Integral Approach to Vulnerability Assessment of Ship's Critical Equipment and Systems

Oleksiy Melnyk[a], Svitlana Onyshchenko[a], Oleg Onishchenko[b], Oleh Lohinov[a], Valentyna Ocheretna[a]

The digital transformation of the maritime industry is almost a fait accompli. Merchant ships today use computing and cyber-dependent technologies for navigation, communications, cargo operations, environmental monitoring, and many other purposes. Nowadays, entire industries and businesses are becoming increasingly dependent on data arrays, and the maritime sector is fully experiencing this transformation. A modern commercial ship is unthinkable without digital technology, and the reasons for the deep digitalization of the fleet are numerous. Emergency systems such as safety monitoring, fire detection and alarms are increasingly reliant on cyber technology. Therefore, cybersecurity is a critical component of ship and shipping safety, and cyber-attacks on maritime transport are a very likely problem. These risks will only increase with the further development of information technology. This article proposes approaches to identifying cyber threats as well as a probabilistic assessment of ship cybersecurity, which is based on an integral approach to assessing the vulnerability of shipboard critical equipment and systems. Estimated probabilities of target and non-target cybersecurity breaches of the ship, as well as their overall probability, which allows considering all chains of events leading to a certain consequence associated with potential losses. The model of probability assessment of ship cybersecurity violation and its consequences, which allows evaluation of possible losses as a result of these events, is presented and mathematically described.

KEY WORDS
~ Information technology
~ Operational technology
~ Cyber-attacks
~ Maritime transport
~ Vulnerability assessment
~ Shipboard critical equipment

a. Odesa National Maritime University, Odesa, Ukraine
e-mail: m.onmu@ukr.net
b. National University "Odessa Maritime Academy", Odesa, Ukraine

doi: 10.7225/toms.v12.n01.002

Received on: Jun 25, 2022 / Revised on: Aug 12, 2022 / Accepted on: Dec 11, 2022 / Published: Apr 20, 2022

1. INTRODUCTION

Cyberattack implies any unauthorized action that can be carried out directly on shipboard equipment or e.g., indirectly on the pilot's electronic device and through it on the ship system as a whole. Any link in the system of critical ship equipment including wireless communication channels can become vulnerable. As a result, there is an activation of 'sleeping' and tacitly integrated functions, elements, and installations in the hardware that in turn can lead to various distortions and failures in work at numerous stages of processing, transformation, and representation of the information in various ship's equipment (Progoulakis, Rohmeyer, & Nikitakos, 2021; Lagouvardou, 2018). It is important to note that a ship can be exposed to a hacker attack not only while in port but also in the open sea. Almost all ship equipment (Caprolu et.al., 2020), from navigation and radar systems to electronic charts, can be subjected to cyberattack. A hacker attack can follow the classic scenario of attacking INMARSAT and similar

satellite communications equipment. Attackers only need a narrow bandwidth and a short communication session, during which normally ships en route regularly report to each other e.g., transmission of telemetry information about the parameters of ship movement, its equipment, ports, cargo condition, and details of the route. These phenomena can be countered by analyzing the nature of attacks on ships (Hyra, 2019) and considering the degree of reliability and availability of shipboard computer systems (Vujović et.al., 2020).

Progressing digitalization of maritime transport brings new threats that lie partly in the principles of using modern IT trends in maritime shipping (Shipunov et al., 2020), which could pose a serious threat to the safety of the maritime industry (Kala & Balakrishnan, 2019). Exploring the nature of major security issues and potential threats to the shipping industry is crucial (Alcaide & Llave, 2020; Melnyk et.al., 2021), which causes the emerging risks in the maritime transport system (Malone & Strouboulis, 2021). Cybersecurity challenges in the maritime sector (Akpan et.al., 2022), particularly in maritime transportation (Bielawski & Lazarowska, 2021), indicate the need to improve the efficiency of safety management systems to ensure the safe operation of computer-controlled ship systems (Melnyk et al., 2022). In particular, cybersecurity of critical infrastructure facilities of the maritime sector plays a key role (Mednikarov et.al., 2020). Of particular relevance is cybersecurity at sea and securing digital maritime routes, as well as upcoming legal challenges in this field (Boyes, 2014). Of particular interest are the growing threat of maritime cyberattacks, the level of maritime cybersecurity preparedness (Greiman, 2020) in the seas and straits, and a comparison of practices among countries (Marcus, 2021). The new IACS (International Association of Classification Societies) uniform cybersecurity requirements (UR E26 and UR E27) will become mandatory on January 1, 2024. In particular, DNV is already offering type approvals for the upcoming mandatory requirements.

