Classification of Cyber Risks for Sea Vessel's Voyage Cycle

Kateryna Shumilova[1], Dmytro Shumilov[2], Anatoly Maltsev[1]

Modern digital transformation in the shipping industry Shipping 4.0 is accompanied by increased automation and autonomy of the ship. This means strengthening the digitization of the ship's navigation systems (cyber systems). Therefore, the safe operation and navigation of modern ships depends on the adequate operation of cyber-physical systems, which are created on the basis of information and operational technologies. Such interconnections of ship information systems inevitably increase the vulnerability of the ship's digital navigation infrastructure to cyber-attacks. The article examines methods of controlling cyber risks of various origins, which determine the priority of flows, their internal interconnection and relations with the sources of messages that form them. The formalization of the qualitative and quantitative properties of information flows of the voyage cycle using matrix and graph-analytical modeling methods has been carried out. A decomposition of information was built and a cluster of information security of ship maneuvering control was defined, with its access closed for cyber-attacks. In the event of cyber-attacks, it is very important for the navigator to determine the moment of it's appearance and the state of navigational devices of the bridge. Usually, the working state of the device is determined by the presence of electric current in it. However, only the presence of current in the device during cyber-attacks is not enough to assess its working condition. Inspection and verification of 11 navigation devices on the bridge takes a lot of time, which the navigator does not have in the event of a cyber-attack. Therefore, we propose to introduce an additional function of controlling the working status of each navigational device, and to transmit the results of all devices to a separate navigation cluster Mk of the navigation bridge via shielded cable lines of the vessel without other methods. This will make it possible to gather information about all the devices in one place on the bridge, protect it from cyberattacks, and quickly determine the operating status of all the navigation devices on the bridge. Descriptive modeling of the meaningful categories of the information space of maritime routes during cyberattacks was performed. The proposed classification of cyber risks has a logical structure based on the grouping of message flows, using the cluster connection coefficient between them. This makes it possible to assess the criticality of the impact of cyber-attacks on the ship and to choose ways to reduce their impact on the maneuvering of the ship in the voyage cycle.

KEY WORDS

~ Cybersecurity of maneuvering
~ Cyber-attacks
~ Cyber-risks
~ Shipping risks
~ Safety of shipping
~ Vulnerabilities

[1] National University "Odessa Maritime Academy", Odesa, Ukraine
[2] Marlow Navigation Ukraine, Odesa, Ukraine
e-mail: yeshum@ukr.net
doi: 10.7225/toms.v13.n01.w20
Received: 17 Aug 2023 / Revised: 1 Mar 2024 / Accepted: 14 Mar 2024 / Published: 15 Mar 2024

1. INTRODUCTION

Information support of shipping is closely related with the constant development of technologies of automated ship navigational systems. In the conditions of restrictions associated with shipping processes in the open sea or complicated sailing conditions, such systems cannot be updated in a timely manner and are, therefore, at a risk of a cyber-attack. Analysis of access points of external information to the equipment of the navigational bridge of modern ships, such as Internet connection, use of satellite and radio communication systems, Automatic Identification System (AIS), radar, Electronic Chart Display and Information System (ECDIS) shows that cyber criminals can carry out cyber-attacks even in the open sea.

International maritime administrations have begun inspections of ships entering their ports from 1 January 2021 for compliance with the International Maritime Organization's cyber security recommendations, as required by Resolution MSC.428 (98) (National vulnerability database, 2024). Therefore, when planning the voyage cycle in the existing ship maneuvering control systems, it is necessary to organize the record of cyber risks.

The research examines methods of countermeasure to cyberattacks, based on the use of software of all maritime structures, as well as the need to classify cyber risks in navigation. The monitoring of the position of the vessel, which is not affected by cyberattacks, is shown and recommendations are provided for solving maritime cyber security issues at the international level. The structure of the article includes: 1) new methods of cyberattacks; 2) the need to analyze the risks of cyberattacks on the ship's information and navigation systems; 3) threat modeling and analysis of information processing technology using the STRIDE (threat classification) and DREAD (risk assessment) methodologies; 4) meaningful categories of distribution of information on shipping organization; 5) descriptive modeling, matrix and graph analytic methods of researching of information flows of the ship's voyage cycle; 6) clustering of information flows; 7) classification of navigational cyber risks; 8) assessment of the accuracy of the ship's position in case of cyber attacks; 9) main aspects of the vulnerability of navigational equipment; 9) recommendations on the establishment of training programs on cyber security and international cooperation.

1.1. Problem of ensuring reliable protection against cyberattacks of the digital navigation infrastructure of shipping

The problem of the emergence of cyber risks for marine systems lies in the spread of 5G networks and in the obsolescence or insecurity of shipboard information technologies. This leaves shipboard devices vulnerable to cyber-attacks using information that keeps waterways operational. The lack of reliable protection of shipboard information systems allowed hackers to implement cyberattacks, which led to significant financial losses (IMO / Maritime cyber risk, 2023). For this reason, the issue of reliable protection of shipping information support and classification of cyber risks requires the development of procedures for preparing ship navigation systems to neutralize cyber-attacks when they occur.

The impact of cyberattacks is specially evident during the voyage cycle of a sea vessel (Shumilova, K., 2022). Relevant research using STRIDE (threat classification) and DREAD (risk assessment) methodologies allows to assess the following factors: potential damage, reproducibility, susceptibility to hacking, the circle of users who will be harmed, the probability of detecting a cyber-attack, the replacement of access objects (network), data modification (transmitted and processed), disclaimer of authorship of messages, announcements, denial of service, privilege escalation. This makes it possible to model threats and analyze information processing technologies in information navigation systems and to quantitatively assess the likelihood of the appearance of cyber risks for ship systems (Kavallieratos, Katsikas, 2020).

STRIDE is a model of threats, used to help to identify and find threats to the system. It is used in conjunction with a model of the objective system that can be constructed in parallel. This includes a full breakdown of processes, data stores, data flows, and trust boundaries. The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the profile of the potential attacker, the most probable attack vectors, and the assets most desirable to the attacker. Threat modeling answers questions such as: *"Where am I most vulnerable to attack?*", "*What threats are most relevant?*", and "*What do I need to do to protect myself from these threats?*".

DREAD (risk assessment model) is part of the computer security threat risk assessment system. The categories are: “Damage – how bad would an attack be?”, “Reproducibility – how easy is it to reproduce the attack?”, “Exploitability – how much work is it to launch the attack?”, “Affected users – how many people will be impacted?” “Discoverability – how easy is it to discover the threat?”.

Therefore, to reduce the probability of the occurrence of such risks, it is necessary to apply a systematic approach using a set of criteria that take them into account. This will enable the selection of cyber security level controls provided in the Industrial Control Systems (ICS) Security Guide and the development of a security architecture for ship cyber resilience (Vujović *et al*., 2020).

Digitization, integration, automation of ships and network systems create the need for new survey of cyber risks for shipping security.

Recent studies (Guide to Industrial Control Systems (ICS) Security, 2015) of the causes of cyber incidents point to the complexity of the relationship between people and cargo processing technologies in ports. Incorrect or unauthorized actions of the crew on board can be a threat to the cyber security of the ship. However, the navigator is at the same time a critical element for strengthening the cyber security management system. Therefore, the behavior of the navigation bridge team on board ship is very important when making an adequate decision to prevent and control cyber risks at sea. The analysis of the factors influencing the perception of cyber risk by the navigation bridge team during offshore operations indicates that perceiving of cyber risks by the navigators can be influenced by the feeling of distance to cyber risks, the limitation of the working environment, which is associated with the implementation of digital navigation systems, and trust in the reliability of their operation.

With the maritime transport system accounting for more than 80% of the global traffic, port stakeholders must develop security plans to respond to all modern cyber risks and potential cyber-attacks. Assessment of the interaction between port information technologies (IT) and cargo handling operational technology (OT) systems indicates the need to consider the economic consequences of cyberattacks that affect the operation of sea ports (Gunes *et al*., 2021).

A cyber security forum in July 2020 reported a 900% increase in the number of cyber-attacks on operational technology systems in the maritime industry (Weaver *et al*., 2022). In the report on the readiness of Acronis (Acronis Cyber Readiness Report) to work in the conditions of cyber-attacks, based on the results of a survey of specialists from 3,400 multinational companies, it was reported that due to the COVID-19 pandemic, 92% of the surveyed enterprises work remotely. It is obvious that the actions of hackers are aimed at remote workers (Maritime cyber-attacks up by 900% in three years, 2020). In the last three months of 2020, 39% of companies experienced attacks on Zoom, Cisco Webex, and Microsoft Teams video conferencing applications (Acronis, 2020; Schroedinger’s Pet(ya), 2017).

Ransomware attacks have increased significantly during the COVID-19 pandemic, 31% of companies reported daily cyberattacks, but 50% reported them at least once a week. According to the estimates of Lloyd's of London, the damage from cyberattacks in the maritime industry was estimated at 200 billion dollars.

The urgency of developing measures to reduce the impact of cyber risks on the information systems of ships is related to the recent cyber-attacks that affected shipping ports. Therefore, it is necessary to understand what risks in the processes need to be assessed through the automation and digitization of ship and port information systems.

