TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 16
Number 4
December 2022
DOI: 10.12716/1001.16.04.13

Review of Ship Information Security Risks and Safety of Maritime Transportation Issues

O. Melnyk[1], S. Onyshchenko[1], O. Onishchenko[2], O. Shumylo[1], A. Voloshyn[1], Y. Koskina[1] & Y. Volianska[3]
[1] *Odesa National Maritime University, Odesa, Ukraine*
[2] *National University "Odesa Maritime Academy", Odesa, Ukraine*
[3] *Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine*

ABSTRACT: In recent years, various types of commerce including transport have suffered significant damage and costs due to cyber-attacks. The geographic scope of freight transportation has no boundaries, attacks can be launched almost anywhere there is an Internet connection. Therefore, there is no immunity from the failure of computer systems and information of delivery processes in the networks of organizations and companies engaged in maritime transportation. In addition, while the consequences of cyber-attacks on major shipping lines and ports, as well as the digital systems of logistics companies, can be comprehensively analyzed, the vulnerability of ships remains insufficiently studied. This paper offers an analysis of the risks in the field of maritime freight transport and the main factors of influence such as digitization on the safety of the transport process. The basic threats to the information system of the ship are defined and the techniques of risk analysis for the ship information security is proposed.

1 INTRODUCTION

For centuries, the shipping of goods by sea has remained the main type of trade relations with the dominant volume of international shipments [1]. Given the global trend toward the progress of digitization of the economy, water transport has not become an exception. Consequently, automation of processes on board of a modern vessel has become a reality, which leads to increase in size of vessels and, as a result, to decrease in the number of crew. Shipboard systems are being upgraded while underway and all business correspondence and crew communication with the shore is effected via Internet. According to a number of experts, extremely low attention is paid to the questions of information security of maritime and inland transport infrastructure objects, seagoing and river ships [2-4]. This is confirmed by the current situation on merchant ships as well as those services [5], products and solutions that have not yet found their application on water transport, where the issues of information security are almost exclusively focused on the restriction of access through passwords and logins or the use of network screens [6,7].

Ensuring cyber resilience of shipboard information systems is becoming more and more important every year [8,9]. Leading shipping organizations, launched a set of cyber security guidelines for ships to help the global shipping industry prevent major safety, environmental and commercial issues that could result from a cyber incident onboard a vessel [10,11]. Thus, cybersecurity awareness issues in maritime transport and cybersecurity trends in information technology studied in [12-15]. Analysis of techniques and attacking pattern in cyber security approach in [16]. Global outlook and managing of cyber security issues studied in [17,18]. Cybersecurity problems in different types of transport of aviation, maritime and automotive industry and their essence, enhancement of cyber

security for cyber physical systems [19,20]. General issues on information security in logistics and transport highlighted in [21-23]. Matters relating to the safe operation of ships and the fundamentals of maritime safety researched in [23-26]. Problems of improving the efficiency of port operation and port facility management have been studied in [27,28]. Development of economic-mathematical model of ship loading and justification of sustainability ranges of commercially expedient ship operation in [29,30,31]. Additional issues of ship operation arrangements and improvement of fleet performance in [32,33].

Given the theoretical basis studied, it should be noted that effective counteraction to risks remains in the plane of creating levels of cyber resistance of the ship, corresponding to high standards and following a risk-oriented approach in the development of security tools, where the development of methods for assessing cyber threats is marked by relevance and practical interest.