The ship's cybersecurity system must exclude the possibility of intrusion by alien conversion systems and ensure control of open access ports and anti-virus protection (Nyrkov et al., 2018; Simpanu, 2018). Thus, ensuring the cyber resilience of the ship's information systems (Onishchenko et al., 2022), which in turn requires the use of e.g., firewalls, regular updating of system data, rejection of outdated operating systems, and introduction of new cybersecurity products. Various modeling such as behavior, conceptual (Meshkat et al., 2020; Yusif and & Hafeez-Baig, 2021), and casual modeling were proposed for cybersecurity (Abel et al., 2018) in order to utilize principles, ideas, and tools to determine the maximum effectiveness of a ship's cybersecurity system.

It should be emphasized that the reviewed works improve the theoretical basis and offer some solutions to enhance the cybersecurity of maritime transport. Development of theoretical provisions using an integral approach to assess the vulnerability of basic or critical systems of a seagoing vessel is of high practical interest. Therefore, the purpose of this study is to analyze potential threats to the ship's cybersecurity, aggregate them, and establish links between various events, cybersecurity breaches and their consequences.

2. METHODOLOGY

2.1. Fundamentals of Ship Cybersecurity Assessment

According to analysts, the potential channels and opportunities for hacker attacks will increase over time, and their types will be changed and modified. Thus, ship's cybersecurity becomes an important factor in ensuring the security of navigation. Notably, the Maritime Safety Committee of the International Maritime Organization (IMO) adopted Resolution MSC.428 (98) - Maritime Cyber Risk Management in Security Management Systems in June 2017. This resolution requires administrations to ensure that cyber risks are addressed in ship security management systems after January 1, 2021. Thus, protection against cyber risks becomes not only an initiative of shipowners, but also an international requirement for them. Today, cyberattacks are not just aimed at stealing shipboard data; at the heart of cyber crime is the control of shipboard systems' operating technology, which is the result of the evolution of maritime piracy, as the mentioned control by outsiders can lead to the takeover of ship's command and control systems. Operational technology (OT) is part of the ship's management and control processes in conjunction with information technology (IT), where IT and OT have different roles within the organization: OT correlates more with the physical world, while IT refers to information processing.

Operational technologies are also part of the ship's 'critical systems', which are vital to the ship, and they are usually separated 'physically' from information systems (Figure 1). Therefore, when it comes to cyberattacks on ships, due to the fact that IT systems interact with OT systems, the focus of cybersecurity issues should be on these two key systems.

According to the analysis of information on the vulnerability of ship systems (Figure 2), we can see that the vulnerability range is very significant and reaches up to 52% in some places, e.g., the positioning system. If we consider cybersecurity as a whole, then both types of ship systems should be obviously targeted when developing appropriate security measures.

Thus, experts distinguish two groups of cyberattacks – 'targeted' and 'non-targeted', in particular, given their following composition (Figure 3):

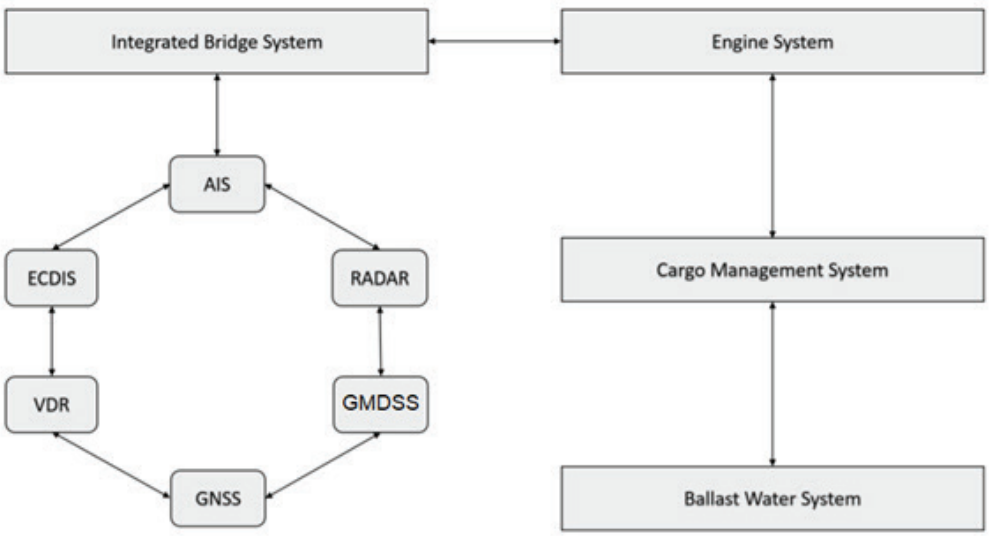

Figure 1.
Critical infrastructure of a network on board ship (Lagouvardou, 2018).