2. METHODOLOGY

A new method of assessing cyber security risks for ship systems can be built on the use of identifying cyber-attack scenarios and implementing risk assessment (Informatsiina, komunikatsiina ta kiber-vrazlyvist krainy, 2019; Vilskiy, G. B., 2014). However, it was developed to assess cyber risks and improve the design of navigation and propulsion systems of autonomous inland waterway vessels. Such a method considers only a few scenarios and does not take into account the existing types of cyber-attacks and their impact on other types of vessels. It also provides for autonomous ship modernization, which will lead to increased funding to ensure the reliable operation of ship systems. The results of the operation of such vessels show that several critical scenarios may occur on the autonomous vessel under investigation, due to known vulnerabilities. They can be sufficiently controlled by making appropriate modifications to the system design.

Cybersecurity threats continue to grow due to the emergence of increasingly sophisticated cyber-attacks (Bolbot *et al*., 2020; Egloff, 2022; Shumilova, K., 2022). To ensure the safe operation of a ship's maneuvering system, it is necessary to ensure that it operates in accordance with recognized international standards and guidelines, such as ISO (International Organization for Standardization) 27000 series, IEC (International Electrotechnical Commission) 62443, NIST (National Institute of Standards and Technology) or guidelines from IADC (International Association of Drilling Contractors) cyber security (National vulnerability database / Information Technology Laboratory / NIST, 2021). Real-world examples of the results of cyber security and network performance audits carried out by DNV GL Marine Cybernetics Advisory on various types of vessels have shown inadequate cyber security mechanisms, software installation errors and inconsistencies between software documentation and installation, vulnerabilities in controllers and insufficient network bandwidth (Lee and Wogan, 2018; Sea Traffic Management: Efficiency and Cybersecurity, 2022; Csorba *et al*., 2017).

Therefore, the systematization of the main shortcomings of the maritime cargo transportation control system, which affect the operation of information ship systems, will allow to perform an analysis of the navigation system architecture of the navigation bridge (Hemminghaus *et al*., 2021; Caprolu *et al*., 2020). This will determine how they can be used by cybercriminals to disrupt maneuvering control systems. Therefore, all ships should be subject to risk analysis of the probability of cyberattacks.

After the first analysis of the probability of a cyber-attack and deficiencies in the crew's training to prevent cyber risks, it is necessary to update the ship's security plan, ensure the appropriate training of the bridge crew on methods of responding to cyber-attacks and perform timely verification of their implementation through periodic audits. New methods (Akpan *et al.*, 2020; Kardakova *et al*., 2020) of cyber-attacks (Table 1, 2) may include the following actions:

- introduction of ransomware/software to allow the vessel to resume operation;
- digital piracy by blocking access to navigational information on the ship;
- espionage to obtain confidential information that can be used by competitors;
- defamation/lawsuit due to non-compliance with the ISPS Code, delay of the vessel, causing interruptions;
- terrorism causing ship collisions, endangering the operation of ports and other vessels.

Types of cyberattacks	Actions of cybercriminals	Consequences
DDOS-attacks of a new type – 2020	Hackers gaining access to devices (Internet of Things, IoT*) by cracking standard passwords	A cyber threat to maritime information systems worldwide. Short-term (about 30 minutes) disconnection of 15% of the entire global Internet and a number of trunk providers. Increased risk of cyber attacks due to a growing demand for Citrix ADC (Application Delivery Controller) to 2023.
Classic hardware attacks ECDIS, VSAT, INMARSAT	Using even a narrow bandwidth of the channel and a short communication session (transmission of telemetric information about the status of equipment, cargo and route navigation) to attack	After gaining control over the communication equipment and access to the local computing network on-board the bridge – conducting an attack on almost any equipment of the ship, any navigation or navigation system. When charging the mobile phone of one of the crew members through the USB port - virus infection and failure of the ECDIS system
Bruteforce, Petya, WannaCry, Bad Rabbit – *brute force* method - virus programs	The use of open data ports, factory access settings (service bookmarks) and even the classic *Bruteforce* method (an attempt *to guess* a password on a computer when an attacker has obtained its encrypted value, which allows a hacker to use powerful computers to test a large number of passwords) Introduction of virus programs into key systems.	Data loss for shipping companies in the back-office business (financial data, information about the crew and confidential materials of counterparties)
SQL Injection – introduction of dangerous code	Hacking sites and programs that work with databases. Implementation of *fileless* malicious code (2020). Such code can bypass antiviruses, as it is executed in RAM.	Implementation of *fileless* code – distribution of dangerous software, theft of information, placement of unauthorized advertising or prohibited information, fraud, penetration into the company's internal network.
Hacking web applications: **Cross-Site Scripting, XSS** – cross-site execution of scripts; **Cross-Site Request Forgery** – cross-site request forgery; **URL Redirector Abuse** – an open redirect	Hiding the IP address of the source of requests, User Agent data and other identifiers by proxying (through an intermediary computer) traffic through third-party servers.	Obtaining access to the *administrative panel* of the communication modem and obtaining the right to execute commands and download data. Impossibility of determining the real location of the attacker, because he uses other proxy servers for identification, which may be located in different countries.

Downloading an exploit is exploiting a vulnerability.	Fast download of an exploit (program code that exploits a vulnerability to carry out an attack), no more than 10 Kb of data, through a narrow communication channel and a short session	Hacking the navigation system. Access to critical data. Introduction of dangerous software. Information system failure.
Ryuk – introducing a ransomware virus	Encrypting captured files with the Ryuk virus and then demanding ransom from the victim.	Loss of important information during decryption as it cuts off the last byte, which in some cases carries critical information, the deletion of which is detrimental to the entire file as a whole.
CWE-20 – malicious request	Sending a special malicious request to create an inadequate system response to it and provide access to data.	Hacking of the ship management system. Obtaining elevated privileges or access to critical data.
Path Traversal – password selection, going beyond the directory	Obtaining data for authorization through password enumeration. Receiving personal data in 44% of the systems in which they are processed. Ability to get full control over the application. Access to important information on the server.	A cybercriminal can view the contents of those folders on the server that should not be accessible to an ordinary user, even in case of authorization on the site. Read access to the file (/etc/passwd) that stores information about Linux users.
Spoofing attack – attacks in the coastal zone on GNSS and AIS navigation equipment	Spoofing attack – substitution, imitation of GPS data received from satellites of navigation positioning systems (hacker/program masquerading as someone else, falsifying data, and gaining an illegal advantage). The use of special equipment for the attack – a signal transmitter, which can be placed in the coastal zone or on a floating object (radio buoy), depending on the power of the transmitter and the assigned tasks.	This equipment introduces distortions in the signals of GNSS systems (e.g., that a ship that is at sea is moving on land). Jamming or jamming systems, causing vessels to return to port due to problems with their navigation systems. Luring a vessel off course. Hacking the ship control system to determine the presence of armed guards on them. Hacking the container terminal management system to control the movement of containers with hidden drugs to avoid detection. Disruptions in cargo deliveries. Financial losses of logistics companies, insurance costs. Port failures. Human victims
Attacks on the pilot's electronic device	Unauthorized influence on the pilot's electronic device and, through it, on shipping processes in general. Activation of *sleeping* and tacitly integrated into the equipment functions, elements and devices.	Various distortions at numerous stages of digital code conversion in untested and uncertified pilot equipment.
Attacks on AIS equipment	Data compromise in the VHF** range. Placing false VHF transmitters transmitting data ranging from false weather conditions to distress signals.	Misleading the ship's crew and forcing them to change the route, which may also have consequences when entering the port's water area and the correctness of the captain's actions.
Attacks on the operating system – exploiting a vulnerability in the Citrix ADC software	Exploitation by hackers of vulnerability CVE-2019-19781 in Citrix ADC (Citrix Application Delivery Controller)	Penetration in 1 minute into the company's internal network and the ability to develop attacks on the private

	software. Execution by hackers of arbitrary operating system commands without authorization.	segment of the network. When using Path Traversal (password traversal) in Citrix ADC software, a hacker can access static files that are not accessible without authorization (Black-Box***-analysis by Positive Technologies)
Rootkit – dangerous programs on the device	Intercept and change the standard processes of the operating system. An attempt to avoid the detection of a cyber attack and the removal of the program.	Rootkits can remain in place for years if not detected. Any information that a device reports about itself cannot be trusted. It is necessary to reinstall the operating system and software and restore data from a backup copy

Table 1. Cyber-attacks on maritime information systems (Source: Shumilova, K. 2024)

*Internet of Things, IoT – a global network of physical devices connected to the Internet. VHF
**-range –- ultra-short waves.
***Black-Box analysis – software testing without access to the internal structure of system components.

