Security
of Infocommunication Systems
and Internet of Things

2023 Vol 1, No 1

https://doi.org/10.31861/sisiot2023.1.01008

Received 06 June 2023; revised 19 June 2023; accepted 26 June 2023; published 30 June 2023

Systematization of Cyber Threats in Maritime Transport

Oleksiy Polikarovskykh*, Yurii Daus, Dmytro Larin and Mariia Tkachenko

Department of Technical Cybernetics and Information Technologies, Odessa National Maritime University, Odessa, Ukraine

*Corresponding author (E-mail: polalexey@gmail.com)

ABSTRACT The paper proposes a classification of cyber-attacks at the present stage of maritime transport development. A classification system for ship blocks and port infrastructure has been developed. The vulnerabilities of the global navigation satellite system are analyzed; this system is the most important subcategory of maritime vehicles and may be a target for cyber-attacks. The paper shows that the rapid spread of cybercrime occurs due to the rapid development of new technologies and their integration into ship and port infrastructures. The main elements of the maritime transport infrastructure are considered: port infrastructure and ship infrastructure. IoT and Big Data can be examples of the spread of such systems. The ship's IT infrastructure, ship's electromechanical and electronic systems, communication systems, automatic identification systems, ship information system are considered. In the port infrastructure, port security systems, port equipment systems, port communication systems are analyzed. The main types of cyber-attacks to which the ship and port parts of the industry are exposed are considered. The signs of attacks on the Internet of things systems on ships and in ports are considered. The trend towards greater system integration cannot be reversed for economic reasons. Such integration makes it possible to reduce the size of the team, build autonomous ships, work in the smart ports system, and makes it possible to save various resources (time, human, fuel and organizational). The paper considers the practical directions and challenges facing the industry in terms of improving the security of maritime transport in cyberspace.

KEYWORDS maritime industry; cyber-attack; port.

I. INTRODUCTION

The sea transport accounts for 90% of the volume of international traffic [1]. These days, the progressive digitalization of the economy has become a global trend, which fully relates to maritime and river transport. Ships are increasing and crews are decreasing due to more and more automation of processes. Some onboard systems receive updates during the voyage; teams have access to the Internet. Some specialists say information securities of sea and river transport are paid very little attention [2]. It can be easily checked on sites of domestic companies providing services and producing products and solutions for maritime and river transport. As a rule, in the description of services, products and solutions information security issues are not mentioned. At best, they mention the possibility of access differentiation with passwords and logins or the use of network screens.

Work with navigation systems, such as an automatic identification system (AIS), Global Navigation Satellite System (GNSS) and Radio Detection and Ranging (RADAR), makes it possible to exploit the vulnerabilities of these systems and lowers the overall level of safety of marine infrastructure. In addition, ships and ports are exposed to very complex and unknown system cyberattacks, which are aimed at port information systems and the main additional equipment of ships. connecting the equipment to the Internet, working with computers that do not support the appropriate level of security, And the lack of preparation of teams for new cybernetic challenges increases even more the probability of a successful attack on the maritime transport infrastructure.

Numerous works prove that the low level of employee training and lack of systematic consideration of cyber security issues is the main problem facing the industry; as a result, attackers use standard methods: they send spam by e-mail and messengers, organize a "denial of service" (DoS) to achieve their goals [3]. Using a safety system construction plan based on industry recommendations is a vital task; such a plan should be coordinated with the strategies of international maritime organizations [4]. The method of updating software via USB media, exchanging information in real time with IoT devices - increases the risk of hacking the system using well-known methods from civil infrastructure. Insecure network services, lack of identification and authentication play a special role here.

Our work presents an overview of cyber security systems and a proposed systematization of cyber-attacks on maritime transport. The classification of types of port and ship equipment has been completed. This classification allows you to systematize threats by types of attacks. The classification of vulnerabilities in ports and ships has been carried out. In section 2, the research methodology is selected and a brief review of the literature on cyber security in the maritime industry is carried out. Section 3 systematizes vulnerabilities on ships and ports, and section 4 classifies attack methods on the above systems. Conclusions are made about possible directions for increasing the stability of systems against complex attacks on hardware and software complexes of marine infrastructure.

II. THREATS IN THE MARITIME INDUSTRY

Based on the reported cyber incidents over a period of ten years, the cases of such cyber-attacks have been classified. It was found that the number of cyber-attacks is increasing and there is a lack of a systematic approach to security practices across the sector. A statistical study [5] identified key systems both on the ship and in port that require increased attention from cyber-attacks because of their respective vulnerabilities. It was statistically proven that the number of vulnerabilities in port infrastructure is higher than on ships.