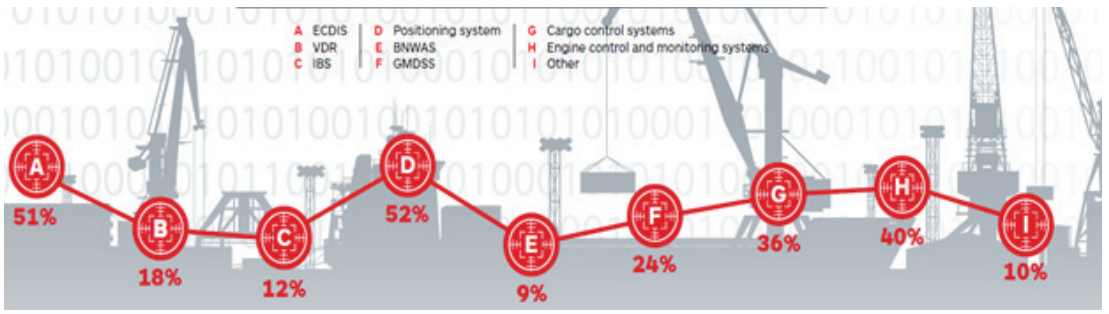

Figure 2.
Vulnerability of ship systems (BIMCO, 2016).

Figure 3.
Types of cyberattacks on ship systems (Kala & Balakrishnan, 2019).

The 2020 BIMCO guidance provides that the main subjects of cyberattacks are activists (including disgruntled employees), criminals, opportunists, states, state-sponsored organizations, and terrorists. Experts have also established the following possible security breach scenarios:

- modifying the ship's data, including its position, course, cargo information, speed, and name;
- creating a 'ghost ship' identified by other ships as a real ship in any world location;
- sending false weather information to specific ships to force them to alter course to avoid a nonexistent gale;
- activating false collision warnings, potentially causing a ship's course to be automatically corrected;
- 'turning' an existing vessel into an invisible one;
- creating non-existent search and rescue helicopters;
- tampering with EPIRB signals that activate alarms on ships in the vicinity;
- conducting a DoS attack on the entire network by initiating an increase in the frequency of AIS messaging.

Ensuring comprehensive cybersecurity measures for a ship requires first a comprehensive assessment of the ship's systems in terms of vulnerability in this context. The components of a cybersecurity assurance system are presented below. Threat and vulnerability identification are the first steps in the proposed approach (Figure 4).

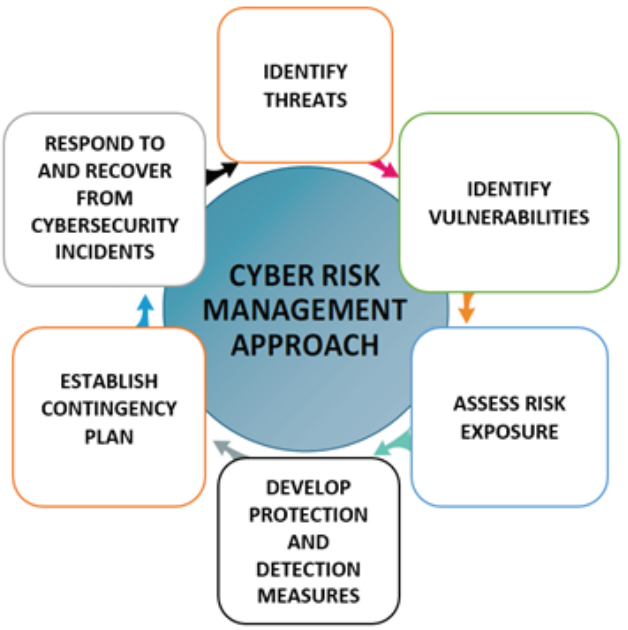

Figure 4.
Cyber risk management approach.

Risk assessment methodology, which, among other things, extends to ship cybersecurity risk assessment, is based on three components - threats, vulnerabilities, and consequences. This triad should form the basis of the cybersecurity assessment of an ocean-going vessel.

The subject study proposes a probabilistic assessment of a ship's cybersecurity, which is formed on the basis of an integral approach to assessing the vulnerability of basic ship systems (operating technologies), targets of cyberattacks (threats), and their consequences.

Note that cybersecurity experts should periodically perform the probabilistic assessment of each component of the ship's technological system. As a result of the assessment, they also form suggestions and alternatives for minimizing cyber risks.

2.2. Ship's Cybersecurity Objects

The main targets of cyberattacks are mentioned above, but this is certainly not their entire list. So, let us take G as the number of possible cyberattack targets, and their multitude described as $A = \{ A_g, g=1,G \}$. Thus, each event A_g characterizes a specific cybersecurity threat.

In addition, we should not forget the cybersecurity threats that are not targeted but result from the causes of the second

block in Figure 1. Most of these threats are similar to threats to an ordinary home or office computer, but their consequences are naturally not comparable.