Navigation systems	Vulnerabilities	Consequences of cyber attacks
Automatic Identification System (AIS)	Signal interference Spreading false information Malicious software Forgery of the device The signal has no encryption. Signal muting	Capture of the vessel Data destruction Theft of valuable data
Electronic Display Information System (ECDIS)	Outdated versions of operating systems Unsafe / unregistered update media	Loss of communication Capture of the vessel Theft of confidential data Compromise of computers and operating systems
Global Navigation Satellite System (GNSS) and GPS	Jamming attacks Weak signal level Dos/DDos attacks Editing Packages. Editing packages is the modification of created or intercepted packages. It involves modifying packages in a way that is difficult or impossible to do during package assembly.	Vessel malfunction Delays in the provision of services Capture of the vessel Theft of valuable data GPS provides false information.
Radar	Jamming attacks Dos/DDos attacks	Vessel malfunction Loss of life and cargo. Delays in freight management
Global Maritime Distress System (**GMDSS** – global maritime communication system in times of distress and to ensure the safety of navigation)	Malicious software Dos/DDos attacks Jamming attacks Signal muting	Incorrect coordinates of the ship's position. In the event of an emergency, the ship will not be able to call for help. Further attacks on the ECDIS system

Industrial Control Systems (**ICS** – industrial control systems, this is the designation of several types of control systems, including systems of supervisory control and data acquisition Supervisory Control and Data Acquisition, SCADA)	Incorrect operation of ACMS (Automatic Control Maritime System) No support for checking system integrity Vulnerability of information Poor patch management Hardware failures Incorrect security configuration Lack of network segmentation Weak password policies Absence of firewalls (Firewall, application-type network screens) No encryption Weak remote access policy Weak USB security policy Lack of SOS response	Ship hijacking Lack of ICS Data leakage Physical damage to objects Tampering with security systems Unplanned stops Equipment damage
Engine and mechanism control systems, as well as power control systems	Malware attack DoS/DDoS attacks Contraband Thefts Manipulation attacks	Ship hijacking Ship diversion Software may be interrupted Damage to the ship Financial losses Disclosure of confidential data
Very Small Aperture Terminal (VSAT) (small satellite ground station – terminal with a small antenna)	False signals Malware attack Theft	Theft of confidential data Downloading dangerous software Changing GPS coordinates
IT- network system	Poor access control DoS/DDoS attacks Weak password policies Malware attacks Poor patch management Incorrect security configuration Poor safety documentation Lack of network segmentation Lack of firewalls No encryption Weak remote access policy Weak USB security policy	Downloading malicious software Unauthorized physical access Unauthorized logical access Loss of confidential documents Financial losses Theft of confidential data Damage to reputation

Table 2. Vulnerabilities of information and navigation equipment (Source: Shumilova, K. 2024)

Common Vulnerabilities and Exposures (CVE) are listed in the Table 3. Each vulnerability is assigned an identification number of the type CVE-year-number and a security ranking with a score range from 0.0 to 10.0.

It is clear that the most important next step for maritime cyber security is to develop a cyber risk classification to separate the content, causes and targets of a cyber-attack. For the maneuvering process, this requires the creation of an updated ship security plan, ensuring appropriate training for the crew and shore service personnel, and assessing the state of the cyber security organization on the ship through periodic audits.

Identification of vulnerabilities	Level	Basic security evaluations
CVE-2020-26294 – Vela is a pipeline automation infrastructure built on Linux container technology. The Vela compiler prior to version 0.6.1 contains a vulnerability that allows server configuration disclosure. This affects all Vela users.	Average	5.3
CVE-2020-36167 – The problem was detected on a server in Veritas Backup Exec before version 16.2, 20.6 before patch 298543, and 21.1 before patch 657517. Loads the OpenSSL library from the installation folder on startup.	High	8.8
CVE-2021-21449 – SAP 3D Visual Enterprise Viewer version 9 allows the user to open a processed IFF file received from untrusted sources, which causes the application to crash and become temporarily unavailable until the user restarts the application.	High	8.8
CVE-2021-21468 – The BW database interface does not perform the necessary authorization checks for the authenticated user, allowing a hacker to read virtually any database table.	Average	6.5
CVE-2020-26773 – introduction of malicious code into the system – allows a remote authenticated hacker to execute arbitrary SQL commands (malicious code) using the date parameter.	High	8.8
CVE-2021-21465 – The BW database interface allows a low-privilege hacker to execute any crafted database queries by exposing the internal database. A hacker can include his own SQL commands that the database will execute without proper cleanup.	Critical	9.9
CVE-2021-21470 – SAP EPM Add-in for Microsoft Office version 1010 and SAP EPM Add-in for SAP Analysis Office version 2.8 allow a verified hacker with user rights to parse malicious XML files, which could lead to an application-based XXE attack.	Average	4.4
CVE-2019-25002 – The problem is in vulnerable software configurations.	Critical	9.8

Table 3. Vulnerabilities (CVE) of information systems according to data from the NIST laboratory (Source: Shumilova K. V., 2021; National vulnerability database / Information Technology Laboratory / NIST, 2021)

However, solving all issues of the organization of cyber security of shipping is a very difficult task. Therefore, in the future, we will consider the planning and management of cyber risks during maneuvering in the course of the voyage cycle of a sea vessel.

2.1. Distribution of information on the organization of ship movement into five semantic categories

Investigation of the consequences of cyberattacks carried out on a ship's maritime information systems based on data from cyber security reports indicate the vulnerable links that are created as a result of accessing these systems. Vulnerable ship systems include the following elements:

- navigation systems of the navigation bridge;
- cargo handling and management systems;
- systems of technical power plants and mechanisms that ensure the movement of the ship and control their work;

- ship access control systems;
- passenger service and management systems on passenger ships;
- administrative and social welfare systems of the crew;
- household and navigation communication systems.

Ship information from the organization of the ship's movement during the transportation of cargo in the voyage cycle can be divided into five meaningful categories: 1) notification of distress and danger; 2) navigation; 3) hydrometeorological; 4) operational; 5) private correspondence.

We will perform descriptive modeling of meaningful categories of the information space of sea routes to understand vulnerable links in cyber-attacks and find ways to manage their level.

In the *first category*, distress and danger messages are transmitted in ship-to-shore, ship-to-ship, shore-to-ship, and shore-to-shore directions. In the coast-to-coast direction, messages circulate between coastal radio stations of the rescue coordination center (RCC), meteorological and hydrographic centers according to established exchange rules. Messages about distress, dangers at sea, pirate attacks, dangerous weather phenomena and other non-standard situations are transmitted from the ship to the shore. The message forms are presented in the components of the Global Maritime Distress and Safety System (GMDSS) and are transmitted automatically after they are updated and initialized. Notifications related to marine pollution are sent in the form specified by the IMO and to the addresses specified in the Shipboard Oil Pollution Emergency Plan (SOPEP).

Shipowners are notified of ship attacks by standard notifications, autonomous and/or automatic ship identification systems (AIS). Messages about shipwrecks, dangers at sea, pirate attacks, dangerous meteorological phenomena and rescue operations are relayed from shore to ship and from ship to ship. In this category, there are notifications by individual participating vessels, confirmed by bilateral exchange. Reports of accidents to one's own vessel and other dangers detected at sea are immediately transmitted to the address of the nearest and/or serviced shore radio station and relayed until confirmation is received from the shore radio station. A vessel in close proximity to a second vessel in distress shall report its actions and assistance capabilities upon receipt of confirmation of the accident from shore. The exchange on the distress communication channel is maintained between the correspondents until the end of the rescue operation. Shore-to-ship, ship-to-shore management involves the exchange of information regarding the protection of the ship and port facilities. Information about accidents and dangers at sea is transmitted from the shore to the ship on emergency frequencies immediately from the moment of its receipt.

When organizing rescue operations, a radio station is appointed on a dedicated communication channel, which immediately transmits the instructions of the rescue coordination center to the participants of the operation. Exchange on this channel between correspondents is preserved until the end of the rescue operation. Alerts about danger at sea are transmitted by shore radio stations within three days as separate messages and in systems of maritime geographical areas in which various governments are responsible for navigation and weather warnings (NAVAREA – Navigational Area) and international automated notification systems (NAVTEX – Navigational Information over Telex) or until the danger expires.

The exchange of information flows between ships takes place in the case of the immediate proximity of the ship accident and the correspondent ship or after rebroadcasting the accident reports of the shore radio station. The dedicated communication channel is maintained permanently and is terminated after the completion of the rescue operation or upon instruction from the shore. When conducting rescue operations, the communication channel between the vessels and the *Coordinator on the spot* is controlled by the shore radio station. Notifications about sea pollution are transmitted by ships to the shore immediately in operational mode until the end of the incident.

The *second category* of information is determined by navigational messages in ship-to-shore and shore-to-ship directions. Typical and unregulated information exchange is carried out from ship to ship. From the shore, the ship receives information about identified navigational hazards, observations at sea about changes in navigation rules, information about areas of training and firing practice. It is transmitted in the NAVAREA and NAVTEX systems. Some important messages may be duplicated by both systems. In some cases, notices are provided by shipowners and/or port agents. Navigational information in the NAVAREA format is transmitted exactly according to the areas, with the schemes established by the international schedule, as well as directly in the NAVTEX format on a specified radio frequency.

Maritime agents, ship owners and their operators in the process of managing the operation inform, if necessary, the captains about the features of the port and the requirements related to entering it. Port authorities transmit information to the ship's captain in radiotelephone and circular mode once an hour. The vessel shall immediately and in accordance with the prescribed procedure notify the coastal administration of the coastal state of any danger detected at sea. Vessels engaged in special operations transmit information about the danger and measures to prevent it every hour or when they get too close to other vessels. In other cases, the exchange is not regulated and takes place on the basis of reciprocity.