The most frequent attacks were of the following types:

- Ransomware attack;
- Fishing attack;
- Malware attack;
- Petya Ransomware;
- GPS spoofing attack;
- Navigation Systems attack;
- A computer virus inside the control systems. [3]

Maritime infrastructure can be divided into two parts: the ship part and the port part. Fig 1 shows the structure of the system under consideration.

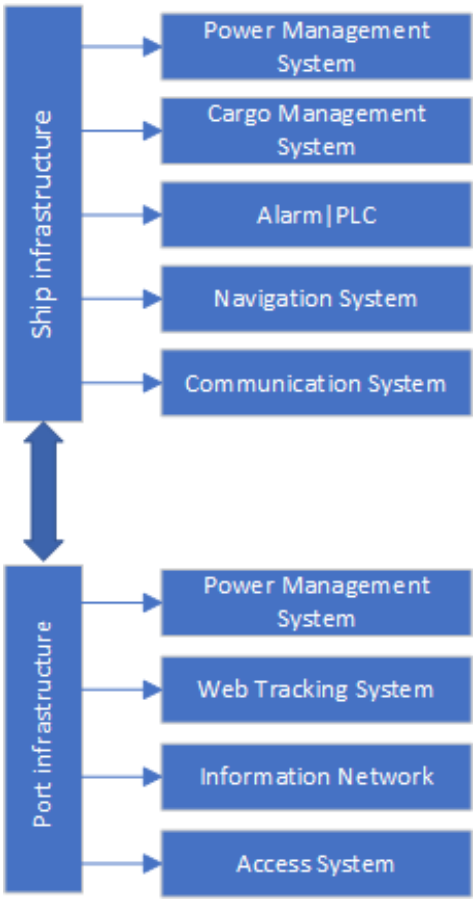

FIG. 1. Maritime transport infrastructure

Based on Fig.1, we will classify the systems of ship and port systems. We will divide the ship infrastructure into two systems: electromechanical and data transmission system. The first includes elements that relate to engines, generators, energy converters, the safety of which depends on a person. The telecommunication system allows the exchange of information between the port and the ship, see Fig.2.

Electromechanical system divides on subsystems:

1. **Power management system**: The main function of this system is to control the generator automatically, which ensures the desired output and power consumption.
2. **Engine**: The most popular engines are diesel engines, which convert thermal energy into mechanical energy, but depending on the size of the ship, the engine type can be different. the engine is controlled by a variety of electronic systems, the safety of which must be high.
3. **Programmable Logic Controllers (PLCs):** These controllers are used to automate work. These PLCs are also integrated into all parts of the control system. They form the core of the control system of the navigation system and serve to prevent accidents. You could say that they control all major ship systems. The number of such controllers on ships is very high.
4. **Water Intrusion Detection System (WIDS):** Every ship is equipped with this system, which is regulated by regulations. If a fixed water level is exceeded, an audible and visual alarm is given. This system must be protected against both electrical and software failures.
5. **Bow thrusters:** Bow thrusters are used at low speed for efficient maneuvering and their damage or malfunctioning due to attack can have dramatic consequences.
6. **Emergency Shutdown System (ESD):** ESD is activated in emergency situations such as fire.
7. **The fuel supply system**: is the system which provides the fuel supply to the injection.
8. **Lubricating oil system:** The lubricating oil system is the most important engine subsystem that ensures the longevity of the machine.
9. **Gyrocompass:** The gyrocompass is an important tool used for navigation, providing indicating the North Pole.
10. **Echo sounder:** The echo sounder measures the depth of the sea. This information is used to pass the ship in narrow places.
11. **Loading and stability computer**: The onboard loading computer ensures that the vessel's stability.
12. **Central cooling water system**: equipment on the ship requires cooling. The cooling system is a sophisticated computerized system.
13. **Stabilizers:** Roll stabilization systems, classified as passive and active, are used to maintaining stability and rewarding motion caused by the sea.
14. **Navigation lights:** Lights are used to report dangerous actions, etc.