2 MATERIALS AND METHODS

2.1 *2.1 Analyses of risks in freight transportation*

The maritime trade is transformed by the digitalization of transport and logistics. Online tonnage chartering platforms are already being introduced due to the understandable fact of saving operational costs and the desire of shipowners to avoid additional costs in the form of brokerage fees. Despite the fact that shipping is a very conservative business, online processes are not just a trend but also a reality of our time. As an example transition to the non-paper bill of lading leads to potential saving of $4 billion per year and if 50% of container industry transitions that way the annual growth rate will be 2.4% by 2030. In addition, the situation with Covid-19 has highlighted the advantages of electronic bills of lading in a very positive way. Shipments have not been stuck in ports because papers were stuck somewhere due to pandemic flight restrictions. It is also noted that eliminating paper in shipping will make every aspect of maritime transportation better, faster, cheaper, more reliable and greener. In addition, the rise of blockchain technology avoids the risks of data loss or hacking attacks on the electronic bill of lading journey from sender to receiver. Most recently, MSC launched an online quote service for shippers called Instant Quote, which simplifies and speeds up the booing process. The company's customers have direct access to shipping rates, which simplifies the supply chain management process. In addition, Maersk has announced an increase in the use of its mobile tracking application that allowed customers to place and track orders remotely during the pandemic. The company was a pioneer along the way, then joined by Hapag-Lloyd, Evergreen Line, ZIM and MSC. Ship's documents, navigation charts and other information are already in digital form and moreover the appearance of underwater drones capable of sailing in front of the ship and transmitting information about the fairway, depths and bounds to the bridge point to the quite logical transition to unmanned pilotage and autonomous ships, which are already being actively implemented, but at the same time all the above is steadily putting pressure on the safety of all processes of ship operation without exception and primarily on safety of cargo transportation.

It is worth noting that transportation of goods by various modes of transport, both domestic and international, is constantly associated with a multitude of risks, the potential damage of which can be calculated in significant monetary terms. In case of maritime transportation there are a lot of risks, such as cargo deterioration, loss, and damage during cargo handling operations as well as risks for the ship in case of fire, capsize, accident, grounding and flooding, severe weather conditions - the list of main risks of marine transportation is far from being complete. To this entire are added modern threats in the form of cyber risks, which universally begin to exert pressure on safety of a vessel and cargo. Therefore, in order to prevent these risks and avoid unforeseen costs both shipowners and charterers need to understand them and know the most common factors along with measures to prevent them.

Among other things, weather conditions, the type of cargo transported the nature of the route and other parameters affect the reliability of shipping. In practice, the most common risks are as follows:

- Cargo damage;
- Cargo loss;
- Delays in shipping terms;

Most common types of cargo claims according to P&I club shown in Figure 1;

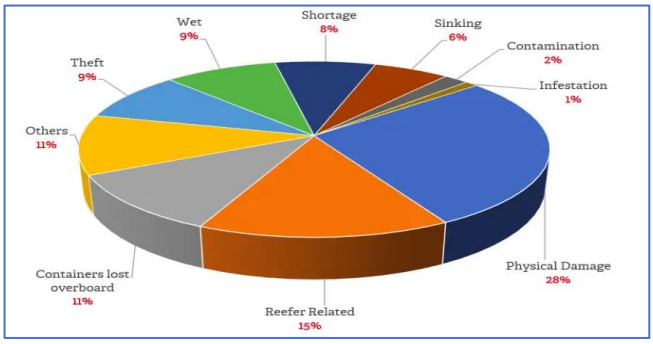

Figure 1. Most common types of cargo claims (containers) Source P&I club

Loss of cargo, including theft, according to statistics of insurance organizations, is the cause of more than a third of all insurance payments. Various kinds of accidents during transportation, which cause damage to the cargo, take the second place, and they account for more than 15% of all indemnities, according to insurance companies. Delayed delivery also causes significant economic losses, both in terms of production disruptions and contractual penalties. In addition to these factors, also notable that the spoilage of goods due to violation of temperature conditions, accidents during loading and unloading and failure to comply with the mode of transportation. All these risks have a negative impact both on cooperation in the field of maritime shipping and on the reputation of the carrier's company as a whole. Now more than ever it is important to know and understand the threats of cyber risks.

2.2 *Overview of cybercrimes in the shipping industry*

Digitalization has spread widely among companies in the maritime transport and logistics sector, improving the entire process cycle in the industry. This has contributed to an unprecedented increase in transport efficiency, which has served to expand revenue channels. However, digitalization has also exposed a number of problems in shipping and maritime logistics companies, making them extremely vulnerable to cyberattacks. This affects every sector of the transportation industry, including shipping, rail, trucking, logistics and delivery. The consequences of such cyber-attacks are costly, disruptive and can lead to financial liability, especially if confidential information is allowed to leak. There are many vulnerabilities for the transportation and logistics industry. These include the increased use of operating technology (OT), new communication and wireless channels directly connected to companies' digital ecosystems, again making companies an easy target for hackers. It is also outdated information technology (IT) regulations and standards, lack of cybersecurity awareness and, last but not least, the shortage of qualified personnel capable of providing professional protection. Ship information exchange cycle presented in Figure 2.