The *third category* is hydrometeorological information, which includes separate notifications about dangerous phenomena. Weather data is transmitted from the shore to the ship according to the regulations. At the request of the shipowner, the captain is given instructions to follow the route indicated by the coastal meteorological centers. Information from the shore to the ship is transmitted by national centers under the terms of the NAVAREA system. Regional and local information is transmitted on request or circularly at set times by the NAVTEX system, port authority channels and shore-based VHF (ultra-short wave) radio stations. Facsimile weather maps are available on the global Internet. Sometimes shipowners give their instructions related to the weather (to stop, shorten the route, etc.) in the interests of commerce, operation and other features. Some shipowners require the ship to provide information on weather conditions on a regular basis. The transmission of weather information is also required when the ship is passing through coastal centers, as well as when conducting rescue operations. The regulation of such transmissions is established by relevant rules or separate instructions.

Ship-to-ship information exchange does not have a regular nature, it is not defined by the regulations except for emergency rescue operations, where such a procedure is established by the RCC or the OSC (*Onsite Coordinator*). In practice, these are fairly common streams of information on VHF during the exchange of ships that have met in the ocean. Hydrometeorological information is updated and transmitted in the normal mode directly, except for Sundays, by areas from the shore to the ship of individual services, which are established for the state in the NAVAREA system, as well as within the framework of transmission in the NAVTEX system. Duplication of messages can be performed at 6 and 12-hour intervals. When dangerous weather phenomena (hurricane, especially strong storm, tsunami) occur, information about them is reported every six hours.

The port authority informs about the local weather upon request from the ship. In some areas, weather reports are made by special VHF meteorological channels, port agents, ship owners and ship operators during regular communication sessions. Local radio and television broadcasts and Internet weather sites are sometimes valuable in this regard. When sailing under the guidance of the coastal center, the weather is transmitted in the form and volume set by it once a day or more often. Sometimes a ship makes such messages at the request of a shore radio station in exchange for the latter's agreement to accept its correspondence for further transmission.

The *fourth category* of information represents the exploitative exchange. This category is formed by shipping companies, port authorities, shore services, agencies in the directions shore-ship, ship-shore, shore-shore. The nature of the information between the shore and the ship is different regarding the activities of the

ship as well as third parties. Notices by time limits do not have a set order and are transmitted within the working day of the shore without considering the possible difference from the ship's time. To draw attention to ships while in port, when a constant watch on the bridge is not maintained, ship signaling duplicating means are sometimes used. Especially important information arrives immediately, at any time of the day. The main exchange between the ship and the shore is situational in nature, except for mandatory messages related to key moments of operation.

From the ship to the address of the ship owner and operator, information is sent about: 1) coordinates of movement at sea; 2) expected arrival at the port; 3) berthing under cargo operations; 4) berthing under auxiliary operations; 5) the expected date of departure from the port. According to the company's rules, the transmission of information regarding navigation at sea is carried out once every 1-3 days at noon ship's time, about berthing with cargo operations every day, the rest - after the end of the work cycle. The charterer has the right to request a different frequency of such transmissions. The most typical are 2-week, 10-, 7-, 5-, 3-, 2-, 1-day messages. Sometimes information is needed within hours.

The *fifth category* defines information about private correspondence in ship-to-shore, shore-to-ship, and ship-to-ship directions. As a rule, it has no value and is useful only to the sender and receiver. Some shipping companies and agencies carry out censorship to avoid information leakage. Private correspondence is prohibited during military operations and special transportation. The order of flow of private information and control over compliance with the established order is entrusted to the captain of the ship. The periodicity of information exchange is not regulated, but sometimes restrictions related to the operating conditions of the vessel are introduced. Private information is not regulated, it is quite typical and is carried out with the help of subscribers who have the possibility to use satellite communication with the ship.

The classification of cyber risks will be carried out according to the characteristics of the navigation parameters of the receivers on the ship and in the shore navigation equipment, which can receive the internal signals of the ship and external transmitters.

2.2. Descriptive modeling of meaningful categories of the information space of sea routes

Descriptive modeling of the information space of waterways allows us to claim that any deviations from the regulations in categories 1-4 of messages lead to destabilization of the information space and create the prerequisites for emergency situations. The completeness and adequacy of the presentation of categories, directionality and periodicity of messages allow to formalize the information space of the shipping process in order to establish the relationship between its disturbances and the occurrence of prerequisites for emergency situations. Solving the tasks is possible using modeling methods with parametric and non-parametric evaluation of complex technical moving systems. The following methods are most developed: matrix modeling, graph-analytical, description of information flows in the form of a tree-type graph, information communication schemes and research analysis of management tasks.

When performing the research, a graph-analytical method was used, which allows you to visually follow the nature of the movement of information and determine the influential points in the event of cyber-attacks. Considering the actual data, these methods most objectively allow to determine the form of interdependent parameters of ship maneuvering control and its quantitative description in the form of a cluster.

When conducting the research, we will use the graph-analytical method, which allows you to visually follow the nature of the movement of information and determine the influential points in the event of cyber-attacks. We will determine the structural components of the information space of the movement process and highlight the lines of communication and the transition of information flows by direct, reverse, and local channels

between the elements of the maneuvering control system and the information relationship between them (Fig. 1).

From the specified research methods, we will use matrix and graph analytical methods to formalize the qualitative and quantitative properties of information flows of the voyage cycle. They allow you to decompose information, perform clustering of information flows, and allocate clusters of information security of ship maneuvering management, allocating it to closed access for cyber-attacks (Vil's'kyy, 2012).

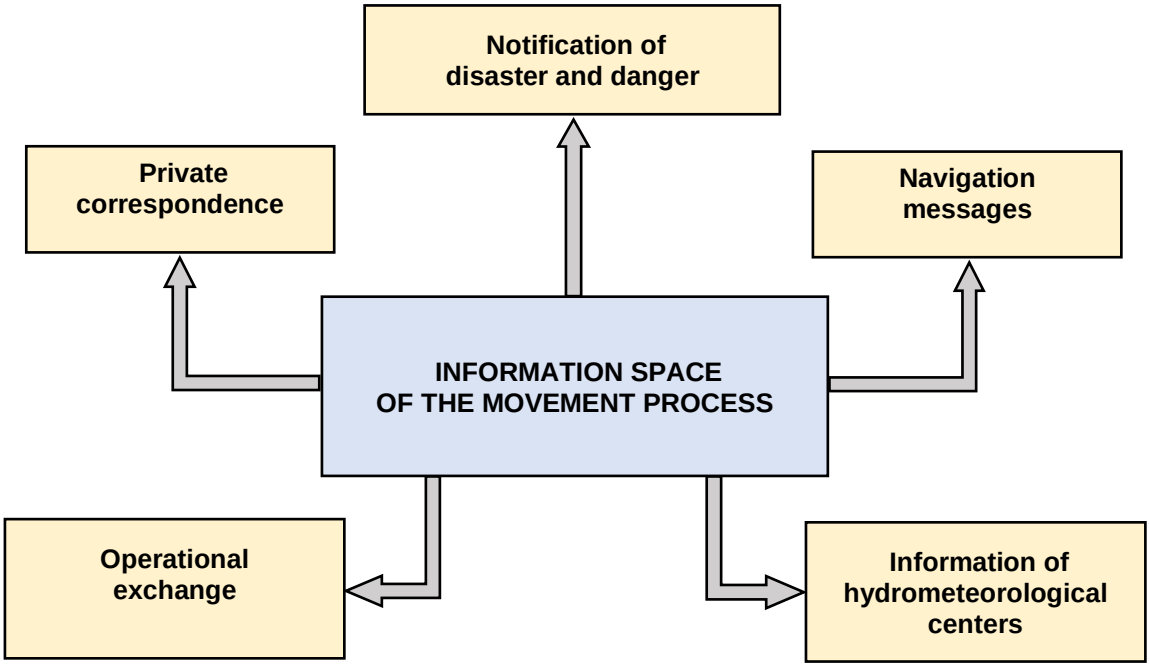

Figure 1. The general structural diagram of meaningful categories of the information space

Let us build a diagram of the structural components of the navigation information space, where we will especially highlight the isolated cluster of the ship with ship information systems $M_к$ (Fig. 2). It allows you to switch to manual control of the maneuvering process in cases where a cyber-attack leads to the failure of regular navigation devices of the navigation bridge.

We will build a graphological scheme of the information space of navigation with a display of information sources in the form of vertices of an oriented graph, showing their relationships (Fig. 3). Each pair of vertices M_i and M_j has a relationship directed from M_i to M_j only if the transition of information from M_i to M_j is carried out. The vertices of the information flow graphs in the ship-to-shore, ship-to-ship, shore-to-ship, and shore-to-shore information direction categories are presented in tabular form (Table 4).