The following example given in Simpanu (2018), describes a case where the absence of a collection of paper charts and a virus-infected ECDIS system lead to a ship's voyage delay. After the system inspection, the virus was quarantined and the ECDIS was restored, but the incident resulted in significant losses.

Therefore, let us distinguish the set $U = \{ U_l, gl=1,L \}$, which characterizes the possible threats to ship cybersecurity, not related to the targeted impact.

Objects that are vulnerable in terms of cybersecurity are various ship systems, which today are managed and controlled by appropriate software and information systems.

It is worth noting that different sources give various views on the composition of these systems, but these approaches mostly coincide.

Thus, the main systems of the cargo ship, vulnerable to cyberattacks, are (Hyra, 2019):

- Bridge systems;
- Propulsion and machinery management and power control systems;
- Electronic Chart Display and Information Systems (ECDIS);
- Automatic Identification System (AIS);
- Access control systems;
- Cargo management systems;
- Core infrastructure systems;
- Administrative and crew welfare systems;
- Communication systems.

Some components of the above list are highlighted as separate systems (e.g. access control system, alarm management system, thruster control system). A visual representation of the location of these systems on board ships is provided in Figure 5.

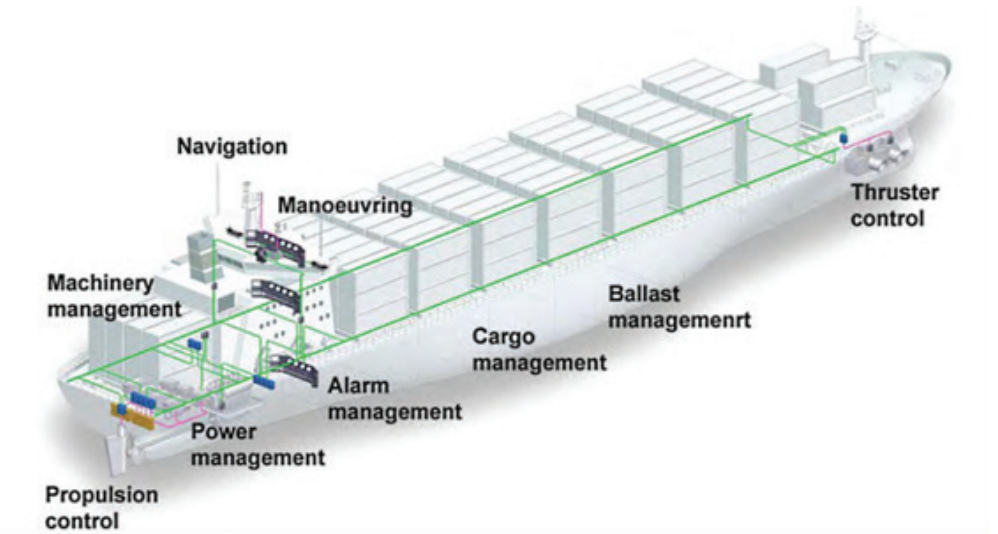

Figure 5.
Main systems of cargo ships vulnerable to cyberattacks (Hyra, 2019).

The 2020 BIMCO guidance provides a more extended and detailed list of these systems. Thus, depending on the specifics of the ship and the degree of aggregation of ship systems when assessing cybersecurity, a specific list of a ship's cybersecurity entities is compiled. To form a generalized assessment, let us assume the number of such ship systems N, and the corresponding set $B = \{ B_n, n=1,N \}$, where the essence is B_n - 'cybersecurity violation of the n-th ship system'.

