Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System

Oleksiy Melnyk[1]†, Svitlana Onyshchenko[2]††, Nataliia Pavlova[3]†††,
Oleksandra Kravchenko[4]††, Svitlana Borovyk[5]††
m.onmu@ukr.net
† Navigation and Maritime Safety Department, Odesa National Maritime University, Ukraine
†† Fleet Operation and Shipping Technology Department, Odesa National Maritime University, Ukraine
††† Port Operation and Cargo Handling Technology Department, Odesa National Maritime University, Ukraine

Summary

Scientific and technological progress is also fundamental to the evolving merchant shipping industry, both in terms of the size and speed of modern ships and in the level of their technical capabilities. While the freight performance of ships is growing, the number of crew on board is steadily decreasing, as more work processes are being automated through the implementation of information technologies, including ship management systems. Although there have been repeated appeals from international maritime organizations to focus on building effective maritime security defenses against cyber attacks, the problems have remained unresolved. Owners of shipping companies do not disclose information about cyberattack attempts or incidents against them due to fear of commercial losses or consequences, such as loss of image, customer and insurance claims, and investigations by independent international organizations and government agencies. Issues of cybersecurity of control systems in the world today have gained importance, due to the fact that existing threats concern not only the security of technical means and devices, but also issues of environmental safety and safety of life at sea. The article examines the implementation of cyber risk management in the shipping industry, providing recommendations for the safe ship operation and its systems in order to improve vulnerability to external threats related to cyberattacks, and to ensure the safety and security of such a technical object as a seagoing ship.

Keywords:
Cyberattacks prevention, cybersecurity of ships, cyber risks, shipping industry.

1. Introduction

Transport safety is a high priority; it is of particular importance in the sphere of merchant shipping as well. Shipping is the industry, which is directly affected by risks of various nature. Risks caused by significant variability of trends and conditions of freight market complexity of technical and technological systems of the vessel as a technical object, form the risks of technical nature. The combination of environmental factors, natural and climatic risks during the operation of the vessel form the risks of the external environment. In addition, finally, cyber risks, which, undoubtedly, are directly related to the level of shipping safety, have recently aggravated, affecting the safety of ship operation. Thus analysis of global fleet accidents, including cyber-attack statistics [1, 3, 4]. In [3, 7-9, 21] works to develop methods to ensure the safe operation of ships, modern methodology of estimation of ship's safety level and ways of its improvement as well as assessment of potentially negative influence of a system of factors on a vessel's operational condition in transportation of oversized and heavy cargo are considered. Nature and origin of major security concerns and potential threats to the shipping industry, seaports security and maritime security aspects studied [10, 14, 17, 20]. Conceptual model of information security and measures to protect an organization's networks and systems [5, 6, 13]. Risk management framework and investment cost analysis and maritime cyber risk management including experimental ship assessment devoted works [11, 12]. Practice of cyber security management on cargo ships and international maritime codes and conventions studied in [15, 16, 19]. Thus, the purpose of this study is to examine current threats to international shipping and analyze the components of cyber risk, identify potential hazards and risks arising during the operation of ships, compare and establish patterns of their occurrence, and develop measures to ensure cybersecurity and security of ships.

2. Ship safety and security measures overview

With the modern development of water transport and waterways, much attention paid to safety issues. Safety of the ship, port infrastructure and first of all the safety of human life at sea includes a whole complex of safety measures, methods and techniques of its provision. Among the main threats to maritime safety remains the insurmountable accident rate of the world' s fleet. One of the reasons for accidents is incorrect, inaccurate or incomplete information. According to statistics, 2/3 of all accidents in the world fleet are caused by navigational accidents. Of these, 85% occurred at a distance from the shore of 5 miles or more, including 30% in the port limits. However, a similar situation is typical for other modes of

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.18

transport: takeoff and landing of helicopters and airplanes, especially with vertical takeoff, parking of heavy trucks, especially large-sized ones. Proper technical condition of the ship, availability of necessary equipment, insurance agreements, approved routes, as well as familiarization with weather conditions of the planned voyage, minimize risks associated with the process of ship control, and ensure the safety of navigation.

