TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation
http://www.transnav.eu
Volume 19
Number 3
September 2025
DOI: 10.12716/1001.19.03.02

Metasystem for Maritime Cybersecurity Management During Digital Transformation at Sea

A. Mrozowska
Polish Naval Academy, Gdynia, Poland

ABSTRACT: Nowadays, maritime transportation is "navigating" the rough waters generated by cyber threats, trying to find a suitable and safe route to allow cargo to be transported by sea. At the current time, when there is a disharmony between the safety environment and technological developments, the willingness of all maritime stakeholders to work together is needed to meet the challenge of ensuring proper cybersecurity management in maritime transportation. The aim of the paper is to describe the metasystem for maritime cybersecurity management during carriage goods by sea. This system takes into account both users and designers of the system. This ensures a holistic approach to maritime security during digital transformation. Finally, the author presents the structure of the meta-cybersecurity system involving the Polish Armed Forces, sea rescue services and individual stakeholders participating in port and sea trade. The practical using of the system is rooted out in the conventional vessel but the author takes into account application the system for maritime autonomous surface ships.

1 INTRODUCTION

Nowadays, maritime transportation is "navigating" the rough waters generated by cyber threats, trying to find a suitable and safe route to allow activity to be conducted at sea. At the current time, when there is a disharmony between the safety environment and technological developments and cyberthreats develop, the willingness of all maritime stakeholders to work together is needed to meet the challenge of ensuring cybersecurity at sea and carrying out various tasks in maritime industry transportation. It is difficult, because the maritime domain has begun to coexist with the cybersecurity domain, which has developed as a result of the digital transformation and has reached offshore operations with all its potential.

In maritime domain which has expanded to include cyberspace, there are maritime stakeholders. They characterize by their individual, unique attributes taking into account the nature of their internal organization, the arrangement of roles and mutual relations/interactions between their various participants. Each of them constitutes an individual safety management system with an organizational structure and a documented system enabling the implementation of safety policies by all the organization's personnel and stakeholders working with it. The complexity of external relations and internal arrangements generates the emergence of a complex cybersecurity management system having its own unique structures of organizational, process and technological nature during while performing theirs duties at sea. The elements of this system and selected elements of the environment in order to carry out the assigned tasks that make up the activity at sea are a variety of interactions that make up a complex system of maritime cybersecurity management. Its structures

include designers of systems, equipment, software, spare parts, etc., as well as users of these designed and implemented solutions. They bring their collection of competence to prepare and implement such new solutions adapting the technological development and cybersecurity environment, taking into account the application of this system over a certain period of time, i.e.: network designer, systems designer, equipment, software designers, ship designers, port infrastructure designers and builders, CCTV, etc. The main aim of the paper is to describe the metasystem for maritime cybersecurity management during carriage goods by sea.

Metasystem for maritime cybersecurity management includes elements that have not previously been included in the present structure of security management systems. However, it is firmly rooted in the hitherto high efficiency of their functionality, which determines the construction of the metasystem. meta system is developed based on the previously adopted safety management standard established in the ISM Code, which takes into account the provisions of resolution MSC.248(98). The provisions of the resolution draw attention to the need to extend the previously developed SMS to include cyber risk, resulting from the digitalization of maritime activities and the threats associated with it. Also, the progressive pursuit of the maritime industry to increase autonomy in shipping generates attention to extending the previously adopted safety management systems to include cyber security management, an integral part of which is to take into account cyber risk. That is very important because the entry into service of ships with varying degrees of autonomy is becoming a matter of time.

The work consists of four chapters, which indicate the stages and needs of the development of security management systems, which ultimately lead to the development of a structure of a cybersecurity management metasystem. The objectives of the individual chapters are as follows:

1. Defining the functional requirements required for implementation in the SMS by the shipowner of a conventional ship in accordance with the provisions of the ISM Code;
2. Implementing the provision Resolution MSC.428 (98) to the previously established SMS, in particular cyber risk management;
3. Indicating the main elements of the cybersecurity management metasystem implementing the cybersecurity management metasystem using management processes
4. Describing elements to ensure safety on maritime communication routes on which both conventional and MASS ships will navigate.