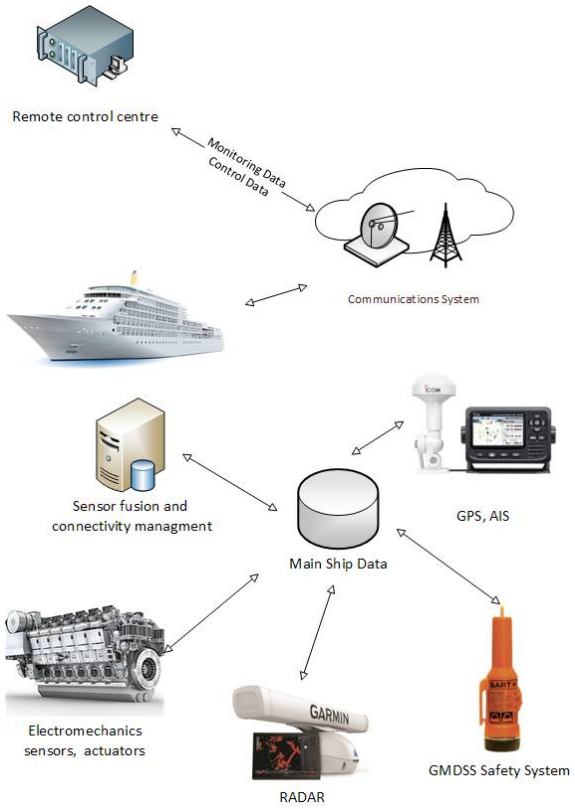

FIG. 2. Diagram of information flows within maritime infrastructure systems

Telecommunications Systems:

1. **Internal communication**: based on VHF (Very High Frequency) communication. It is necessary when requesting assistance and/or transmitting a distress signal. In addition, hand-held VHF communications are also used for purposes such as communicating with local government officials. The Global Maritime Distress and Safety System (GMDSS) use satellite and terrestrial communications to communicate with authorities. The Digital Selective Calling System (DSC) is the most important way to signal a ship's distress and location
2. **Network:** Network systems on ships are designed with high demands on levels of transmission reliability. Shipboard network information systems transmit and process data from all systems and performs data exchange between all equipment
3. **Navigation:** The satellite navigation system is the most vulnerable system on a ship to cyberattack. Although the system relies on highly accurate and expensive satellite systems, the implementation features provide a particularly wide range of possibilities for attackers. Hackers are able to inject invalid information into the signal and thereby throw the ship off course.
4. **RADAR:** Radar is the backbone of the navigation system and plays a key role in steering the ship. Marine radars use two frequency bands, 10 GHz and 3 GHz.
5. **Content delivery networks for passengers**: provide Internet access via Wi-Fi. The provision of Internet access on the ship is difficult, provided mainly by satellite channels.
6. **ECDIS**: ECDIS from Electronic Chart Systems (ECS) is a mandatory real-time navigation tool. It is regulated by the International Maritime Organization (IMO). ECDIS is a real-time system that allows the crew to determine the ship's position. This system generates several charts such as Electronic Chart of Navigation (ENC) and Admiralty Raster Charts (ARCS); updating the charts via the Internet or via USB is a prerequisite for safe navigation.
7. **Automatic Identification System (AIS):** AIS provides static, dynamic and course data. AIS data contains a number of details that can be used by malicious actors. Hackers can use the signals of this system to determine the ship's vulnerabilities, analyze the ship's IT infrastructure architecture (See Fig. 3). The AIS architecture contains: Time Division Multiple Access (TDMA) - vessels use the same frequency and the transmitted frame is divided into time slots, each of which contains location data and vessel data. The duration of such a frame is 60 s, and it, in turn, is divided into 2250-time intervals. Digital Selective Calling (DSC): It allows ships to receive distress calls from others. The system uses Gaussian Minimum Shift Keying (GMSK): this modulation has high spectral efficiency and low inter-channel interference.

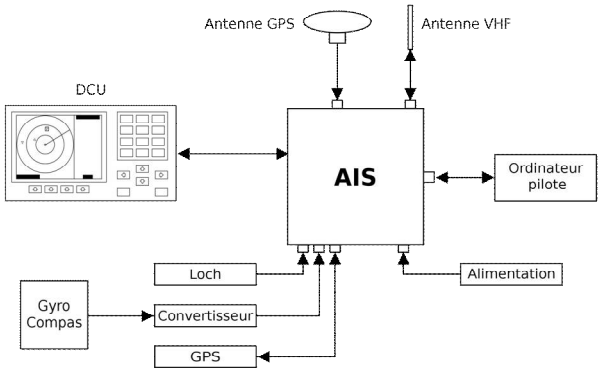

FIG. 3. AIS schema [5]

The Port Infrastructure: The port connects the land part of business structures with sea vessels. Ships are loaded and unloaded in the port; cargo is tracked.