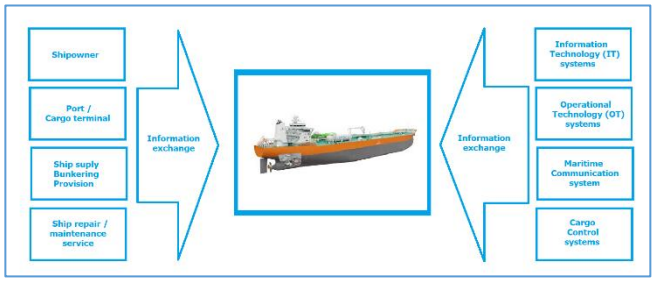

Figure 2. Ship information exchange cycle

It is notable that the frequency of cyberattacks targeting the shipping sector is increasing on average, from once every few years earlier to almost every month today. In addition, while several of them are quite extensive and amount to millions of dollars, other cyberattacks targeted major transportation companies to disrupt email systems and logistics processes. Moreover, hackers are increasingly trying to hack into data stored on networks that carry not only cargo information, but also innovations and updates to company information security, which directly affects efficient and quality customer service. Digital enhancements such as automated orders, shipment tracking and access to billing information make this possible. While such benefits are extremely valuable to the customer, they require the storage of large amounts of sensitive data collected through online platforms, phone apps and other mobile devices, which are some of the most unreliable channels due to the lack of strict cybersecurity protocols [23]. The main ship systems that are most vulnerable to external attacks can be grouped into four groups as shown in the Figure 3;

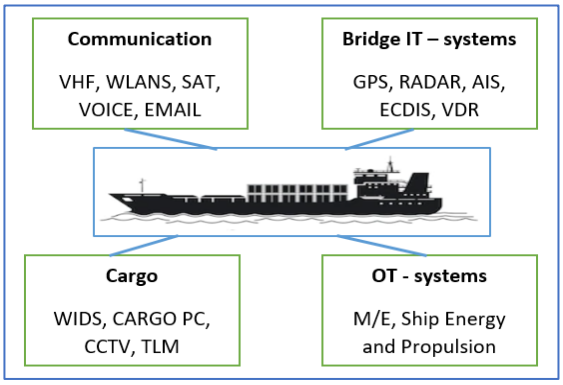

Figure 3. Key systems vulnerable to cyberattacks

Cyber-attacks on seagoing ships dramatically increased only in the first few months since the pandemic breakout. From a cybersecurity perspective, 2021 was not a good year for the maritime and logistics industry. The frequency of attacks on ships increased by 33% - and that is after a huge increase in attacks on ships and port systems in 2020. The increase in the number of attacks probably reflects, in part, the record increase in cybersecurity incidents of all types over the past year. However, it is also likely that attackers have chosen to focus on the maritime industry, given its critical role in securing the global supply chain. In the scenario of hackers taking control of a ship, that is carrying something truly vital, like food, water, or medicine. They could such as stopping the ship for as long as they want, and the shipowners can do nothing but give them whatever they ask for. The above would lead to significant delays, the economic damage of millions of dollars as well as a political and social crisis.

According to information security experts, different types of malware are behind these cyberattacks. They infiltrate a computer or network; it locks computers, preventing personnel from using them, and demands payment to unlock the machines. The payment can be made in cryptocurrency, such as bitcoins. Even, sometimes computers are not unlocked after payment. Experts and governments have made numerous accusations against attackers, from accusations against individual hackers and organized crime, to accusations against some governments. The attacks were not primarily directed at the cargo facilities, but at the business infrastructure, that supports this core business of moving cargo around the world. According to statistics, the total value of damage from cybercrime in 2021 was the most significant compared to previous years, Figure 4.