The work was prepared based on the author's own experience in the functioning of systems gained during several years of experience in a position responsible for the development, implementation and improvement of the SMS (ISM Code) and studying the literature on the subject, mainly legal acts, drafts of changes in regulations related to the development of autonomous shipping as a member of the MSC Section at the IMO Center at PRS. The result of the conducted research is the structure of the meta-system for managing cybersecurity, which takes into account its implementation by all maritime stakeholders including those who will be responsible for managing MASS operations.

2 FUNCTIONAL REQUIREMENTS ACCORDING TO PROVISION OF ISM CODE

The standard for managing the safe operation of ships was established by SOLAS`74, implemented in Chapter IX of the Convention. The provisions of the ISM Code obligated the shipowner or the entity managing on its behalf to establish, implement, maintain and improve a safety management system. SMS means "an organizational structure and documented system that enables the shipowner's personnel to effectively implement safety and environmental policies." The main formative elements of the SMS are as follows: international formal regulations, flag state of the vessel regulations, classifier regulations security, non-technical, environmental risks internal regulations of the shipowner/manager regulations at the local level. A system is a kind of structured and documented roadmap for ensuring the safe operation of a ship.

A properly functioning SMS is essential in eliminating risks to human life and health, material losses and environmental pollution. The SMS is a comprehensive system, which takes into account both management through quality and environmental management, with the overriding goal of creating safe working conditions at sea. The shipowner/manager will not be allowed to operate ships, if they do not also meet the functional requirements established in the ISM Code that includes the following functional requirements:

- safety and environmental policy;
- instructions and procedures to ensure safe operation of ships and protection of the environment in accordance with relevant international and flag state legislation;
- specific terms of reference and manners for mutual communication between shore-based and ship-based employees, as well as the communication of these employees among themselves;
- accident reporting procedures, as well as non-compliance reporting procedures;
- procedures for operation and emergency preparedness;
- procedures for internal audits and management system reviews.

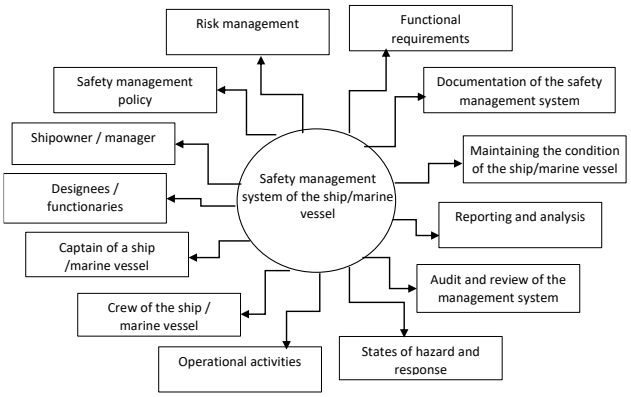

Figure 1. SMS components in accordance with the functional requirements of the ISM Code. Source: Own study.

The diagram in fig. 1 presented the main components of the SMS according to the functional requirements integral to it. Without their fulfillment, the safety management system cannot be properly established by the shipowner and then verified for compliance with the requirements of the ISM Code by the maritime administration, resulting in the inability to operate a ship/marine vessel.

The ISM Code tool is a well place in this area as a solution to expand its provisions. Therefore, implementing cybersecurity solutions through the provisions of the ISM Code has become the right solution. The provisions of this international document are both rigorous to implement, but versatile enough to allow ship owners/managers to implement its provisions taking into account the specifics of their operations and the types of ships/marine vessels they manage. In addition, these requirements oblige the shipowner to take a systemic approach to maritime safety at every organizational level of the ship owning company, including both the shipowner's office staff and the crew members of the ship/marine vessel. The digitalization of the maritime industry has forced the need to implement solutions to ensure cybersecurity at sea therefore MSC.428(98) resolution, as implemented in the ISM Code, appears to be the first step towards a systemic approach to ensure the appropriate level of cybersecurity for conventional vessels, remote or autonomous ship operations with various levels of autonomy.