Classification by types of hazards (types of emergencies) based on such ship conditions, which pose a real threat to safety or loss of seaworthiness, and then six main types of hazards can be classified as these conditions, namely:

- Hull damage and integrity impairment due to the effects of external heavy operating loads (excessive wave loads, heavy ice conditions, contact with submerged floating objects);
- capsizing of the vessel or its excessive inclination which does not allow to continue the voyage, caused by incorrect loading, shifting of cargo and damage of its securing equipment, icing;
- ship sinking (loss of buoyancy) due to hull watertightness failure which is not directly connected with the influence of extreme operational loads, at corrosion or similar structural damages;
- loss of propulsion and steering as a result of failure of the main engine or propeller-rudder complex;
- contact with external objects (navigational emergencies): collision, grounding due to force majeure circumstances, navigators' errors, failure of navigation equipment, pilot or traffic control system errors, other vessel or object, incomplete navigation and charting support, including unmarked on the chart shallows and submerged objects;
- fire or explosion in the ship's compartments caused by a short circuit of electrical wiring or ignition of electrical equipment.

Further improvement of the International Convention for the Safety of Life at Sea, 1974. (SOLAS-74), along with new challenges to international maritime safety, led to the development and adoption of a new chapter XI-2 of the Convention (SOLAS-74), and with it the International Ship and Port Facility Security Code (ISPS Code). These documents established and unified the minimum safety standards mandatory for participating countries in international maritime transport of goods and passengers. This was an important step of the world community for the creation of a global maritime safety system. According to this code, the organization classified the main threats to international maritime security as terrorism, piracy, armed attacks, theft of cargo and ship's property, drug and arms smuggling, transportation of illegal migrants and cyber threats. The cybercrime, which is a current threat to ship security, raises the need to consider the practice of training crewmembers to defend against attacks, and to understand how cyber risks arise in order to reduce the likelihood of their occurrence.

As technology expands its horizons, the information security of ships and shipping companies is increasingly at risk. Cyber threats are on the rise and the number of cyberattacks worldwide has multiplied. The widespread implementation of digital transformation initiatives on ships, ports and shipping companies, sometimes at the expense of security aspects, has led to serious security threats that need to be addressed in advance to safeguard against data leakage. Cybercriminals may have different reasons for trying to gain access to company or ship data and systems, ranging from identity theft to undermining the company's reputation.

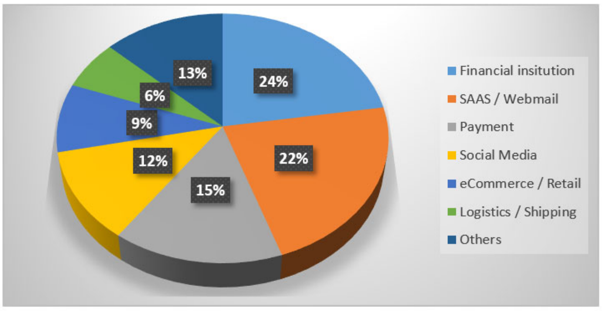

Fig. 1 The most targeted industries for cyberattacks 2020-2021 [APWG's Phishing Activity Trends Report]

According to the Maritime Business Survey, 77% of respondents considered cyberattacks a high or medium risk to their companies, but only 64% said their company has a business continuity plan in place in case of a cyber incident. Only 24% said it is checked every three months and only 15% that is checked every 6-12 months. Only 2 in 5 respondents said their organization protects vessels from operational technology (OT) cyber threats, with some respondents going so far as to call their company's OT cyber risk policy "negligent."

3. Cyber Security Management System on Cargo Ships

International shipping is crucial to world trade. The vast majority of goods for various purposes are transported by sea. With more than 55,000 merchant ships and nearly 4,000 ports, the global maritime transportation system is open and flexible, making it vulnerable to terrorist threats and attacks, and could be used to smuggle weapons, drugs, human trafficking or provide logistical support to terrorist organizations.

The measures to counter threats from cyberattacks are estimated to require ship owners and operators to invest more than a billion dollars, and the annual operating costs will increase even further in the future. Statistics provide information on the global industry sectors most susceptible to cyber espionage. As an example, in 2020, the transportation sector ranked eleventh with 28 cyber espionage incidents (Fig.2).