The port provides commercial transportation services, government special services, and multiple security activities.

1. **Closed-Circuit Television (CCTV) Control**: In the port, it is necessary to monitor the entire territory (people, transport, loading procedures, customs operations) in real time. Today, high-resolution IP cameras are used for this, the security of which is a difficult task at the level of the security of the operation of the entire network infrastructure of the port.

2. **X-ray Scanner:** Automated cargo scanning systems require special attention in terms of computer security and resistance to intruder attacks.
3. **The Port Community System** is a platform that allows you to track goods in real time, providing access to up-to-date information at all stages of goods processing, minimizing service time. In the system, users can search through databases. All this information is transmitted only to authorized users, and authorization procedures require the attention of cybersecurity specialists. The Port Community System provides information about cargo, its certificates. The tracking module receives information from the AIS system. The user can see the ship's course in real time and receive video streams, ship's telemetry information streams. Mooring coordination component: organizes ship docking by offering up-to-date information about the process. The user can automatically create a docking plan and access information such as loading/unloading duration through the interface. In addition, the user can get a visual representation of the berth to assist port workers in the successful docking process. Warehouse allocation component: presents a visual representation of the warehouse to optimize the search for specific goods. Interconnection with other modes of transport: provides services related to the connection of a warehouse with a downstream mode of transport. This interface simplifies the management of goods and provides real-time updates on the status of the shipment. Invoicing component: generates and monitors all invoices. The interface includes berthing data and consolidates energy and water consumption information. Analytical component: regularly updates and generates statistical reports on past transactions. It also alerts you to specific violations related to port services.

III. SYSTEMATIZES VULNERABILITIES ON SHIPS AND PORTS

AIS attack: A hacker in the corresponding AIS receiver radio channel with transmits Frame Check Sequence (FCS). The hacker then transmits a message on the appropriate radio channel of the AIS receiver, using the FCS needed for the particular receiver of the ship against which the attack is carried out. For a successful attack, the hacker can change the information about the longitude, latitude and altitude of the object. Or send a false message.

Global Navigation Satellite Systems namely GPS, GLONASS, Galileo, and BeiDou. The vulnerability of GNSS to cyber-attacks arises from the absence of proper authentication and encryption measures, leaving the system exposed to potential breaches. The dissemination of counterfeit position information significantly amplifies the likelihood of collisions, with notable instances occurring in the Black Sea. Figure 4 illustrate the methodology GPS attack by spoofing. A GNSS spoofing attack consists of two sequential steps: first, synchronization with the satellite's signal, followed by the amplification of the transmitted signal's power.

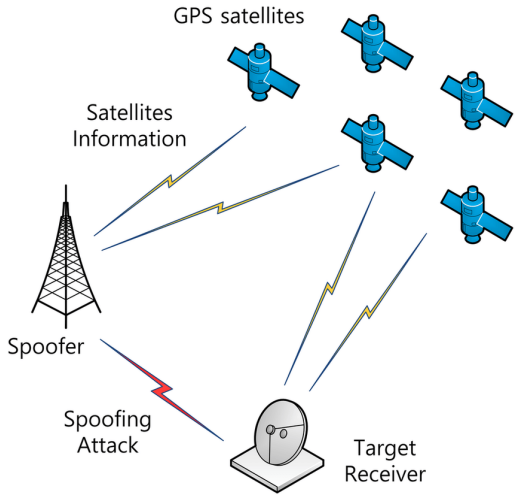

FIG. 4. GPS attack by spoofing

FIG. 5. Maritime threat countermeasure system

Spear-phishing, a commonly employed technique, involves sending emails containing links to insecure content with the intention of unauthorized access. If the attack is successful, the perpetrator installs keyloggers to capture passwords.

Distributed Denial of Service (DDoS) attacks, considered criminal activities, aim to compromise a port's information system by overwhelming the network with excessive traffic, thereby denying access to its websites. Consequently, the functioning of maritime services and the ability to track cargo are jeopardized. The impact of DDoS attacks on cyber-physical maritime systems is evaluated in [6] using simulations. The model incorporates a ship, a controller, and a gate, with the simulated attack specifically targeting the communication between these various components.