3 THE PROVISION OF RESOLUTION IMO MSC.428(98) AND THEIR IMPLEMENTATION TO SMS, IN PARTICULAR CYBER RISK DURING TECHNOLOGY TRANSFORMATION AT SEA (IN MARITIME TRANSPORT)

The introduction of the resolution's provisions into the SMS resulted in the need to implement cyber risk management methods by ship owner/ manager. In addition, the functional requirements have been expanded to add the following issues related to ensuring cybersecurity management, by:

- establishing a cybersecurity management policy;
- preparing and implementing cybersecurity management procedures;
- identifying cybersecurity resources and assets both in the ship management/owner's office of the marine vessel and directly on the ships;
- ensuring proper means and channels of communication;
- ensuring that incidents can be reported, analyzed, and responded to;
- identifying threats and assessing risks of occurrence using cyberspace;
- identifying opportunities to improve already implemented solutions through systematic management system audits and reviews of the SMS management.

The elements that affect the design of the SMS under the current ISM Code and the incorporated MSC. 428(98) resolution and in the context of maritime autonomous surface vessels are based on cybersecurity management. Cyber risk management is important to ensure proper preparation in case of crisis situation at sea caused by cyberattack on the networks and systems of a ship or stakeholders of the maritime industry (maritime transport). Cyber risk management defined in an iterative process that consists of: identifying, analyzing, assessing (figure 2) and communicating cyber risk, and accepting, transferring, avoiding or reducing risk to an acceptable level while taking into account the costs and benefits of actions taken by stakeholders participating in managing maritime cyber risk. The stages of cyber risk management in maritime transport have been decomposed into four main stages, in line with the approach to critical infrastructure security management:

- preventing cyber threats;
- preparing for cyber threats;
- responding to cyber threats;
- recovering the ability to perform tasks.

Proper cyber risk management is important due to the fact that MASS came into force soon in international voyage. Moreover, MASS and conventional vessel will be proceeding in the some sea area but they have different situation awareness. It is worth emphasizing that cybersecurity issues are not addressed in the MASS Code. Therefore, it seems that the ISM Code, together with the expanded IMO resolutions, will support the safety of MASS operations as well as conventional ships. Safety management systems will need to address individual issues of managing MASS operations and in correlation with MASS operations of conventional ships, as well as smart seaports.

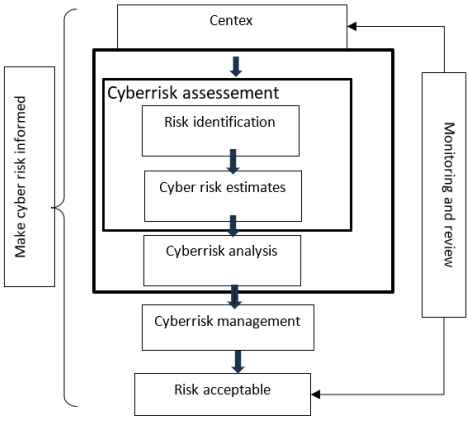

Figure 2. Cyber risk management process based on ISO/IEC 27001:2022. Source: Own study based on J. Krawiec, Cyberbezpieczeństwo. Podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2019.

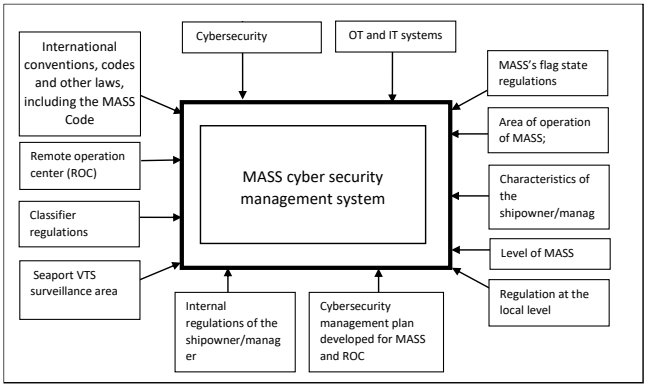

Figure 3. Elements influencing the design of the safety management system of MASS with various levels of autonomy.

The elements that affect the design of the SMS under the current ISM Code and the incorporated MSC. 428(98) resolution and in the context of maritime autonomous surface vessels are shown in the fig.3.