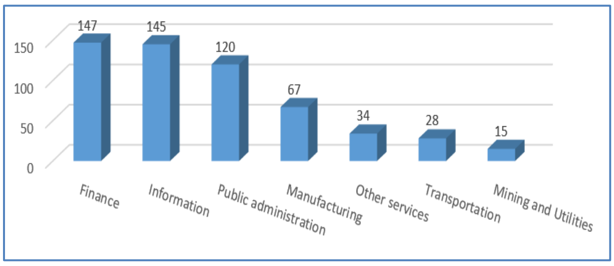

Fig. 2 - Global industry sectors most targeted by cyber espionage in 2020 (Statista)

However, any additional costs are significantly less than the potential cost of even a major terrorist attack, according to maritime security statistics. Moreover, savings from increased efficiency in measures aimed at securing ships can offset some of the additional costs. Implementing the ISPS code and ensuring the safety of ship's crew and port personnel requires resources in the form of qualified personnel, equipment and technology.

A global trend is the progressive digitalization in all industries, and maritime transport is no exception, which is actively developing electronic navigation, automation of ship control processes, communication and security technologies. Increase in automation of modern ships, reduction of the number of crewmembers, widespread use of shipboard software and its updating through open access to the Internet are just a few factors influencing the safe operation of the ship. The International Maritime Organization considers the following ship systems to be vulnerable to cyberattacks as:

- Main engine control systems;
- Systems of cargo handling and control;
- Control systems for energy supply equipment;
- Ship access control systems;
- Crew welfare systems;
- The ship's public Internet networks;
- Administrative systems and networks;
- Communications systems.

Based on this, we can conclude that a modern oceangoing vessel is highly vulnerable to a planned cyberattack. Based on the findings and conclusions of maritime industry analysts and experts, it is necessary to consider the current state of maritime safety in relation to regulations. During the 98th session of the International Maritime Organization (IMO) Committee on Maritime Safety (CMO) approved Circular MSC-FAL.1/Circ.3 "Manual on Cyber Threat Management in the Maritime Industry" and Resolution MSC.428(98) - Cyber Threat Management in the Maritime Industry within Safety Management Systems. This resolution requires increasing crew awareness of current threats and cyber threats in order to ensure both information security and ship security. The circular emphasizes the need for a security management system that meets the requirements of the ISPS code. Encourage Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

Today, digital pirates are most interested in opportunities to take control over ships' communication networks and information systems. Onboard IT (information technology) and OT systems (operating technologies) prone to cyber risks include, first of all, electronic chart display and information system (ECDIS), voyage data recorder (VDR), control systems of cargo operations, power plant and power supply, as well as radio communication and data transfer systems. The real consequence of malware infecting a ship's systems can be a change in ship data, including position, cargo information. As example under the influence of malware, false information about stormy weather conditions can be sent to specific ships forcing them to change course. Hacking into the route data recorder can change current ship parameters, such as speed, data displayed from radar stations (radar) and other navigation equipment. Cybercriminals can delete audio recordings and information from the ship's course control and steering systems, as well as data on the condition of pressurized tanks, bulkheads, doors and hatches.

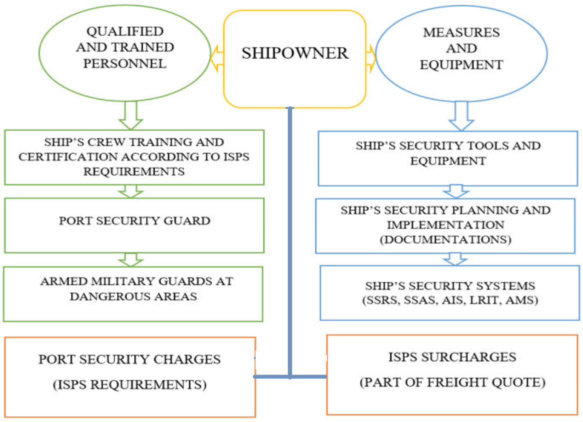
QUALIFIED AND TRAINED PERSONNEL
SHIPOWNER
MEASURES AND EQUIPMENT
SHIP’S CREW TRAINING AND CERTIFICATION ACCORDING TO ISPS REQUIREMENTS
PORT SECURITY GUARD
ARMED MILITARY GUARDS AT DANGEROUS AREAS
SHIP’S SECURITY TOOLS AND EQUIPMENT
SHIP’S SECURITY PLANNING AND IMPLEMENTATION (DOCUMENTATIONS)
SHIP’S SECURITY SYSTEMS (SSRS, SSAS, AIS, LRIT, AMS)
PORT SECURITY CHARGES (ISPS REQUIREMENTS)
ISPS SURCHARGES (PART OF FREIGHT QUOTE)