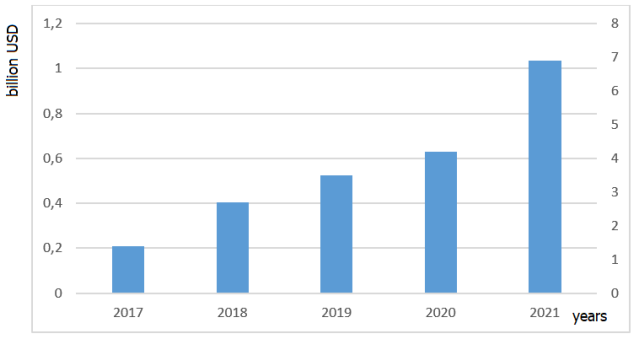

Figure 4. Total cost of cybercrime
(Source FBI internet crime report – 2021)

The processes of digitalization are increasingly taking a prominent place in the management of systems and instruments of various types of ships. Today, such sophisticated engineering structures, necessary in today's global economy, can be halted by a new generation of computer users, and the merchant ship, like any digital system, can be hacked. There is an opinion that it is often easier to hack into the websites of logistics and shipping companies that operate in ports than to gain access to the ship's systems. According to SMM Maritime Industry Report 2021, 84% of ship owners and operators are already aware of the threat and consider cybersecurity important or very important, given that the global supply chain has become a favorite target for cybercriminals, as evidenced by recent attacks on numerous shipping companies and vessels. According to a maritime cyber risk-consulting firm, an average of one new incident per day. While it is encouraging that the shipping industry is becoming more aware of the problem, it looks like there is more work to be done. According to hackers themselves, ships are often wide open to cyber-attacks. Increasingly more processes on board ship are elements of an automated control system, which in turn can be divided into systems that carry out the navigation and motion control process, the working process of ship operations and the cargo handling process, including cargo stowage, storage and carriage, Figure 5.

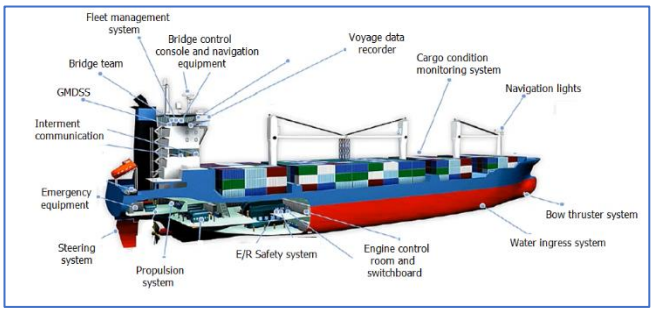

Figure 5. Systems of automatic control and monitoring of processes on board ship

All these processes are implemented by means of technical systems consisting of many structural elements, units, mechanisms, aggregates, i.e. a complex of technical facilities, which serve for automatic control, and monitoring of the vessel processes. This includes all measuring and control devices, including shipboard computers for control or monitoring of processes, which can inevitably serve as a target for cyberattacks and consequently paralyze the operation of each of the systems presented.

3 RESULTS AND DISCUSSION

Cybersecurity in maritime transport, especially in relation to moving objects such as ships, is crucial since it has a potential impact on personnel, ship, environment, company and cargo and is primarily aimed at protecting information and data from unauthorized access, manipulation and breach. The reasons for which cyber incidents can occur are as follows: cybersecurity incident, unintentional system failure, loss or manipulation of external device data, system failure due to software failures or crew influence leading to the infiltration of malware into ship systems [10].

Information security risk in the classical form is defined as a function of three variable components, including:

- probability of existence of a threat to the ship's information security;
- probability of system vulnerability (level of insecurity);
- potential impact of external factors.

If any of these variables tends to zero, then the total risk for the ship's information systems tends to zero. The main categories of factors of destabilization of normal operation of ship information systems include:

- Physical damage to the technical (technological, navigational) systems of the vessel as a result of cybersecurity breach caused by intentional or accidental physical impact on the system or its components (fire, water, electrostatics, environmental impact, theft, loss, inept handling of equipment or data storage medium);
- Violation of safety due to failure of basic system components and functions that support the functioning of the systems (for example, failure of the power supply network, main engine speed control system, direction finding, positioning, etc;);
- Violation of safety due to disturbances caused by, for example, electromagnetic radiation, voltage fluctuations, electronic interference;
- Technical failure or violations caused by system failures or related non-technical capabilities (hardware or software failure, overload, unrepairable);
- Technical attacks. Security breach caused by attacks and exploitation of its vulnerabilities in configuration, protocols, programs, etc. (network scanning, login attempt, interference, denial of service).