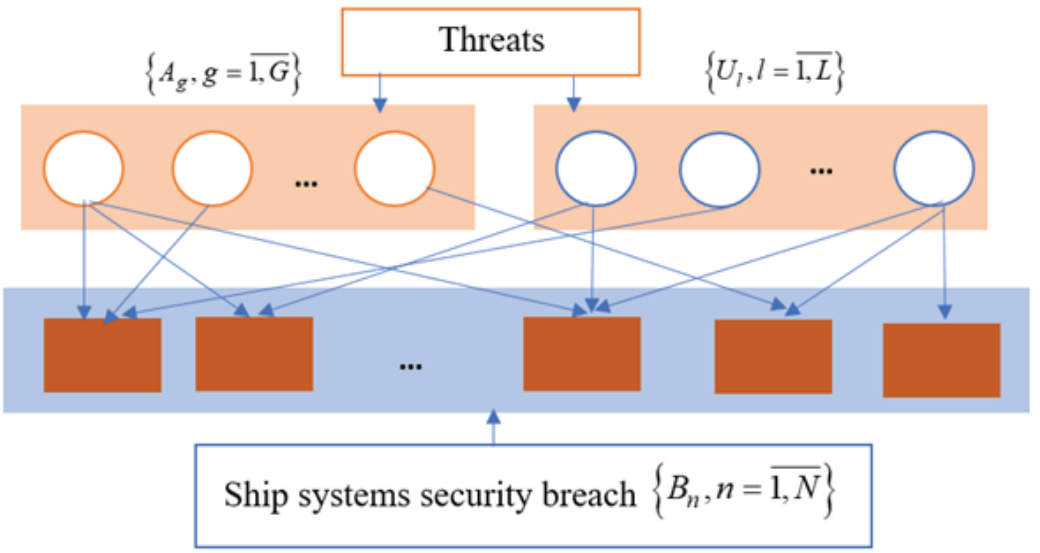

Figure 6.
Relationship 'threats - ship systems'.

It is necessary to note that each threat A_g is connected to the influence on specific ship systems, the threat U_l is characteristic almost for all ship systems (Fig. 5); however, taking into account the presence of features on each ship, we will consider the generalized variant in which each type of threats is connected to a specific set of ship systems.

Thus, multiple ship systems listed above which are vulnerable to cyberattacks of the ship are formed:

$$\Omega^B_{Ag}, g = 1, G \quad (1)$$

$$\Omega^B_{Ul}, l = 1, L \quad (2)$$

related respectively to threats A_g и U_l.

Note that the events $A = \{ A_g, g=1,G \}$ and events $U = \{ U_l, l=1,L \}$ are joint, i.e. they can occur at the same time.

Each threat can be characterized by a probabilistic assessment $0 \le P(A_g) \le 1$, which is formed on the basis of expert opinions, considering the specifics of the vessel, cargo, and the area of her operation. The probabilities $0 \le P(U_l) \le 1$ are determined on the basis of statistics by cybersecurity specialists.

2.3. Probability of Breach and Consequences for Ship's Cybersecurity

Suppose the results of successful cyberattacks are M variants (Fig.7), forming a multitude of consequences $C = \{ C_m, m=1,M \}$, which have a monetary value of $R = \{ R_m, m=1,M \}$.

Examples C_m could be 'a delay in passage', 'increased sailing time', etc. Some C_m may coincide with the threats (goals) of cyberattacks formulated in set A. Thus, the goal of the cyberattack either is achieved and then its result coincides with the threat, or the goal is not achieved, but other consequences may occur (e.g., the already mentioned 'increase in voyage time'). Another example of a consequence could be an 'accident due to a breach of navigational safety'. Thus, different cybersecurity breaches can lead to the same consequences, while at the same time, a cybersecurity breach of one of the ship systems under the influence of a certain cyberattack can lead to different consequences.

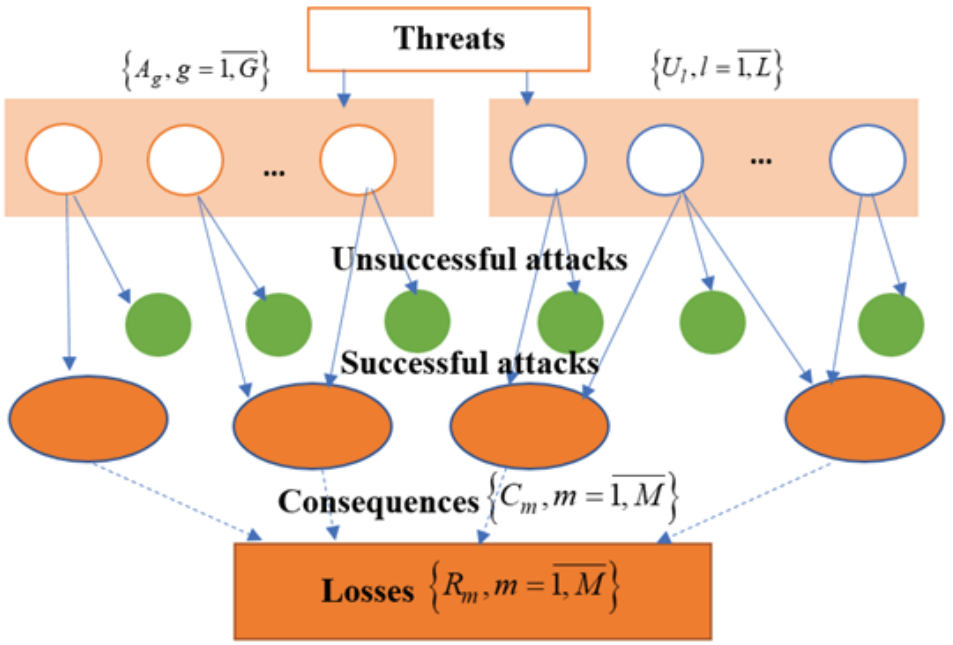

Figure 7.
Relationship 'threats'- 'consequences'.