Fig.3 Techniques and methods provided for ship security

Both ship security and cybersecurity are important because of their potential impact on the crew, ship, environment, company and cargo. Cybersecurity refers to the protection of IT, OT, information and data from unauthorized access, manipulation and breach. Cybersecurity covers risks associated with loss of availability or integrity of security-critical data. A cybersecurity breach can occur as a result of an incident affecting the accessibility and integrity of the OT, such as corruption of map data stored in the Electronic Chart Display and Information. System (ECDIS), failure occurring during maintenance and software updates, loss or manipulation of data from external sensors critical to ship operations - this includes Global Navigation Satellite Systems (GNSS).

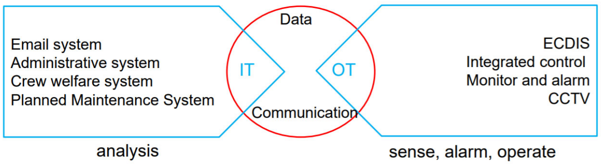

Fig. 4 Information and operation technologies converge [19]

A set of factors simultaneously acts on a vessel in the process of operation, representing risks both for its technical condition, seaworthiness and information security. As an example, it is possible to consider mathematical model of technically justified system of minimization of risks for ship safety, including information security. Based on experts' assessments of probability of realization of threats to ship's safety, the significance of each threat is calculated and the level of organizational measures in natural terms to restore operational capability of the ship in case of its violation is estimated. Further, the total risk of ship workability failure is calculated as sum of risks on each of directions. The result of the solution of the described problem will be distribution of resources of the crew or the shipping company in the allocated areas of activity, which minimizes the risks of failure or impairment of the vessel's performance by the safety criterion.

Let for ship as technical system set dependences of risks Ri of ship operability failure on costs Xi for their prevention (i.e. exclusion, reduction) on i-th safety direction (insufficient safety measures, lack of vigilance, failure of ship information and technical ship systems, failures due to insufficient crew qualification)

$$Ri = F(Xi) \tag{1}$$

Where *i*=1...n, n - the number of the indicated directions of the countermeasures;

Thus, when minimizing the risks for vessel safety we will use such an indicator as the level of costs in material expression for protective programs and algorithms, number of on-duty personnel, composition and number of devices and equipment for renewal of the vessel's operational integrity in case of its failure in one or several directions.

The following values are to be noted:

1) Total risk of system failure:

$$R = \sum_{i=1}^{n} Ri \tag{2}$$

2) Z - the maximum amount of costs for the reduction (elimination) of identified risks;
3) ZMAXi - maximum amount of material costs for implementation of the i-th direction;
4) ZMINi - minimum amount of material costs for implementation of the i-th direction.

Then we can formulate the following mathematical programming task, where each risk must be minimized, and the total cost of their prevention must be less than or equal to the maximum cost of reducing (eliminating) the identified risks. The cost of risk prevention for each aspect must be greater than the minimum amount set for that aspect, but not exceeding the maximum amount for the same aspect.

$$\begin{gathered} \sum_{i=1}^{n} Ri = \sum_{i=1}^{n} F(Xi) \rightarrow min; \\ \sum_{i=1}^{n} Xi \ \leq Z; \\ ZMINi \leq Xi \leq ZMAXi; \\ Xi \geq 0; \end{gathered} \tag{3}$$

This system is economically feasible if the total cost of prevention, reduction or elimination of the accumulated (defined) risks does not exceed or equals the total maximum cost of costs allocated for the reduction (elimination) of imminent risks. Thus, the total volume of resources and means for vessel protection from one threat must not exceed the total volume of all resources and means available for vessel protection. That is why there is a possibility of building a mathematical model for determining the potential hazards, which has the possibility of determining the coefficient of probability of threat realization or occurrence of potential hazards. In another case, the problem of reserving elements of the security system can be considered, which is solved to protect against the violation of confidentiality of the information processed on the ship.