Thus, the information exchange process of the voyage details, cargo and ports of call remains largely unprotected, which opens the door to manipulation and unauthorized access shown in Figure 6.

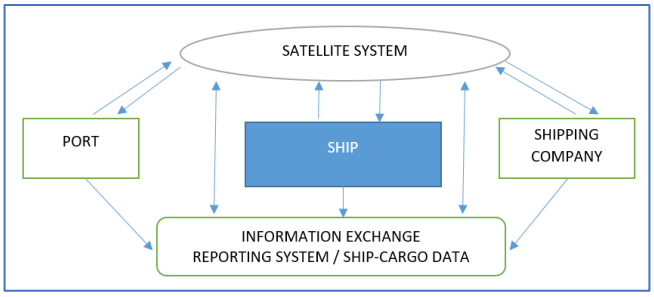

Figure 6. Scheme of ship information exchange process

According to [2], which developed jointly by the International Organization for Standardization and the International Electrotechnical Commission, the proposed security assessment technique should ensure that risk assessments produce comparable and reproducible results. At the same time, the standard does not contain a specific formula for calculating the risk assessment. However, according to [3] the following classic formula for calculating risk is given:

$$R = P(t) \cdot S \quad (1)$$

where R is the risk value; $P(t)$ - probability of realization of the threat to the information security of the vessel (a mixture of qualitative and quantitative scales is used); S - degree of threat impact on a particular system (system cost in qualitative and quantitative scale).

As a result, it becomes possible to determine the value of risk in relative system, which in turn can be ranked according to the degree of importance for the risk management procedure for the information security of the ship.

According to security management techniques for information technology, risk calculation occurs according to the following formula:

$$R = P(t) \cdot P(v) \cdot S \quad (2)$$

where $P(t)$ - probability of a threat to the information security of the ship; $P(v)$ - the probability of a system security vulnerability; S - value of the system (the amount of damage) in USD.

As an example of the values of threat probabilities $P(t)$ and $P(v)$, a qualitative scale with three levels (low, medium and high). Numerical values in the range from 0 to 4 are presented to estimate the value of the system S. The shipping company in which the information security risk assessment is carried out must compare their qualitative values. According to [7], the risk level is calculated taking into account the following indicators: resource value, level of threat and degree of vulnerability. As the values of these parameters increase, the risk increases. Thus, the formula can be presented in the following form:

$$R = S \cdot L(t) \cdot L(v) \quad (3)$$

where S - the value of the system (the amount of damage); $L(t)$ - level of threat; $L(v)$ - level (degree of vulnerability).

In practice, the technology for determining risks to the information security of the ship takes place on the table positioning values of the threat level, the degree of probability of exploitation of the vulnerability, and the value of the asset. The risk value can vary from 0 to 8, resulting in a list of threats with different risk values for each asset. The standard proposes the following risk ranking scale: low (0-2), medium (3-5) and high (6-8). This allows identifying the most critical risks [4].

In common techniques for the assessment of information security risks, the assessment of the degree of possibility of information security threat realization the threat level is assessed by the following qualitative and quantitative scale: unrealizable - 0%, medium threat - 40%, means average - from 21% to 50%, etc. Determining the severity of consequences for different types of information system is proposed to be assessed using a qualitative-quantitative scale, i.e. minimum - 0.5% of component value, high – from 1.5% to 3%.

To make a qualitative assessment of information security risks, a table of correspondence between the severity of consequences and the probability of threat implementation is used. If it is necessary to make a quantitative assessment for cargo system as example, the formula can be presented in the following form:

$$R = P(v) \cdot S \quad (4)$$

where S - the value of the loss (the degree of severity of the consequences).