Each consequence C_m is associated with subsets of sets *A* and *U* (targeted and non-targeted cybersecurity violations) and a subset of set *B* (ship systems).

Thus, we assign to each consequence C_m a set of Ω_{C_m}, the elements of which are those pairs of attacks and systems that lead to the consequence in question:

$$\Omega_{Cm} \supset \left(\bigcup_{g=1}^{G} \Omega^{B}_{Ag} \cup \bigcup_{l=1}^{L} \Omega^{B}_{Ul} \right), m = 1, M \quad (3)$$

Based on the cost characteristics of the ship's daily maintenance, ship repair costs, etc., the shipowner's losses can be derived in monetary terms and the ship's crew expenses should also be considered.

Note that, depending on the state of the cybersecurity system, each type of potential threat can be implemented as a cyberattack (successfully or not) and lead, respectively, to consequences or not (see Figure 7). The barrier between attacks as a result of threat realization and consequences is the ship's cybersecurity system, which is linked to each ship's system.

Since cybersecurity breaches are associated with specific ship systems, the following events

$$B_k \cdot A_g, B_k \in \Omega^{B}_{Ag}, g = 1, G \quad (4)$$

$$B_s \cdot U_l, B_s \in \Omega^{B}_{Ul}, l = 1, L \quad (5)$$

reflect the fact that the cyberattack (cybersecurity breach) is related to the relevant ship system.

In turn, the consequence C_m is manifested after the occurrence of events (4) or (5). Thus, complete and incomplete chains of dependent events are formed, which are mathematically represented as products of dependent events:

$$A_g \cdot B_k, B_k \in \Omega^{B}_{Ag}, A_g \in A \quad (6)$$

$$A_g \cdot B_k \cdot C_m, C_m \in C, B_s \Omega^{B}_{Ul}, U_l \in U \quad (7)$$

$$U_l \cdot B_s, B_s \in \Omega^B_{Ul}, U_l \in U \quad (8)$$

$$U_l \cdot B_s \cdot C_m, C_m \in C, B_s \Omega^B_{Ul}, U_l \in U \quad (9)$$

Full chains of events include consequences for the ship and the shipowner; incomplete chains consider only a cybersecurity breach.

The probability of each chain respectively is:

$$P(A_g \cdot B_k) = P(A_g) \cdot P(B_k | A_g) \quad (10)$$

$$P(A_g \cdot B_k \cdot C_m) = P(A_g) \cdot P(B_k | A_g) \cdot P(C_m | A_g \cdot B_k) \quad (11)$$

$$P(U_l \cdot B_s) = P(U_l) \cdot P(B_s | U_l) \quad (12)$$

$$P(U_l \cdot B_s \cdot C_m) = P(U_l) \cdot P(B_s | U_l) \cdot P(C_m | U_l \cdot B_s) \quad (13)$$

We denote *S* - ship cybersecurity breach, an event that is the sum of all events associated with various types of cyberattacks (both targeted and non-targeted). Assume S_1 ship's cybersecurity breach due to targeted cyberattacks, and S_2 a ship's cybersecurity breach due to non-targeted attacks. Note that the events S_1 and S_2 in their theoretical consideration are joint, but of course the probability of the event is quite little, and the probability of these events S_1 and S_2 occurring together is even less. Nevertheless, in matters of safety, even events insignificant in terms of probability must be considered.

3. RESULTS AND DISCUSSION

Mathematically, the events in question are described as follows:

$$S_1 = \sum_{g=1}^{G} \sum_{B_k \in \Omega^B_{Ag}} A_g \cdot B_k \quad (14)$$

$$S_2 = \sum_{l=1}^{L} \sum_{B_s \in \Omega^B_{Ul}} U_l \cdot B_s \quad (15)$$

$$S = S_2 + S_2 = \sum_{g=1}^{G} \sum_{B_k \in \Omega^B_{Ag}} A_g \cdot B_k + \sum_{l=1}^{L} \sum_{B_s \in \Omega^B_{Ul}} U_l \cdot B_s \quad (16)$$

The reasoning presented above allows us to estimate:

1) probability of a ship's cybersecurity breach $P(S)$;
2) probability of the consequences of a ship's cybersecurity breach;
3) property damage as a result of a ship's cybersecurity breach.