Port scanning involves attackers employing techniques to probe the least secure network ports. The objective is to ascertain the status of services, determine the operating system version, and identify the types of databases in use. At advanced levels, hackers utilize IP fragmentation as a means to bypass packet filters. Another approach to port scanning revolves around open port polling techniques, specifically targeting layer 4 of the OSI model (the transport layer), to scan IP addresses.

Social engineering attacks are mostly based on using human curiosity or emotions to carry out malicious actions [7,8,9]. Understanding human behavior is critical to the success of these attacks, and social networking or instant messaging systems serve as a valuable source of information for hackers about network activity in the port. For example, a hacker can gather important information by posing as someone else on platforms such as Facebook or Instagram. Strict adherence to security policies is the only effective method of combating such attacks.

Malware, Ransomware, and Trojans are types of attacks that typically aim to disrupt information systems or servers by hitting interconnected computers. The main vulnerability of IT infrastructure to such threats is the lack of antivirus software. In addition, the lack of antivirus software and the use of external devices have further facilitated the efforts of hackers. Widely known was the Petya 27 virus attack, which specifically targeted the services of shipping company Maersk, hitting its terminals and causing more than $200 million in damage [10,11,12]. In addition, a Maritime threat countermeasure system should be implemented in the industry, see Fig. 5.

IV. CONCLUSION

The increasing complexity and integration of IT systems in the maritime sector, as well as their inclusion on the global Internet, has made the maritime domain an integral battleground for hackers and security professionals. Consequently, these systems are exposed to significant cybersecurity threats. We found that the lack of awareness among ship and port personnel requires enhanced cybersecurity measures in maritime systems.

To address the lack of staff awareness of cybersecurity issues, maritime organizations should engage experts to implement staff awareness programs. The program should contain educational materials suitable for crew members at different levels. In addition, cybersecurity knowledge should be incorporated into training programs for all maritime personnel. To address cybersecurity issues in the maritime industry, it is critical to ensure cybersecurity transfers from other engineering industries to maritime situations. Efforts should be made to transfer knowledge and skills from industries with more experience in dealing with cybersecurity attacks and protecting industrial control systems, which will benefit the maritime transportation industry.

AUTHOR CONTRIBUTIONS

O. P. – conceptualization, methodology; Y. D. – investigation; D. L. – writing-original draft preparation; M. T. – writing-review and editing.

COMPETING INTERESTS

The authors declare no competing interests.

REFERENCES

[1] B. Mednikarov, Y.Tsonev and A. Lazarov Analysis of Cybersecurity Issues in the Maritime Industry. Inf. Secur. 2020, 47, 27–43.

[2] Kapalidis, P. Cybersecurity at Sea. In Global Challenges in Maritime Security; Springer: Berlin/Heidelberg, Germany, 2020; pp. 127–143.

[3] Tam, K.; Moara-Nkwe, K.; Jones, K. The Use of Cyber Ranges in the Maritime Context. 2020.Available online: https://pearl.plymouth.ac.uk/handle/10026.1/16067 (accessed on 11 November 2021).

[4] USCG.mil. 2022. United States Coast Guard Cyber Strategic Outlook. [online] Available at: <https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf> [Accessed30 June 2022].

[5] Automatic identification system. Available online: https://en.wikipedia.org/wiki/Automatic_identification_system (accessed on 11 November 2021)

[6] Bou-Harb, E.; Kaisar, E.I.; Austin, M. On the impact of empirical attack models targeting marine transportation. In Proceedings of the 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Naples, Italy, 26–28 June 2017; pp. 200–205

[7] Siddiqi, Murtaza Ahmed, Wooguil Pak, and Moquddam A. Siddiqi. 2022. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures" Applied Sciences 12, no. 12: 6042. https://doi.org/10.3390/app12126042

[8] Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M. Cybersecurity Challenges in the Maritime Sector. Network. 2022; 2(1):123-138. https://doi.org/10.3390/network2010009

[9] Ferreira, A., & Lenzini, G. (2015, July). An analysis of social engineering principles in effective phishing. In 2015 Workshop on Socio-Technical Aspects in Security and Trust (pp. 9-16). IEEE.

[10] Lagouvardou, S. Maritime Cyber Security: Concepts, Problems and Models; Kongens Lyngby: Copenhagen, Denmark, 2018.

[11] Jensen, T., 2017. Cyber-attack hits shipper Maersk, causes cargo delays - Reuters [WWW Document]. URL https://www.reuters.com/article/us-cyber-attack-maersk/cyber-attack-hits-shipper-maersk-causes-cargo-delaysidUSKBN19J0QB (accessed 4.19.19).