Cyber risk management is the process of identifying, analyzing, assessing and eliminating cybersecurity threats to a ship. To do this, the initial step in a cyber risk management is a cyber risk assessment. This will accurately identify the threats that exist and provide a true picture of the severity of any given threat that could threaten the ship's overall cyber security. In a general sense, the examined components can be represented as a conceptual model of ship security, shown on the following sketch (Fig. 1).

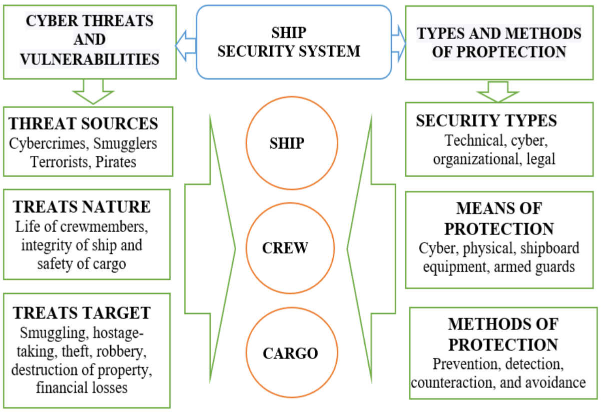
CYBER THREATS AND VULNERABILITIES
SHIP SECURITY SYSTEM
TYPES AND METHODS OF PROPTECTION
THREAT SOURCES
Cybercrimes, Smugglers Terrorists, Pirates
TREATS NATURE
Life of crewmembers, integrity of ship and safety of cargo
TREATS TARGET
Smuggling, hostage-taking, theft, robbery, destruction of property, financial losses
SHIP
CREW
CARGO
SECURITY TYPES
Technical, cyber, organizational, legal
MEANS OF PROTECTION
Cyber, physical, shipboard equipment, armed guards
METHODS OF PROTECTION
Prevention, detection, counteraction, and avoidance

Fig. 5 Conceptual model of ship security

The ship's cyber security concept can be roughly divided into two levels: upper and lower. A recognized person - the shipowner's representative, who is directly responsible for the safety of the company's own fleet, heads the upper level. This may be the company manager, fleet manager, or a security officer who is directly responsible to him. The top-level program includes strategic decisions on ship safety, so the program should have the following main objectives:

- Strategic planning of security measures;
- Development and implementation of a policy in the field of security of the own fleet;
- Risk assessment and risk management;
- Coordination of activities in the field of fleet safety;
- Monitoring of activities on board.

The main goal or concept of the lower-level program is to ensure reliable and economically feasible protection of the ship. At this level, decisions to be done on the following issues: which arrangements, means and methods of protection are to be used, which technical equipment is to be installed, whether comprehensive management is carried out, whether the safety system as a whole is monitored and weak points are identified, whether systematic training of the crew is provided, etc. The lower level program is the responsibility of Master, ship security officers, and head of departments. The most important activity at this level is the evaluation of criticality and effectiveness of measures.

Therefore, when building a model of ship security, it is necessary to take into account that the use of the most modern methods and means of protection should be achieved by measures aimed primarily at the protection of human life, which must be a priority in relation to the vessel.

4. Conclusion

The rate of growth of global trade and the intensity of international shipping are largely responsible for the growth of accidents in the global fleet. However, in parallel, there are threats to maritime safety associated with unauthorized access and manipulation of vessel information and data, which pose a danger not only to the crew and vessel, but also to the environment, the shipowners company and the cargo. The article considers the main directions of application of technologies, processes and controls to protect the ship its systems, programs, devices and data from cyberattacks that pose a potential threat to information security and offers a set of measures to ensure the safety of ships. All above-mentioned factors prove the fact that impossibility of information security problem solving by traditional methods, such as systems control by ship crew only, is the reason for creation and implementation of new and more effective information security systems, which is extremely urgent and one of the priority tasks.
From the foregoing, the conclusion can be drawn that a modern seagoing ship is extremely vulnerable to a planned cyberattack. Ports also need protection from cyber threats, so the international maritime organization recommends that cyber risk management should be a natural extension of existing maritime safety and security management practices. The cyber security is also considered as a part of maritime security, and this is reflected in a number of recommendations developed by leading international maritime communities. However, there is no single approved approach to describing specific cyber threats and assessing them, forcing each shipping company to determine independently the level of possible threats and the ways to prevent them.