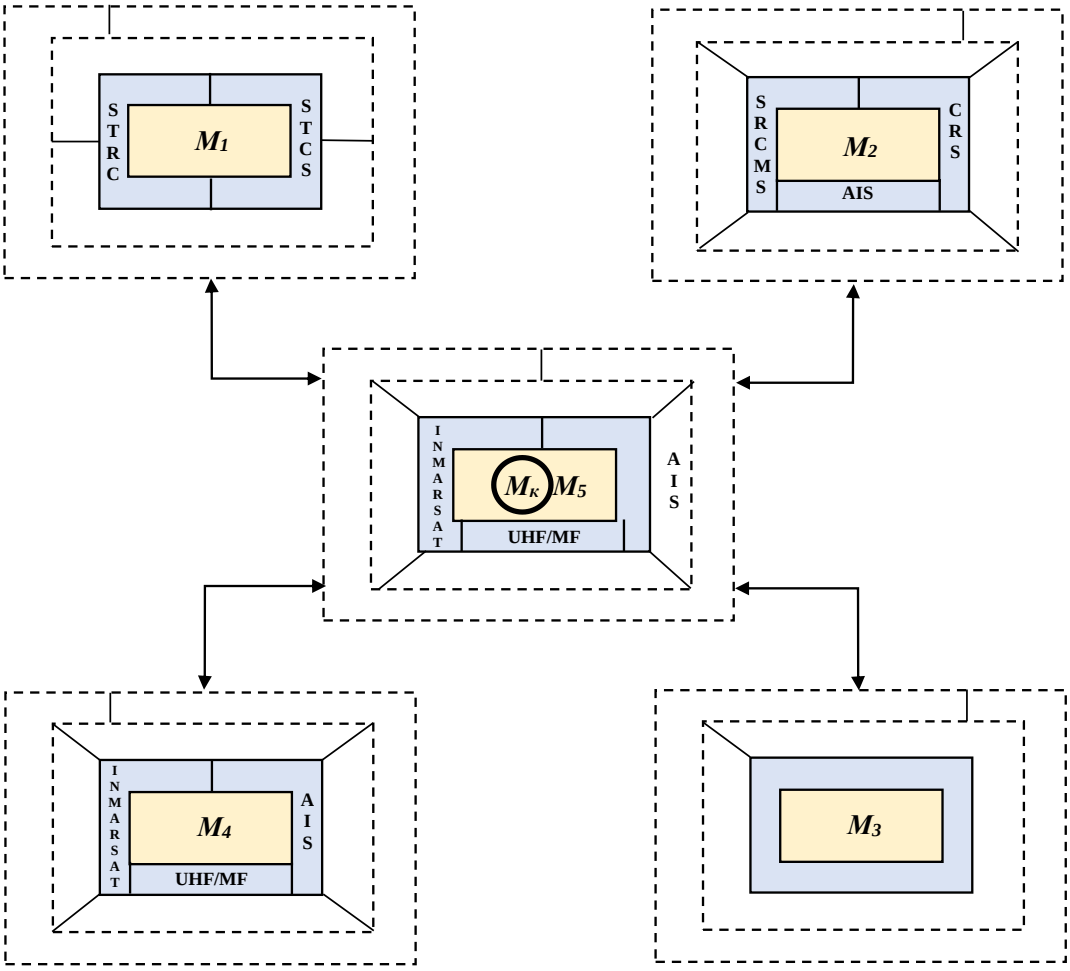

Figure 2. Structural components of the navigation information space:

M_1 – port information systems (STRC – ship traffic regulation center, STCS – ship traffic control system + area of responsibility of the state); M_2 – information systems on waterways (SRCMS – system of remote control of the movement of ships, CRS – coastal radar station, AIS); M_3 – satellite information systems; ***Мк,*** M_5 – isolated ship cluster and ship information systems (INMARSAT, AIS, UHF/MF – intermediate wave range); M_4 – ship information systems (INMARSAT, AIS, UHF/MF)

We will consider the characteristics of information flows in the system and their influence on the information field of the navigation process using the property of graph isomorphism, which is possessed by information sources on waterways.

The rows of the matrix characterize the number of sources of information for the shipmaster, and the columns – the number of interconnections of information flows at this point of the ship's route. The adjacency matrix *R* and the value of the state order determine the storage duration of the components that are intermediate in relation to the original ones.

Degree adjacency matrices $R, R^2, \ldots, R^N$ and the total matrix $R = \sum_{n=1}^{N} R^n$ are formed so that they simplify the recording of information models and establish a mutually unambiguous correspondence of data exchange between the components of the graph as follows (1):

$M_{11} - M_{12} = E_{11}$, $M_{11} - M_{21} = E_{12}$, $M_{11} - M_{22} = E_{13}$, $M_{11} - M_{23} = E_{14}$, $M_{11} - M_{52} = E_{1.10}$

$M_{12} - M_{11} = E_{21}$, $M_{12} - M_{21} = E_{22}$, $M_{12} - M_{22} = E_{23}$, $M_{12} - M_{23} = E_{24}$, $M_{12} - M_{52} = E_{2.10}$

$M_{21} - M_{11} = E_{31}$, $M_{21} - M_{22} = E_{32}$, $M_{21} - M_{23} = E_{33}$, $M_{21} - M_{24} = E_{34}$, $M_{21} - M_{52} = E_{3.10}$

$M_{52} - M_{12} = E_{10.1}$, $M_{52} - M_{21} = E_{10.2}$, $M_{52} - M_{22} = E_{10.3}$, $M_{52} - M_{23} = E_{10.4}$, $M_{52} - M_{11} = E_{10.10}$ (1)

№	Vertices of information flow graphs	Information formation systems	
		Sources	Receivers
1.	M_1-M_2	port	coastal
2.	M_1-M_3	port	satellite
3.	M_1-M_4, M_1-M_5	port	ship
4.	M_2-M_1	coastal	port
5.	M_2-M_3	coastal	satellite
6.	M_2-M_4, M_2-M_5	coastal	ship
7.	M_3-M_1	satellite	port
8.	M_3-M_2	satellite	coastal
9.	M_3-M_1, M_3-M_5	satellite	ship
10.	M_4-M_1	ship 1	port
11.	M_4-M_2	ship 1	coastal
12.	M_4-M_3	ship 1	satellite
13.	M_4-M_5	ship 1	ship 2
14.	M_5-M_1	ship 2	port
15.	M_5-M_2	ship 2	coastal
16.	M_5-M_3	ship 2	satellite
17.	M_5-M_4	ship 2	ship 1

Table 4. Vertices of information flow graphs

Let us create static adjacency matrices R, R^2, …, R^N and the total matrix $R = \sum_{n=1}^{N} R^N$. To simplify the entry of the matrix, we establish a mutually unambiguous correspondence of the information exchange processes between the components as follows:

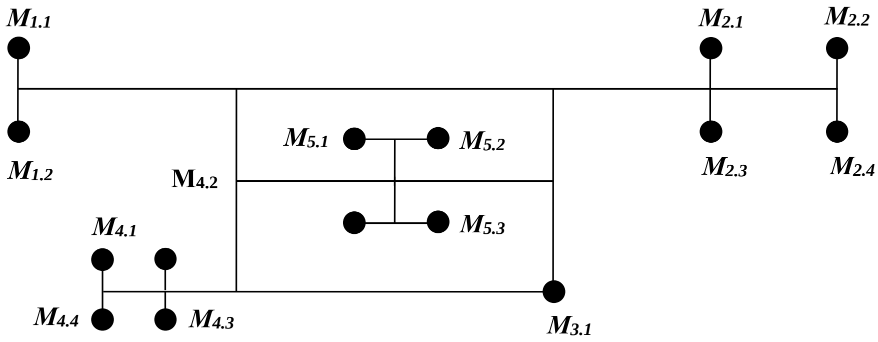

Figure 3. Graphological diagram of the information space of the shipping process

Let us compile the corresponding message adjacency matrix (2):

$$R = \begin{pmatrix} E_{11}\ E_{12}\ E_{13}\ E_{14}\ E_{15}\ E_{16}\ E_{17}\ E_{18}\ E_{19}\ E_{1.10} \\ E_{21}\ E_{22}\ E_{23}\ E_{24}\ E_{25}\ E_{26}\ E_{27}\ E_{28}\ E_{29}\ E_{2.10} \\ E_{31}\ E_{32}\ E_{33}\ E_{34}\ E_{35}\ E_{36}\ E_{37}\ E_{38}\ E_{39}\ E_{3.10} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ E_{10.1}\ E_{10.2}\ E_{10.3} E_{10.4} E_{10.5}\ E_{10.6}\ E_{10.7}\ E_{10.8}\ E_{10.9}\ E_{10.10} \end{pmatrix} \quad (2)$$

The number of states is determined by the order of the adjacency matrix. Each state determines the volume of information when performing certain types of maritime operations, and the technology of it's implementation. At the same time, the same operation can be performed in different ways, each of which requires a different amount of information. The information security cluster by maneuvering the vessel opens up the possibility of selective data collection, facilitates the calculation of information security threats, modeling of probabilistic distributions of hazards in sections of the waterway. In this case, the sample uses many categories of nautical messages, each of which is represented by a set of a certain number of subclasses and is described by the expression:

$$X_L = \{X_1\,(K_{n1}),\ X_2\,(K_{n2}),\ X_3\,(K_{n3}),\ \dots,\ X_L\,(K_{nm})\} \quad (3)$$

where X_L – set of classes of nautical messages; K_n – set of subclasses of each nautical message.

Based on the theory of cluster analysis, the task of clustering information flows of waterways during maneuvering includes the gradation of existing nautical messages on a number of non-intersecting subsets. It is necessary that each cluster consists of objects close to the metric, and the objects of different clusters differ significantly. At the same time, in the process of clustering, an important aspect is the concept of distance $p\ (x, x')$, which plays the role of the number of objects and connections involved in the formation and transmission of a certain stream of data parameters. Algorithmization of formation of clusters of information flows of waterways is performed using heuristic graph algorithms, statistical algorithms, and hierarchical clustering algorithms. The calculation of the cluster structure of information security should be performed in symbiosis of statistical methods with the method of hierarchical clustering.

