного обеспечения // Безопасность информационных технологий. 2019. Т. 26, № 3. С. 68-79. DOI: 10.26583/bit.2019.3.06.
23. *Nkoro E.C., Njoku J.N., Nwakanma C.I., Lee J.-M., Kim D.-S.* Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach // Electronics 2024, 13, 276. URL: https://doi.org/10.3390/electronics13020276.
24. *Nwakanma C.I., Ahakonye L.A.C., Njoku J.N.; Odirichukwu J.C., Okolie S.A. Uzondu C., Ndubuisi Nweke C.C., Kim D.-S.* Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review // Appl. Sci. 2023, 13, 1252. doi.org/10.3390/app13031252.
25. *Bolbot V., Sandru A., Saarniemi T., Puolakka O., Kujala P., Valdez Banda O.A.* Small Unmanned Surface Vessels-A Review and Critical Analysis of Relations to Safety and Safety Assurance of Larger Autonomous Ships // J. Mar. Sci. Eng. 2023, 11, 2387. URL: doi.org/10.3390/jmse11122387.
26. *Raheman F.* From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security // Journal of Computer and Communications, 2024, no. 12, pp. 252-282. URL: doi: 10.4236/jcc.2024.123016
27. *Fabro M., Gorski E., Spiers N., Diedrich J., Kuipers D.* Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies '' DHS Industrial Control Systems Cyber Emergency Response Team, 2016. URL: https://www.hsdl.org/c/view?docid=797585.
28. Zero Trust Strategy and Roadmap. US Department of Defense Releases Nov. 22, 2022 URL: https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/ (дата обращения 29.04.2025).
29. Zero Trust. Maturity Model. April 2023. Version 2.0. Cybersecurity and Infrastructure Security Agency. Cybersecurity Division. URL: https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf/ (дата обращения 29.04.2025).
30. *Nazarov A. N., Mikhalevich I. F.* Methodology development and implementation of protected hardware and software platform based on the existing // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, March 14-15, 2018. Institute of Electrical and Electronics Engineers Inc., 2018. P. 8350623-5. DOI 10.1109/SOSG.2018.8350623.
31. *Amro A., Gkioulos V.* Cyber risk management for autonomous passenger ships using threat informed defense-in-depth. Int. J. Inf. Secur. 22, 249-288 (2023). https://doi.org/10.1007/s10207-022-00638-y.

Информация об авторах:
Баранов Леонид Аврамович, *Российский университет транспорта (МИИТ), д.т.н., профессор, Москва, Россия. ORCID: 0009-0005-1262-8270*
Михалевич Игорь Феодосьевич, *"Российский университет транспорта (МИИТ), д.т.н., с.н.с., Москва, Россия. ORCID: 0000-0001-8712-1005*