References

[1] Safety and navigation review. Allianz Global Corporate & Specialty SE. Available at: https://www.iims.org.uk/wp-content/uploads/2020/07/AGCS-Safety-Shipping-Review-2020.pdf. (Accessed 10.02.2022)

[2] Korovin, A.: *Ensuring safe operation of the tanker fleet in the continental shelf areas of the Arctic seas.* Bulletin of the Kamchatka State Technical University (6), 54-56 (2007)

[3] European Maritime Safety Agency (EMSA). Preliminary annual review of maritime casualties and incidents for 2014-2020. Retrieved from http://www.emsa.europa.eu/publications.html. (Accessed 10.02.2022)

[4] Safety at sea. Retrieved from https://safety4sea.com/23073-maritime-casualties-and-incidents-reported-in-2019 (2019)

[5] Yarochkin, V.: *Information security*: Textbook for university students. - Moscow: Academic Project, 2nd ed.-2004. 544 p. Gaudeamus (2004)

[6] Conceptual model of information security. Avaiable at: https://sivcomsks.com/kontseptualnaya-model-informatsionnoy-bezopasnosti/ (Accessed 10.02.2022)

[7] Melnyk, O., Bychkovsky, Yu.: *Modern Methodology of Estimation of Ship's Safety Level and Ways of its Improvement*. Transport Development 2 (9), (2021)

[8] Onyshchenko, S., Melnyk, O.: *Modelling of changes in vessel operational condition during transportation of oversized and heavy cargoes.* Technological audit and production reserves, 6/2 (56), 66-70 (2020)

[9] Onyshchenko, S., Shibaev, O., Melnyk, O.: *Assessment of potentially negative influence of a system of factors on a vessel's operational condition in transportation of oversized and heavy cargo*. Transactions on Maritime Science 10(1), 126-134 (2021)

[10] Melnyk, O., Onyshchenko, S., Koryakin, K.: *Nature and origin of major security concerns and potential threats to the shipping industry*. Scientific Journal of Silesian University of Technology. Series Transport 113, 145-153 (2021)

[11] Lee, In.: *Cybersecurity: Risk management framework and investment cost analysis*. Business Horizons 64(5), 659-671 (2021)

[12] Svilicic, B., Kamahara, J., Rooks, M., Yano, Y.: *Maritime Cyber Risk Management: An Experimental Ship Assessment*. Journal of Navigation, 72(5), 1108-1120 (2019)

[13] Creech, J., Ryan, J.: *AIS The Cornerstone of National Security?* Journal of Navigation 56(1), 31-44 (2003)

[14] Seaport security: how to choose the right technology? Worldvision. Available at:https://worldvision.com.ua/ru/articles/obespechenie-bezopasnosti-v-morskih-portah-kak-vibrat-pravilnuyu-tehnologiyu. (Accessed 20.11.21)

[15] INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA - 1974. (SOLAS74) Available at:https://docs.cntd.ru/document/901765675. (Accessed on 15.11.21)

[16] INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE. [Electronic source] Available at https://ips.ligazakon.net/document/MU02257. (Accessed 15.11.21)

[17] Büger, K.: *What is maritime security?* Maritime Policy 53, 159-164 (2015)

[18] Kavallieratos G, Katsikas S.: *Managing Cyber Security Risks of the Cyber-Enabled Ship*. Journal of Marine Science and Engineering 8(10), 768 (2020)

[19] Practice of Cyber Security Management System on Cargo Ship. China Classification Society, IMO: Guidelines On Maritime Cyber Risk Management (MSC-FAL.1-Circ.3) (2018)

[20] Melnyk, O., Bychkovsky, Y., Voloshyn, A.: *Maritime situational awareness as a key measure for safe ship operation*. Scientific Journal of Silesian University of Technology. Series Transport 114, 91-101 (2022)

[21] Burmaka, I., Vorokhobin I., Melnyk, O., Burmaka, O., Sagin, S.: *Method of Prompt Evasive Maneuver Selection to alter Ship's Course or Speed*. Transactions on Maritime Science 11(1), (2022)