The expediency of the hierarchical clustering method consists in dividing flows into non-intersecting subclasses and constructing using dendrogram graphs that clearly define intracluster connections. For the information security space of the waterway, a metric is introduced showing the magnitude of determining the distances between clusters. This space is called metric. For calculations in the metric space of information security clusters, the Euclidean metric is used, in which cluster distances correspond to the expression:

$$d_{ij} = \sqrt{\sum_{k=1}^{n} \frac{(x_{ik} - x_{jk})^2}{\sigma_k^2}} \quad (4)$$

where p_{1i} is the value of the probabilities of occurrence of risks according to the relevant prerequisites of threats; X_i – the category of nautical message; μ_x – *the* parameter of the risk occurrence for information security of the ship's maneuvering.

3. RESULTS AND DISCUSSION

3.1. Classification of navigational cyber risks. Semantic categories of incoming ship information flows

The classification of cyber risks will be carried out according to the characteristics of the navigation parameters of the receivers on the ship and in the shore navigation equipment, which can receive the internal signals of the ship and external transmitters. In order to structure the various types of impact of cyberattacks on the navigation devices of the navigation bridge and the system of coastal aids to navigation, we will classify them according to their functional purpose, the degree of impact of cyberattacks on the information with which this device works, and the ability of the ship to manage this impact of cyberattacks (Shumilova, K., 2022). This will make it possible to switch to using devices that are not affected by such attacks. To do this, it is necessary to determine the semantic categories of information flows, their structure and content, and perform their descriptive modeling to analyze the degree of impact of cyberattacks and research ways to reduce the impact when they occur (Fig. 4).

Semantic categories of the input information flows to the ship, their structure and content are of interest for navigation purposes. Other types of information and its content should not be transmitted simultaneously with navigational information. Such synchronous transmission can be perceived as a cyber-attack. The origin of the transmission of ship information is carried out from devices, the principle of operation of which is based on the transmission of information in the form of a sounding signal and the reception of the reflected signal after returning to the ship. According to the content of information, the object of cyber-attacks are navigational, hydrometeorological and operational types. The content of the distress and danger transmission is not affected by cyber-attacks since the channel does not have a receiver in the system. Private information is usually checked only at the direction of the shipowner. When using information for the usual and automatic method of controlling the maneuvering of the ship, it is susceptible to the influence of cyber-attacks, and when using a special method, constructive measures are taken to isolate the influence of cyber-attacks and the operation of the ship when they occur.

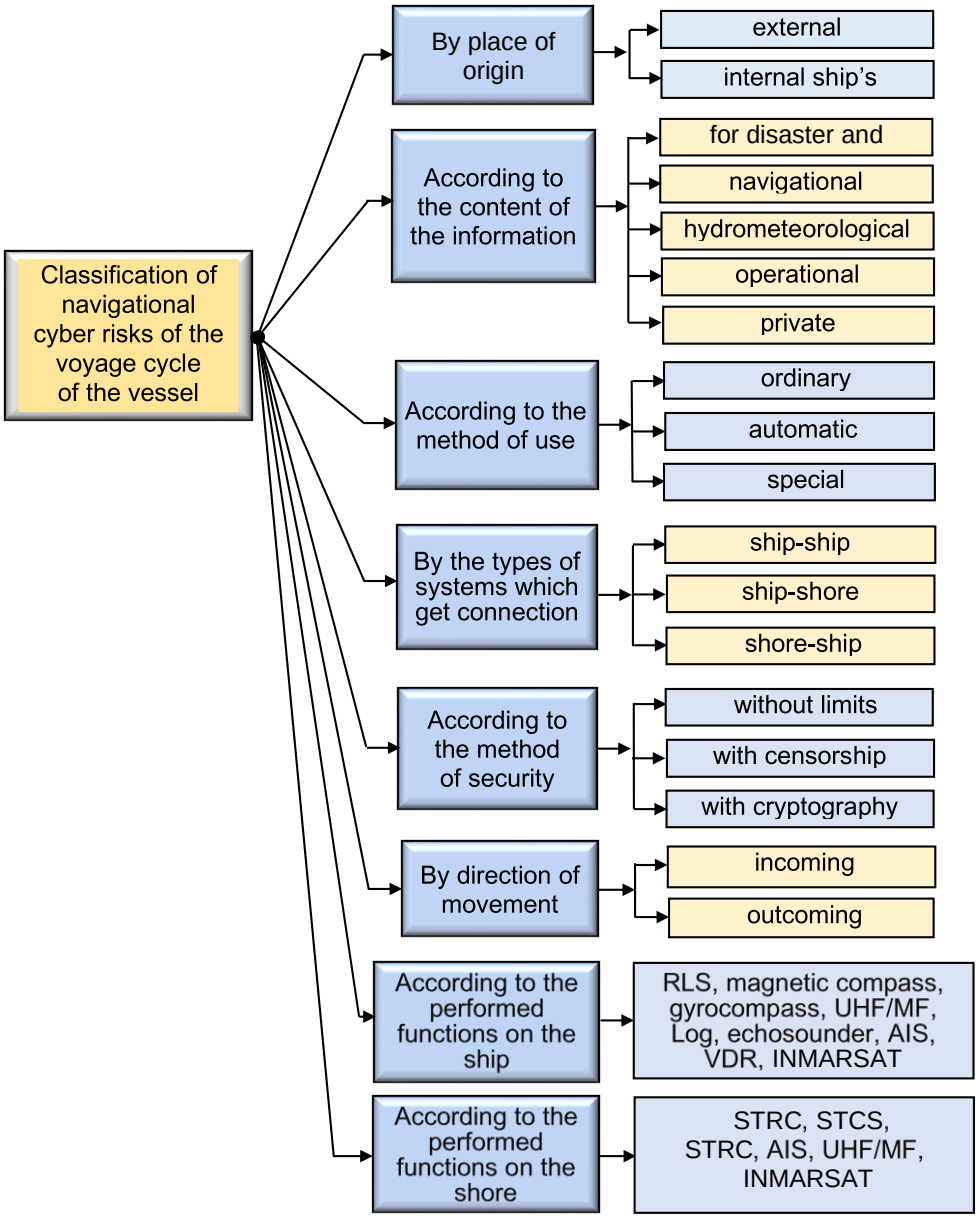

Figure 4. Classification of navigational cyber risks of the voyage cycle of the vessel:

RLS – radiolocation station, AIS – automatic identification system, VDR – voyage data recorder, UHF/MF – radio communication on ultra-short and intermediate waves, INMARSAT – international maritime satellite communication, STRC – ship traffic regulation center, STCS – ship traffic control system, SRCMS - system of remote control of the movement of ships

According to the types of systems that communicate, ship-to-ship and shore-to-ship systems are the most affected by cyber-attacks. At the same time, as our analysis showed, the zones of dangerous navigation risks coincide with the zones of occurrence of cyber-attacks (Modernized maritime industry transports cyberthreats to sea, 2019).

According to the method of protection, the usual way of transmitting information and with censorship does not protect against the influence of cyber-attacks. The only way to securely transmit data is to transmit it

with cryptography, but it requires the use of special technical means and the coordination of a single international system. According to the direction of movement, the source information of the own ship, as a rule, does not contain signals of cyber-attacks. Signals of cyberattacks are perceived with incoming streams of information that arrive at radio receivers or navigation devices, the principle of operation of which involves receiving a reflected probing signal.

According to the functions performed on ships, the RLS, UHF/MF, log, echosounder, AIS, VDR, and INMARSAT satellite system have receivers that can receive useful and specially created parasitic signals. Therefore, they must be disabled in the event of cyber-attacks, and it is necessary to use navigation devices and maneuver control methods that are not affected by cyber-attacks. For this, you need to use a magnetic compass, a gyrocompass, and astronomical and visual methods of determining the position of the vessel (Maltsev *et al*., 2019; Surinov & Shumilov, 2023).

According to the functions performed on shore, navigation systems, coastal buoyage system, navigation devices STCS, SRCMS, STRC, AIS, UHF/MF and satellite system, according to the principle of operation have receivers that can receive useful and specially created harmful signals. For this reason, they should be disabled in the event of cyber-attacks. It is necessary to use navigation devices and methods of maneuvering ships that are not affected by cyber-attacks in a certain area of responsibility.