Having considered all the above methods of risk assessment in terms of calculating the value of information security risk, it is worth noting that the calculation of risk is performed using the value of threats and cargo value. A significant disadvantage is the assessment of the value of cargo (the amount of damage, damage, delay) in the form of conditional values. Conditional values have no units of measurement applicable in practice; in particular, they are not a monetary equivalent. As a result, it does not give a real representation of the level of risk, which can be transferred to the particular ship system. Thus, it is proposed to divide the risk calculation procedure into the following stages:

- Calculation of the value of technical risk;
- Calculation of potential damage.

Under the technical risk is understood the value of information security risk, consisting of probabilities of realization of threats and use of vulnerabilities of each component of ship information structure taking into account the level of their confidentiality, integrity and availability. For the first step, the following formulas can be given:

$$\begin{aligned} R_c &= I_c \cdot P(T) \cdot P(V) \\ R_i &= I_i \cdot P(T) \cdot P(V) \\ R_a &= I_a \cdot P(T) \cdot P(V) \end{aligned} \quad (5)$$

where R_c - confidentiality risk value; I_c - information system confidentiality factor; $P(T)$ - threat realization probability; $P(V)$ - vulnerability usage probability; R_i - integrity risk value; I_i - information system integrity factor; R_a - availability risk value; I_a - information system availability factor.

The application of this algorithm will allow making a more detailed assessment of risk, to obtain as a result a dimensionless value of the probability of damage risk for each type of ship systems separately. Subsequently, it is possible to calculate the value of damage. For this purpose the average risk value of each type of ship's system and the damage of potential losses are used. The value of damage (D) is calculated by the following formula:

$$D = R_{av} \cdot S \quad (6)$$

where R_{av} - the average value of risk; S - losses, USD.

Thus, the proposed technique enables to correctly assess the value of information security risk and calculate monetary losses in case of incidents that threaten the safety of cargo transportation process.

4 CONCLUSION

For many maritime companies, a premeditated cybersecurity policy for both their own fleet and the entire shipping process has so far not been a priority. However, the rapidly growing number of cyberattacks and emerging regulatory tools have made them realize

that they cannot continue to remain relatively indifferent for long. Attacks are becoming more active, and they are a consequence of the fact that hackers get enough information about cargo and routes to know which companies pay insufficient attention to cybersecurity. Therefore, in order to effectively counteract the risks to ships and shipping companies, it is necessary to build a multi-layered cyber resilience system that meets high standards to protect the supply chain including the ship in the process of maritime transportation and to follow a risk-oriented approach in the development of security tools. There is also a need to develop tools to allow the shipowners to evolve in this direction and take appropriate cyber resilience measures covering several dimensions - technology, regulation, processes and personnel including ship crew.

REFERENCES

[1] S. Reidy, "The basics that everyone must know about cargo damage", Arviem (2020). Available at: https://arviem.com/the-basics-that-everyone-must-know-about-cargo-damage.

[2] Information technology. Methods of ensuring security. Information security management systems. Requirements ISO/IEC 27001, Standartinform (2006), 54 p.

[3] Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology, NIST 800-30 (2002), 56 p.

[4] E. Legchekova & O. Titov, "The method of information security risk calculation. Gomel", BTEU (2017).

[5] O. Melnyk, S. Onyshchenko, O. Onishchenko, O. Lohinov & V. Ocheretna, "Integral approach to vulnerability assessment of ship's critical equipment and systems", Transactions on Maritime Science (2023), 12(1).

[6] ISO/IEC 27035, Information technology, Security techniques, Information security incident management, (2011) 78 p.

[7] Information security standard BS ISO/IEC 27001:2005 (BS 7799-2:2005) Information security management.

[8] O. Onishchenko, K. Shumilova, S. Volyanskyy, Y. Volyanskaya & Y. Volianskyi, "Ensuring Cyber Resilience of Ship Information Systems", TransNav, (2022) 16 (1), pp. 43 - 50.

[9] Common cyber-security vulnerabilities in ships, Hatteland technology. Available at: https://www.hattelandtechnology.com/blog/cyber-security-vulnerabilities-on-board-ships.

[10] The Guidelines on Cyber Security Onboard Ships (BIMCO). The Guidelines on Cyber Security onboard Ships, Version 4.

[11] Keeping cargo moving: Maritime Cybersecurity, Security Practitioner Insights. Webinar series (2016).