In order to assess $P(S)$, it is necessary to establish the co-occurrence/non-occurrence of the events that form *S* in (16). Theoretically, targeted and non-targeted cyberattacks can occur simultaneously and in different ship systems, which determines the theoretical coincidence of the events that form *S*. Practically, these probabilities tend to 0. Thus, in a targeted attack, hackers typically seek to gain control of a particular ship's system. The effect of non-targeted attacks is also manifested in a specific ship system. Therefore, the events forming are taken as incompatible. This fact will be considered when estimating the probability of this event and its two components:

$$P(S_1) = \sum_{g=1}^{G} \sum_{B_k \in \Omega^B_{Ag}} A_g \cdot B_k \; P(A_g) \cdot P(B_k | A_g) \quad (17)$$

$$P(S_2) = \sum_{l=1}^{L} \sum_{B_s \in \Omega^B_{Ul}} U_l \cdot B_s \; P(U_l) \cdot P(B_s | U_l) \quad (18)$$

$$P(S)=\sum_{g=1}^{G}\sum_{B_k\in\Omega^{B}_{Ag}} P(A_g)\cdot P(B_k|A_g)+$$

$$\sum_{l=1}^{L}\sum_{B_s\in\Omega^{B}_{Ul}} P(U_l)\cdot P(B_s|U_l) \quad (19)$$

Therefore, (17) - (19) estimate respectively the probabilities of targeted and non-targeted ship cybersecurity violations as well as their overall probability.

The resulting $P(S)$ must be identified according to some kind of cybersecurity scale. In particular, there should be a threshold value $P\cdot(S)$, which defines the boundary of acceptable values of $P(S)$, at

$$P(S)\le P\cdot(S) \quad (20)$$

cybersecurity risk is classified as tolerable, otherwise critical.

In turn, the likelihood of the integrity of ship's cybersecurity (event S):

$$P(S)=1-P(S) \quad (21)$$

Note that (11) and (13) describe the probabilities of the chains of events – 'attack-vessel-system-sequence'. The probability of each consequence considers all the chains of events leading to a particular consequence:

$$P(C_m)=\sum_{A_g\cdot B_k\in\Omega_{Cm}} P(A_g)\cdot P(B_k|A_g)\cdot P(C_m|A_g\cdot B_k)+$$

$$\sum_{U_l\cdot B_s\in\Omega_{Cm}} P(U_l)P(B_s|U_l)\cdot P(C_m|U_l\cdot B_s),\ m=1,M \quad (22)$$

Each consequence-event C_m, $m=1, M$ is associated with a potential loss R_m, $m=1, M$ as a result of a cybersecurity breach, the average value of which is estimated as:

$$R=\sum_{m=1}^{M} R_m\cdot P(C_m) \quad (23)$$

This value reflects the shipowner's risks as a result of a cybersecurity breach of the ship.

Note that in reality risks as a result of cybersecurity breach are not inherent only to the shipowner. For example, the loss of ship's control can lead to an accident, and if it is a tanker, the consequences are a possible environmental disaster due to an oil spill. It can be argued that the full list of consequences of cybersecurity breach includes all possible consequences of accidents at sea. That is why it is so important to pay as much attention to this aspect of safety as to other, traditional issues of ship and maritime safety in general.

4. CONCLUSION

Utilization of computer systems on board modern sea-going ships brings cybersecurity issues of maritime transport to the forefront in view of possible failure, malfunction, or errors in their operation, which can be crucial for the functionality of the vessel and, as a result, cause negative effects on its safety and security, and the safety of navigation as a whole.

The ship's cybersecurity management system should be integrated into the security and safety systems and should be involved at all levels from the management of the shipping company ashore to the ship's administration including all crew members to ensure safe operation and routine activities on board ship. Primarily, the control over reception, storage, and processing of information data, which can be a basis in the acceptance of administrative or operational decisions, should be established. Additionally, in order to develop a set of measures aimed at cybersecurity of the ship, all vulnerable technical systems must be clearly identified, categorized, and adequately protected. Comprehensiveness or integrity is important to ensure the effectiveness of any measures. Incidents related to various contingencies, such as unplanned course changes, machinery automation failures due to cyberattacks

or other types of cyberattacks, could only be excluded by a comprehensive approach to ship cybersecurity system design. The practical implementation of ship vulnerability assessment and the proposed model can be supported by the development of measures and preventive actions by shipowners and operator companies to improve the cybersecurity of the fleet, such as control of open access ports, antivirus protection and firewall, regular system data updates, abandonment of outdated operating systems, introduction of new cybersecurity products.

CONFLICT OF INTEREST:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES:

Abel, S., Xiao, L., & Wang, H., 2018. Causal Modeling for Cybersecurity. 209-212. Available at: http://doi.org/10.1109/SocialSec.2018.8760379.

Akpan, F., et.al., 2022. M. Cybersecurity Challenges in the Maritime Sector. Network, 2, pp. 123-138. Available at: https://doi.org/10.3390/network2010009.