[12] Formby, D.; Durbha, S.; Beyah, R. Out of control: Ransomware for industrial control systems. In Proceedings of the RSA Conference, San Francisco, CA, USA, 14–17 February 2017

Oleksiy Polikarovskykh

In 2015, he received a Doctor of Science degree (D.Sc. in Engineering) at the State University of Intellectual Technologies and Communication (Odessa, Ukraine) in the field of signal synthesis in telecommunication systems. In 2019 Full Professor of the Department of Telecommunications Technologies, Khmelnitsky National University (Khmelnitsky, Ukraine). Currently, Full Professor of the Department of Technical Cybernetics and Information Technologies, Odessa National Maritime University . Research includes issues related to the development of devices for signal synthesis, the theory of cybersecurity and Software Defined Radio.

Yurii Daus

In 1991 he received the degree Ph. D. in the field of mathematical modeling energy and mass exchange. Since 2023, associate professor of the department "Technical cybernetics and information technologies named after Prof. R.V. Mekta" of Odessa National Maritime University. I hold the position of assistant rector for information activities and cyber security. Research includes issues of cyber security and information protection, neural networks, mathematical modeling.

Dmytro Larin

In 2005 he received the degree of PhD in 2005 at the Odesa National Academy of Telecommunication named after A.S. Popov. I hold the position of associate professor of the department "Technical Cybernetics and Information Technologies named after prof. R.V. Merkt" of Odesa National Maritime University. Research includes issues of robotics, the Internet of Things, and information security.

Mariia Tkachenko

In 2012 she graduated from the Odesa National Maritime University with a major in “Information control systems and technologies” and receive the qualification of “system engineer”. In 2017 she received a degree Candidate of Physical and Mathematical Sciences at the Odesa I.I. Mechnikov National University (Odesa, Ukraine) in field elaborating an expert software package for statistically optimal determination of the parameters of binary systems. Currently Lecturer of the Department of Technical Cybernetics and Information Technologies named after Prof. R.V. Merkt, Odessa National Maritime University (Odessa, Ukraine).

Систематизація кіберзагроз на морському транспорті

Олексій Полікаровських [1,*], Юрій Даус[1], Дмитро Ларін[1] та Марія Ткаченко[1]

[1] Кафедра технічної кібернетики та інформаційних технологій, Одеський національний морський університет, Одеса, Україна

*Автор-кореспондент (Електронна адреса: polalexey@gmail.com)

АНОТАЦІЯ У роботі запропоновано класифікацію кібератак на сучасному етапі розвитку морського транспорту. Розроблено систему класифікації суднових блоків та портової інфраструктури. Проаналізовано вразливість глобальної навігаційної супутникової системи (ГНСС), ця система є найважливішою підкатегорією морських транспортних засобів і може бути мішенню для кібернетичних атак. У роботі показано, що швидке поширення кіберзлочинів виникає у зв'язку зі швидким розвитком нових технологій та їх інтеграції до суднової та портової інфраструктури. Розглянуто основні елементи інфраструктури морського транспорту: портова інфраструктура та судова інфраструктура. Розглянуто IT інфраструктуру судна, електромеханічні та електронні системи судна, комунікаційні системи, системи автоматичної ідентифікації, корабельна інформаційна система. Розглянуто системи безпечного мореплавства, систему AIS, ECDIS системи супутникової навігації. У портовій інфраструктурі проаналізовано системи портової безпеки, системи портового обладнання, портові комунікаційні системи. Розглянуто основні види кібератак яким піддаються судова та портова частина галузі морських перевезень. До найнебезпечніших можуть бути віднесені: атаки соціальної інженерії, сканування портів, розподілені атаки на відмову в обслуговуванні, складні вірусні атаки. Особливо небезпечними є атаки на систему AIS та атаки на системи глобального супутникового позиціонування. Розглянуто ознаки атак на системи інтернету речей на кораблях та портах. Запропоновано систематизований підхід до роботи з кібернетичними ризиками. Встановлено, що тенденція до підвищення інтеграції систем не може бути змінена з економічних причин. Така інтеграція дає змогу зменшувати розмір команди, будувати автономні судна, працювати в системі розумних портів, дає можливість економити різні ресурси (часові, людські, паливні та організаційні). У роботі розглянуто практичні напрями та завдання, що стоять перед галуззю у плані підвищення безпеки морського транспорту в кіберпросторі.

КЛЮЧОВІ СЛОВА морська промисловість; кібератака; порт.