4 THE MAIN ELEMENTS OF CYBERSECURITY MANAGEMENT METASYSTEM USING OF MANAGEMENT PROCESSES

The digital sea project under development, on which MASS will mostly sail, systematically replacing conventional ships, needs a system that is hierarchically superior to the systemic approach to maritime safety and cybersecurity management adopted to date. By extending understanding of management systems, the author builds a metasystem for managing cybersecurity in maritime transportation during the digital transformation of shipping, at the threshold of which are MASS with various levels of autonomy. The resulting metasystem is capturing an emerging transformation focusing on the sources of construction of safety and security management systems, their interactions, and the designers of these systems along with their users. In addition to the resulting metasystem, an interpretive paradigm is created, which involves taking into account subjective sources of data processed on the basis of knowledge, but allowing the implementation of new solutions under certain conditions of uncertainty arising from the inability to predict the phenomena occurring in the new way of implementing maritime transportation in the cyberdomain, taking into account MASS as an object transporting various types of goods. The metasystem for maritime cybersecurity management, shown in fig.4, includes elements that have not previously been included in the structure of safety and security management systems. However, it is firmly rooted in the hitherto high efficiency of their functionality, which determines the construction of the metasystem. Its structures included designers of systems, equipment, software, spare parts, etc., as well as users of these designed and implemented solutions. They bring their collection of competence to prepare and implement such new solutions adapting the technological development and cybersecurity environment, taking into account the application of this system over a certain period of time. Network, systems, equipment, software designers, ship designers and builders, port infrastructure designers and builders, CCTV, etc. Designers design on the basis of data and sets of competencies to make the closer and farther users of the system form a kind of metasystem, built from functional requirements to execute maritime transportation globally.

The selection of these components is the result of perceiving the issue of the safety management system from as the result of their dynamic interactions. Regardless of the development of automation, technology, autonomy in shipping, this clash between the functionality of devices and the center as a human being will have its place.

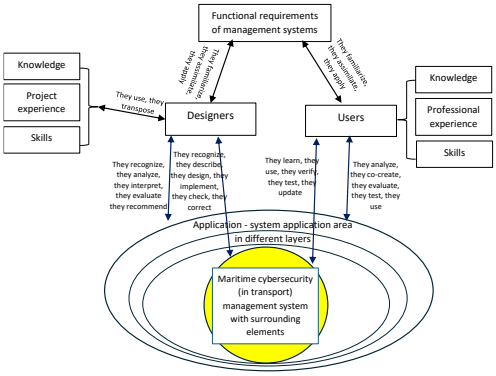

Figure 4. Metasystem for maritime cybersecurity management. Source: Own study

However, the functioning of the metasystem in the age of the technological revolution at sea is being pinned down by a sequence of activities in the form of implementing processes that link the elements of the metasystem to each other.

Fig. 5 shows the expanded metasystem with management processes. The first of these is planning. It includes the development of strategies and action plans necessary for their implementation. This includes analyzing the environment, assessing resources, and forecasting events.

The second management process in metasystem is organizing, which involves arranging and allocating resources so that the set goals can be met. In this process, the organizational structure is defined, along with roles, responsibilities, and the allocation of tangible and intangible assets for task performance. The work system, planned and operational activities are also defined.

Another process is directing, that is, motivating, communicating and supervising the implementation of the tasks set. Also included in this stage is the identification of anomalies and problems and the relocation of resources to carry out tasks arising from disturbances, emergency conditions, etc., as well as the handling of detected anomalies, emergency conditions, etc.

The final process is monitoring and evaluating the results based on the actions taken. It involves comparing results with assumptions and identifying deviations from the assumed norm. It also provides an oversight of activities, that they are appropriate and timely.

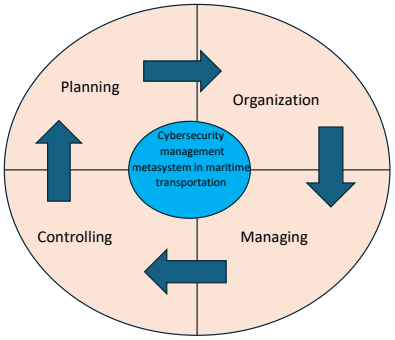

Figure 5. The architecture of management processes in the metasystem of cybersecurity management in maritime transportation. Source: Own study