Analyzing the above data (Pavlinović *et al*., 2023; Ha, H.-T. *et al*., 2023; Kimberly & Kevin, 2018; Kanwal *et al*., 2022; Tam, K. *et. al*., 2019; Onishchenko *et al*., 2022; Nikčević-Grdinić, 2017), it is clear that cyber-attacks on ship's navigational information equipment can significantly affect the probability of occurrence of a navigational risk. Therefore, in matters of cyber security (Rolf & Aalberg, 2018; Ramirez-Peña *et. al*., 2020; Semlambo *et. al*., 2022; . Stazić *et. al.*, 2017; U.S. Coast Guard Warns Shipping Industry on Cybersecurity, 2019), it is important for ships to focus on the main aspects of the vulnerability of navigation equipment (Table 5; Shumilova K. V., 2021):

- The protection of own data of the shipping companies and ships during the voyage cycle must be based on the timely implementation of modern intelligent and preventive solutions in the field of IT/OT (Information Technologies/Operational Technologies).
- Improvement of countermeasures against cyberattacks, which must be based on interaction using the software of all maritime structures that interact with ships during the voyage cycle.
- Early implementation of system solutions for preparing vessels for cargo transportation to work in the conditions of cyberattacks and issuing recommendations for managing maneuvering in the event of their occurrence.
- Conducting cyber-independent monitoring of the vessel's position by astronomical and visual means unaffected by cyber-attacks.

№	Categories of procedures. Devices	Necessary actions
1.	**Responsible persons for ensuring the protection of information of the ship's IT system.** List of responsible persons.	Update the list of responsible persons in a timely manner, considering changes in crew, illness, mental state and redistribution of responsibilities.
2.	**List of ship's IT systems.** Operational documentation for each system: **AIS, ECDIS, VDR, TOS, EPIRB, GNSS, GPS**, etc.	Compile and maintain an up-to-date list of all the ship's IT equipment: administrative systems and networks; communication systems; undercarriage systems; cargo handling and management systems; engine, machine and power management systems; access control systems; passenger service and management systems; ship's public internet networks intended for use by passengers.
3.	**Organizational and administrative documents.** Rules, instructions and procedures on cyber security, in which restrictions on unauthorized actions of the crew are introduced, demarcation of access is described, requirements for passwords.	Familiarize the crew with mandatory documents for personal signature: introductory briefing on the ship; initial training at the workplace; repeated training at the workplace; unscheduled training at the workplace; targeted instruction.
4.	**Software. Connection.**	Use only installed software (software) on working IT devices. Do not open attachments in letters with unfamiliar extensions, from unfamiliar addressees. Do not ignore warning messages from programs. Do not connect unexpected wireless devices to the network, even if it is very convenient for you. Remember that wireless connections must be properly secured.
5.	**Network equipment.** **Event logs** – in Microsoft Windows, a standard way for applications and the operating system to record and centrally store information about important software and hardware events.	Check that there are no resources available simultaneously to the ship's IT system and the network.

Table 5. Recommended procedures for cyber security of the ship information and navigation system (Source: Shumilova K. V., 2021)

International cooperation on cyber security already exists within the framework of the IMO. It is only necessary to spread the requirements that exist to the states for navigational risks. In addition, it requires the introduction of an electronic navigational calculation device when performing observational calculations during cyber-attacks.

Recommendations:

- It is necessary to increase the level of training for shipmasters to perform their work in traditional ways: determining the position of the ship by visual means; the use of astronomical methods of determining the position; manual documentation of movement and maneuvering parameters.
- In addition, it is necessary to develop an electronic chronometer, to provide the ship with a sextant and a stopwatch. In addition to those indicated on the ship, it is necessary to have a limited number of spare paper maps for observational counting in case of cyber-attacks.
- In addition, it is necessary to oblige the countries in the zone of which the cyber-attack occurred to transfer detailed information to the International Maritime Organization IMO for putting it on maps, charts and other information sources on the safety of navigation. Although partially, such a system already exists.

4. CONCLUSIONS

The main problem of the global system of cyber security of maritime information channels is the lack of qualified state structures that organize and control the proper state of supervision of the training of personnel of sea vessels to work in conditions of cyber-attacks (Andrew, 2021; Bratić *et al*., 2019; Calder, 2020). Therefore, it is necessary to train maritime specialists in cyber security, shore personnel who manage the work of ships at sea, and ship navigation bridge teams because in conditions of incomplete information, they have to take decisions regarding the movement of the ship in the event of navigational risks and emergency events. The given classification of cyber risks made it possible to develop a logical structure of a single information bank of subject data of the ship maneuvering control system, based on the grouping of message flows according to the use of the cluster connection coefficient between them and the nature of the influence of cyber risks. The obtained results can be used in the design of systems of information support for decision-making when maneuvering in conditions of cyber-attacks.

The assessment of the accuracy of the position, which the ship should use in cyber-attacks and performed observational calculations, will depend on:

- technical characteristics of backup devices, which are used when choosing methods of position control and accuracy assessment, when they are used and calculated;
- time of day, availability of coastal landmarks for determining the location of the vessel by visual methods and visibility of the horizon line for using astronomical methods during navigational work;
- readiness of the navigator to perform procedures to determine the position of the ship by visual and astronomical methods and the presence of the necessary navigational instruments and tools – a chronometer, a stopwatch, a sextant, a magnetic compass direction finder on the upper deck and a navigational calculator.

According to the recommendations of the Bridge Procedures Guide (Bridge Procedures Guide, 6th Edition, 2022), four stages of safe passage planning and accident-free movement planning are offered when planning a safe voyage and organizing an accident-free movement: I. Appraisal. II. Planning. III. Execution. IV. Monitoring (New Bridge Procedure Guide released, 2022).

However, the accuracy of navigation in restricted sailing conditions cannot be guaranteed only by meeting the requirements of the IMO and the International Association of Lighthouse Authorities (IALA). Therefore, it does not ensure the navigational safety of sailing a large tonnage vessel in restricted conditions at short distances to danger (less than two miles). In such sailing conditions, it is additionally necessary, after planning the route of the voyage cycle, to take into account the analysis of navigational risks that will be encountered in the future passage.

The shortcoming of the existing recommendations is precisely the lack of a separate *risk analysis and assessment stage*, which must be performed after planning the passage coordinates (Patent na korysnu model 151907 (51) MPK G08G 3, Maltsev, Surinov, Shumilova K. V., 2022).

The accident-prone sections of the passage must be identified in advance during the planning of the voyage cycle using navigation manuals – charts, sailing directions and other informational materials on navigation and cyber risks. This is important, because the lack of time during voyage does not allow the necessary calculations to be performed in a timely manner.

The second problem when planning the passage in the voyage cycle is the lack of systematized data on cybernetic dangerous areas. Therefore, we will consider accident-prone areas of navigational risks, information on which is included in charts, sailing directions and other navigational sources, as those that coincide with the existing areas of probable cyber risks. The reason for such a decision is the most likely threat of the use of accident-prone areas by cyber criminals to organize cyber-attacks because the existence of prerequisites for the occurrence of an accident has been reliably established. Therefore, it is necessary to introduce in the meaningful model of preparation for the passage a separate stage of planning the voyage cycle, such as *analysis and assessment of navigational and cyber risks*, which must be performed after planning the coordinates of the passage (Patent na vynakhid MPK G08G 3/02 (2006.01), Maltsev, Shumilova K. V., Shumilov D. I., Muraviov, 2023). Completion of such a stage will allow to prepare the ship and the crew for sailing in accident-prone areas while managing the ship in conditions of navigational risks and in the event of cyber-attacks.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

10 naibilsh vrazhaiuchykh kiberatak v istorii, 2021. Available at: https://itta.info/10-najbilsh-vrazhayuchix-kiberatak-v-istorii/

Acronis pidhotuvala zvit acronis pro kiberzahrozy na osnovi informatsii z merezhi operatyvnykh tsentriv kiberzakhystu Acronis, 2023. Available at: http://surl.li/gqzzl

Akpan, F., et al., 2020. Cybersecurity Challenges in the Maritime Sector, Network, 2(1), pp. 123-138. Available at: https://doi.org/10.3390/network2010009.

Andrew, B. M., 2021. Chapter 10 - Information security and cyber threats and vulnerabilities. Intermodal Maritime Security, Elsevier, pp.169-193. Available at: https://doi.org/10.1016/B978-0-12-819945-9.00010-1.

Bolbot, V. et al., 2020. A novel cyber-risk assessment method for ship systems. Safety Science, 131. Available at: https://doi.org/10.1016/j.ssci.2020.104908.

Bratić, K. et al., 2019. Review of Autonomous and Remotely Controlled Ships in Maritime Sector, Transactions on Maritime Science, 8(2), pp. 253-265. Available at: https://doi.org/10.7225/toms.v08.n02.011.

Calder, A., 2020. Cyber Security: Essential principles to secure your organization. IT Governance Publishing, p. 69. Available at: https://doi.org/10.2307/j.ctv10crcbg.

Caprolu, M. R., et al., 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. in IEEE Communications Magazine, 58(6), pp. 90-96. Available at: https://doi.org/10.1109/MCOM.001.1900632.

Csorba, M. J., Ramos de Carvalho, C., and Boff, S., 2017. Plain Sailing? Observations of Cybersecurity and Network Health Problems in Control Systems at Sea. Paper presented at the OTC Brasil, Rio de Janeiro, Brazil. Available at: https://doi.org/10.4043/28039-MS.

Cyber attacks on the rise in the maritime industry, 2023. Available at: https://prosertek.com/blog/cyber-attacks-in-the-maritime-industry/

Egloff, F. J., 2022. The Sea and Cyberspace: Comparison and Analytical Lines of Enquiry. Semi-State Actors in Cybersecurity (New York, 2022; online edn, Oxford Academic, 21 Apr. 2022). Available at: https://doi.org/10.1093/oso/9780197579275.003.0005

Guide to Industrial Control Systems (ICS) Security. Retrieved from https://www.nist.gov/publications/guide-industrial-control-systems-ics-security.