Alcaide, J.I. & Llave, R.G., 2020. Critical infrastructures cybersecurity and the maritime sector, Transportation Research Procedia, 45, pp. 547-554. Available at: https://doi.org/10.1016/j.trpro.2020.03.058.

Bielawski, A., & Lazarowska, A., 2021. Discussing cybersecurity in maritime transportation. Maritime Technology and Research, 4(1). Available at: https://doi.org/10.33175/mtr.2022.252151.

Boyes, H., 2014. Maritime Cyber Security – Securing the Digital Seaways. Engineering & Technology Reference. Available at: http://doi.org/10.1049/etr.2014.0009.

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

Greiman, V., 2020. Defending the Cyber Sea: Legal Challenges Ahead. Journal of Information Warfare, 19(3), pp. 68–82. Available at: https://www.jstor.org/stable/27033633.

Hyra, B., 2019. Analyzing the Attack Surface of Ships In DTU Compute Department of Applied Mathematics and Computer Science. Master thesis. Technical University of Denmark. Avaialble at: https://backend.orbit.dtu.dk/ws/portalfiles/portal/218483747/190401_Analyzing_the_Attack_Surface_of_Ships.pdf.

Kala, N., & Balakrishnan, M., 2019. Cyber Preparedness in Maritime Industry. International Journal of Scientific and Technical Advancements, 5(2), pp. 19-28.

Kimberly T., & Jones, K.D., 2018. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy, 3, pp 147-164. Available at: https://doi.org/10.1080/23738871.2018.1513053.

Lagouvardou, S., 2018. Maritime Cyber Security: concepts, problems and models. Master thesis. Technical university of Denmark, 128 p. Available at: https://backend.orbit.dtu.dk/ws/portalfiles/portal/156025857/Lagouvardou_MScThesis_FINAL.pdf.

Malone, I. & Strouboulis, A., 2021. Emerging Risks in the Marine Transportation System 2001-2021. The National Counterterrorism Innovation, Technology, and Education Center, 70 p.

Marcus N., 2021. The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore, Sea Power Soundings, 42. Available at: https://www.navy.gov.au/sites/default/files/documents/Soundings_Papers_42_2021.pdf.

Maritime cybersecurity project, 2018. Maritime Security Center. American Bureau of Shipping. Available at: https://www.stevens.edu/sites/stevens_edu/files/files/MSC/ABS Maritime%20CybersecurityFinalProject%20Report.pdf.

Mednikarov, B., Tsonev, Yu., & Lazarov, A., 2020. Analysis of Cybersecurity Issues in the Maritime Industry. Information & Security: An International Journal, 47(1), pp. 27-43. Available at: https://doi.org/10.11610/isij.4702.

Melnyk, O., et al., 2022. Basic aspects of ensuring the shipping safety. Scientific Journal of Silesian University of Technology. Series Transport, 115, pp. 11-22. Available at: https://doi.org/10.20858/sjsutst.2022.115.1.

Melnyk, O., et al., 2022. Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. International Journal of Computer Science and Network Security, 22 (03), pp. 135-140. Available at: https://doi.org/10.22937/IJCSNS.2022.22.3.18.

Melnyk, O., Onyshchenko, S., & Koryakin, K., 2021. Nature and origin of major security concerns and potential threats to the shipping industry. Scientific Journal of Silesian University of Technology. Series Transport, 113, pp.145-153. Avaiable at: https://doi.org/10.20858/sjsutst.2021.113.11.

Meshkat, L. et al., 2020. Behavior Modeling for Cybersecurity. 1-7. Available at: http://doi.org/10.1109/RAMS48030.2020.9153685.

Nyrkov, A., et al., 2018. Mathematical models for solving problems of reliability maritime system. In: Advances in Systems, Control and Automation. LNEE, 442. Available at: https://doi.org/10.1007/978-981-10-4762-6_37.

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.

Progoulakis I, Rohmeyer P, & Nikitakos N., 2021. Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering, 9(12), p.1384. Available at: https://doi.org/10.3390/jmse9121384.

Shipunov, I., et al., 2020. Principles of using modern IT trends in maritime shipping. E3S Web of Conferences. 203. 05005. Available at: http://doi.org/10.1051/e3sconf/202020305005.

Simpanu, K., 2018. Ships infected with ransomware, USB malware, worms. Available at: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms.

The Guidelines on Cyber Security Onboard Ships, 2020. Version 4, BIMCO, 64 p.

Turyahumura, B., 2021. Maritime cybersecurity: comparing practices between developing countries : the case study of Kenya and Spain. World Maritime University Dissertations. 1757. Available at: https://commons.wmu.se/all_dissertations/1757.

Vujović, I., Čoko, M., & 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.

Yusif, S., Hafeez-Baig, A., 2021. A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research. 16. 1-24. Available at: http://doi.org/10.1080/19361610.2021.1918995.