The diagram in fig.6 shows the elements that build the management process for achieving the goal of ensuring the safety of maritime transportation and uninterrupted delivery of cargo on time. Given the complexity of the problem and the many different stakeholders operating under conditions of uncertainty and subjectivity in the era of digital transformation, decision-making at the level of the central bodies that will carry out the implementation of management processes should be taken into account. The leading role should be taken by the Ministry in charge of digitization together with the Ministry of Maritime Affairs, which on the basis of the established pattern of proceeding based on management processes, involve other bodies with specialists from different industries, so as to jointly develop a system based on knowledge and experience, but also experts who do not have dedicated knowledge of IT, cybersecurity or maritime safety, but are logisticians or experts from the manufacturing industry, etc. A kind of mixture of different kinds of potential is being created, based on processes that result in decisions based on actions: planned, organized, guided and controlled. They comprehensively shape the concept of a cybersecurity management system for shipping cargo by sea. The decision that is the end result of the decision-making process affects the entire operation of the concept.

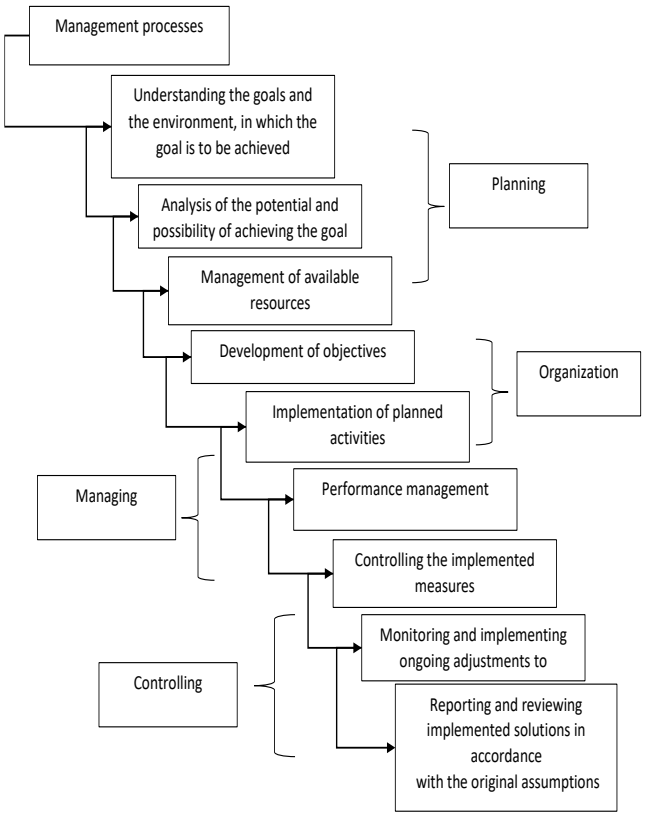

Figure 6. Elements that build decision-making processes. Source: Own study

5 THE ELEMENTS TO ENSURE SAFETY ON MARITIME COMMUNICATION ROUTES WHERE OPERATE CONVENTIONAL VESSEL AND MARITIME AUTONOMOUS SURFACE SHIP

The cyberdomain of maritime transportation has become a complex environment of occurring relationships between its resources, constituting a logical sequence of consecutive actions and also parallel activities , the implementation of which leads to the execution of tasks arising from the implementation of maritime transportation. An industry that is critical to the multidimensionality of global safety, but its vulnerability to a range of threats occurring in the maritime transportation cyberdomain constricts to properly define and organize security in the new safety environment of the maritime transportation domain. The main focal points of maritime transportation, are the means of transport, i.e., the ship carrying various types of cargo, and the point of contact between land and sea, where goods are transshipped - the seaport.

A seaport, due to the significant amount of information processed in it to ensure global trade and port operations, is an information hub (fig.7). Moreover, a vessel with all its data potential, which it uses to ensure the safety of navigation, ship operation and handling of transported cargo, is an information hub (fig.8).

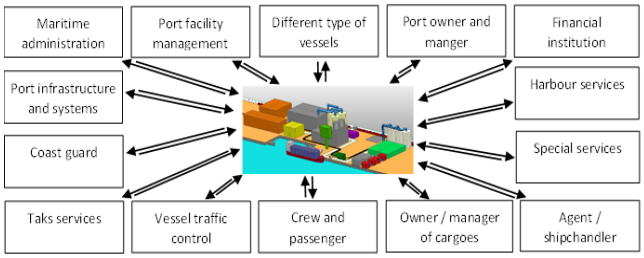

Figure 7. Seaport as an information hub.