Gunes, B., Kayisoglu, G. and Bolat, P., 2021. Cyber security risk assessment for seaports: A case study of a container port. Computers & Security. Vol. 103, p. 102196. Available at: https://doi.org/10.1016/j.cose.2021.102196.

Ha, H.-T., Ngo, L., Pham, V.-C., and Nguyen, T.-L., 2023. The Improvement Model of Navigational Safety for Inland Waterway Transport. Transactions on Maritime Science, 12(1). Available at: https://doi.org/10.7225/toms.v12.n01.003.

Hemminghaus, C., Bauer, J., Padilla, E., 2021. BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 15(1), pp. 35-44. Available at: http://dx.doi.org/10.12716/1001.15.01.02.

IMO / Maritime cyber risk, 2023. Available at: http://surl.li/rbwep

Informatsiina, komunikatsiina ta kiber-vrazlyvist krainy: analizuiemo prychyny ta naslidky, 2019. Available at: https://ecpl.com.ua/news/14844/

Kanwal, K., et. al., 2022. Maritime cybersecurity: are onboard systems ready? Maritime Policy & Management, pp. 1-19. Available at: https://doi.org/10.1080/03088839.2022.2124464.

Kardakova, M. et al., 2020. Cyber Security on Sea Transport. In: Murgul, V., Pasetti, M. (eds) International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2018, EMMFT-2018, Advances in Intelligent Systems and Computing, 982. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-19756-8_46.

Kavallieratos, G. and Katsikas, S., 2020. Managing Cyber Security Risks of the Cyber-Enabled Ship. Journal of Marine Science and Engineering, 8(10), p. 768. Available at: https://doi.org/10.3390/jmse8100768.

Kimberly, T., and Kevin, D. J., 2018. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy, pp. 147-164. Available at: https://doi.org/10.1080/23738871.2018.1513053.

Lee, A. R. and Wogan, H. P., 2018. All at Sea: The Modern Seascape of Cybersecurity Threats of the Maritime Industry. OCEANS 2018 MTS/IEEE Charleston, Charleston, SC, USA, pp. 1-8, Available at: https://doi.org/10.1109/OCEANS.2018.8604554.

Maltsev, A. S., et al., 2019. Sistemy prinyatiya resheniy po upravleniyu dvizheniem sudna, monografiya, Kherson: Kherson State Maritime Academy, p. 244.

Maritime cyber-attacks up by 900% in three years, 2020. Available at: http://surl.li/rbwep

Modernized maritime industry transports cyberthreats to sea, 2019. Available at: https://www.csoonline.com/article/3410236/modernized-maritime-industry-transports-cyberthreats-to-sea.html

National vulnerability database / Information Technology Laboratory / NIST, 2021. Available at: https://nvd.nist.gov/

National vulnerability database, 2023. Available at: https://nvd.nist.gov/

New Bridge Procedure Guide released, 2022. Available at: https://sqemarine.com/new-bridge-procedure-guide-released/

Nikčević-Grdinić, J., 2017. Improving Safety at Sea Through Compliance with International Maritime Safety Codes. Transactions on Maritime Science, 6(2), pp.130–139. Available at: https://doi.org/10.7225/toms.v06.n02.005.

Onishchenko O., et al., 2022. Ensuring Cyber Resilience of Ship Information Systems. TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, 16(1), pp. 43-50. Available at: http://doi.org/10.12716/1001.16.01.04.

Patent na korysnu model 151907 (51) MPK G08G 3/02 (2006.01), 2022. Systema vyznachennia navihatsiinykh ryzykiv reisovoho tsyklu ta upravlinnia yikh rivnem. / Maltsev A. S., Surinov I. L., Shumilova K. V. Zaiavnyk Natsionalnyi universytet «Odeska morska akademiia». – 2022 01850 Available at: https://sis.ukrpatent.org/uk/search/detail/1707808/.

Patent na vynakhid MPK G08G 3/02 (2006.01), 2023. Systema upravlinnia kiberbezpekoiu manevruvannia morskoho sudna pry reisovomu tsykli. / Maltsev A. S., Shumilova K. V., Shumilov D. I., Muraviov H. M. Zaiavnyk Natsionalnyi universytet «Odeska morska akademiia». – № a202300014; zaiavleno 03.01.2023; opublikovano 09.08.2023, Biul. 32, p. 139-140. Available at: https://sis.nipo.gov.ua/uk/search/detail/1722440/.

Pavlinović, M., Račić, M. and Mišura, A., 2023. The Importance of Digitalization for Sustainable Development of Maritime Industry. Transactions on Maritime Science. 12(2). Available at: https://doi.org/10.7225/toms.v12.n02.w03.

Ramirez-Peña, M. et al., 2020. Assessing Sustainability in the Shipbuilding Supply Chain 4.0: A Systematic Review, Sustainability 2020, 12(16), p.6373. Available at: https://doi.org/10.3390/su12166373.

Rolf, B., & Aalberg, A. L., 2018. Maritime navigation accidents and risk indicators: An exploratory statistical analysis using AIS data and accident reports. Reliability Engineering & System Safety, pp. 174-186. Available at: https://doi.org/10.1016/j.ress.2018.03.033.

Schroedinger's Pet(ya), 2017. Available at: https://securelist.com/schroedingers-petya/78870/

Sea Traffic Management: Efficiency and Cybersecurity, 2023. Available at: http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-113223

Semlambo, A., Mfoi, D. and Sangula, Y., 2022. Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA). Journal of Computer and Communications, 10, pp. 29-43. Available at: https://doi.org/10.4236/jcc.2022.1011003.

Shumilova K. V., 2021. Realizatsiia stratehii kiberbezpeky v systemi upravlinnia bezpekoiu sudna | Implementation of the strategy of cybersecurity in safety management systems of the ship / Shumilova K.V. // Naukovo-tekhnichnyi zbirnyk «Sudnovodinnia» / «Shipping & Navigation». – Odesa: NU «OMA», 2021, Vypusk 31, pp. 99-107. Available at: https://doi.org/10.31653/2306-5761.31.2021.99-107.

Shumilova, K., 2022a. Classification of navigational risks of the ship's voyage cycle. The Scientific Heritage, 95, pp. 52-72. Available at: https://doi.org/10.5281/zenodo.7014246.

Shumilova, K., 2022b. Development of the method for planning navigational risks in preparation of a ship voyage cycle. Science and Education a New Dimension, X(34), 268, pp. 23-31. Available at: https://doi.org/10.31174/SEND-NT2022-268X34-05.

Shumilova, K., 2022c. Systematyzovanyi pidkhid do klasyfikatsii navihatsiinykh ryzykiv reisovoho tsyklu morskoho sudna. Scientific Collection «InterConf+», 24(121), pp.337-358. Available at: https://doi.org/10.51582/interconf.19-20.08.2022.032

Shumilova, K., 2023. Pryntsypy normuvannia pry planuvanni parametriv reisovoho tsyklu morskoho sudna v rehlamentuiuchykh dokumentakh mizhnarodnoi morskoi orhanizatsii. Scientific Collection «InterConf+», (34(159), pp. 344-359. Available at: https://doi.org/10.51582/interconf.19-20.06.2023.034.

Stazić, L., Komar, I., and Račić, N., 2017. Evaluation Methodology for Ship's Planned Maintenance System Database. Transactions on Maritime Science, 6(2), pp. 109-116. Available at: https://doi.org/10.7225/toms.v06.n02.002.

Sudnoplavna haluz vyiavylasia bezzakhysnoiu pered kiberzlochyntsiamy, 2023. Available at: https://logist.fm/news/sudnoplavna-galuz-viyavilasya-bezzahisnoyu-pered-kiberzlochincyami

Surinov, I. and Shumilov, D., 2023. Cybersecurity of the Processes of Manoeuvring in Confined Waters. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 17(3), pp. 723-732. Available at: http://dx.doi.org/10.12716/1001.17.03.25.

Tam, K., et. al., 2019. Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities. International Conference on Marine Engineering and Technology Oman 2019 (ICMET Oman), Muscat, Oman. Available at: https://doi.org/10.24868/icmet.oman.2019.005.

TOP-10 naibilshykh khakerskykh atak, 2023. Available at: https://ilounge.ua/ua/review/top-10-bolshih-hakerskih-atak

U.S. Coast Guard Warns Shipping Industry on Cybersecurity, 2019. Available at: https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402

Vilskiy, G. B., 2014. Informatsionnaya bezopasnost sudovozhdeniya: monografiya, Mykolaiv: Vydavnytstvo FOP Shvets V. D., p. 336

Vil's'kyy, H. B., 2012. Klasteryzatsiya morskykh povidomlen, Kherson: Nauk. Visnyk KHDMA, 1(6), pp. 472-474.

Vujović, I., Čoko, M., and Kuzmanić, I., 2020. Reliability and Availability of Ship's Computer Systems Based on Manufacturer's Data and Worksheets. Naše more, 67, pp. 25-31. Available at: http://doi.org/10.17818/NM/2020/3.11.

Weaver, G. A. et al., 2022. Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. Transportation Research Part C: Emerging Technologies, 137. Available at: https://doi.org/10.1016/j.trc.2021.103423.