[12] Y.C. Lee, S.K. Park, W.K. Lee, & J. Kang, "Improving cyber security awareness in maritime transport: A way forward", Journal of the Korean Society of Marine Engineering (2017), 41. pp. 738-745.

[13] P.S. Seemma & Sundaresan, Nandhini & M, Sowmiya, "Overview of Cyber Security", IJARCCE (2018), 7, pp. 125-128.

[14] G. Srikanth & S. Kandukuri, "CyberSecurity Trends in Information Technology and Emerging Future Threats", Conference: Recent Trends in Computer Science and Information Technology", (ICRCSIT–2020).

[15] V. Filinovych, & Z. Hu, "Aviation and the Cybersecurity Threats", Conference: International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021).

[16] A. Sharma, A. Tyagi, & M. Bhardwaj, "Analysis of techniques and attacking pattern in cyber security approach: A survey", International journal of health sciences (2022), pp. 13779-13798.

[17] U. Singh & P. Singh, "Managing Cyber Security. Journal of Management and Service Science", (JMSS), (2022), 2. pp. 1-10.

[18] T. Lamba & S. Kandwal, "Global Outlook of Cyber Security", Third International Conference on Information Management and Machine Intelligence (2022), pp. 269-276.

[19] M. Lehto, "Cyber Security in Aviation, Maritime and Automotive", In book: Computation and Big Data for Transport (2022).

[20] R. Bolz, M. Rumez, F. Sommer, J. Dürrwang & R. Kriesten, "Enhancement of Cyber Security for Cyber Physical Systems in the Automotive Field Through Attack Analysis", In book: embedded world Conference 2020 Proceedings.

[21] Information Security in Logistics and Transportation, Tadviser (2020). Available at https://www.tadviser.ru/a/619857.

[22] Visualization of the maritime transportation market. Interlegal. Available at: https://interlegal.com.ua/ru/publikacii/virtualizaciya_rynka_morskih_perevozok/.

[23] S. Chan, E. Yehuda, R. Schaefer, A. Schneuwly, S. Zicherman, S. Deutscher, & O. Klier, "Navigating Rising Cyber Risks in Transportation and Logistics", Boston Consulting Group (2021).

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

[25] S. Onyshchenko & O. Melnyk, "Probabilistic Assessment Method of Hydrometeorological Conditions and their Impact on the Efficiency of Ship Operation", Journal of Engineering Science and Technology Review (2021), 14 (6), pp. 132 – 136.

[26] I. Burmaka, I. Vorokhobin, O. Melnyk, O. Burmaka & S. Sagin, "Method of Prompt Evasive Manuever Selection to Alter Ship's Course or Speed", Transactions on Maritime Science (2022), 11 (1), pp. 1 – 9.

[27] N. Malaksiano, "On the stability of economic indicators of complex port equipment usage", Actual Problems of Economics (2012), 138(12), pp. 226–233.

[28] I. Lapkina, M. Malaksiano & M. Malaksiano, "Optimization of the structure of sea port equipment fleet under unbalanced load", Actual Problems of Economics (2016), 183(9), pp. 364–371.

[29] A. Weintrit, T. Neumann, T. Safety of marine transport introduction. Safety of marine transport: Marine navigation and safety of sea transportation (2015) (pp. 1-4) doi:10.1201/b18515

[30] Y. Kirillova & Y. Meleshenko, "Development of an economic and mathematical model of loading a freight and passenger ferry", Eastern-European Journal of Enterprise Technologies (2016), 3 (4-81), pp. 28 - 37.

[31] E. Kirillova, "Justification of stability ranges of commercially reasonable, allowable loss-making and crisis operation of the vessel", Eastern-European Journal of Enterprise Technologies (2015), 6 (3), pp. 4 – 10.

[32] O. Drozhzhyn, Y. Koskina & I. Tykhonina, "Liner shipping": The evolution of the concept, Pomorstvo (2021), 35 (2), pp. 365 – 371.

[33] O. Drozhzhyn & Y. Koskina, "The model of container feeder line organization focused on the nature and parameters of external container flows", Communications - Scientific Letters of the University of Žilina (2021), 23 (2), pp. A94 - A102.