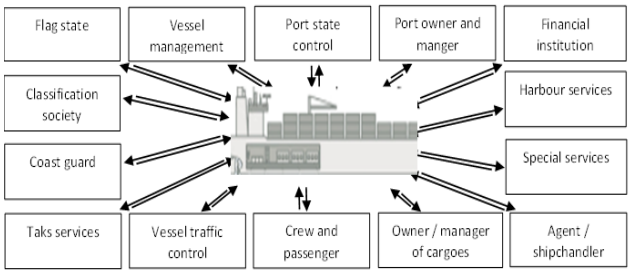

Figure 8. Vessel as an information hub.

When defining management processes in a cybersecurity management system, it is important to consider the ship/marine vessel and the port facility, which are the center of the system. However, in order to ensure their realization of tasks, the maritime cybersecurity management system consists of the following systems that constitute the external environment:

- system for defending maritime routes in communication and cyberspace;
- ship traffic surveillance and management system;

– government administration management system (shipping);
– the system for protecting the maritime national border;
– cybersecurity system for networks and systems;
– maritime search and rescue system;
– operational communications and alert system.

Taking into account the intensification of technological development in the maritime industry, figure 5.10 shows the elements of the external environment and the relationship between the maritime cybersecurity management system using maritime autonomous surface ships. In this case, the ship and port facility safety management systems that have been extended to include cybersecurity issues, disappeared. This is due to the assumption that this system will support MASS 3 and 4, which level of autonomy will require the organization of remote operation centers and consideration of response in the event of disruption to the MASS operating system, as well as disruption to the remote operation center itself. New elements have been included in the MASS maritime transportation cybersecurity management system to enable operational activities at the appropriate level of MASS navigation safety as navigation safety in the body of water on which MASS, as well as conventional ships, will operate. Also, when MASS enters service, automation and autonomy are increased at the port facilities targeted by MASS. Therefore, systems related to autonomy at the port facility are also included.

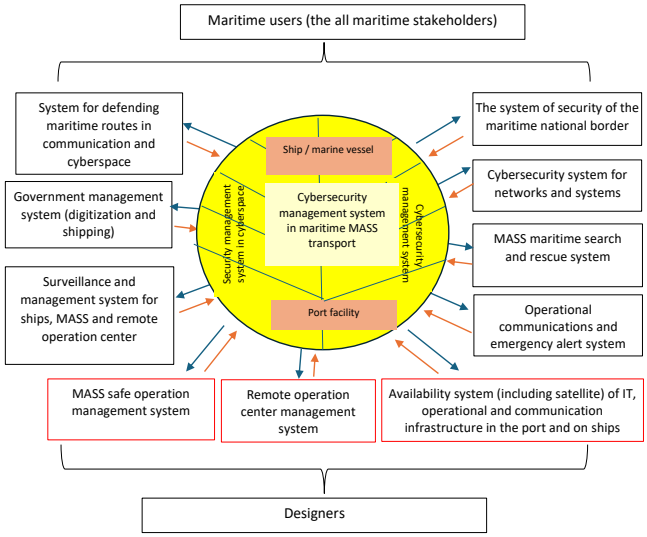

Figure 9. Elements of the external environment of the MASS maritime cybersecurity management system. Source: Own study

The cybersecurity management system for maritime transportation is presented. The system consist of number of subsystem which extended part of managing safe operation, the remote control system from the center, and the architecture and its accessibility of the network and systems in cyberspace. However, just listing the systems and building them is not enough: the right interface between them is needed, so that conventional ships and autonomous ships can travel the sea routes together, the interface between the systems, which takes into account other operational systems of conventional ships and MASS, is needed to ensure their appropriate level of safety. There is a need for a design and usable element that ensures the safety of navigation as well as data transmission of data at sea at the same time.

Therefore, the system includes designers who participate at every stage of system development, starting from the design of devices, networks, systems, technology implementation, project preparation, etc. Moreover, it causes the culture of safety at sea to evolve towards a culture of cybersecurity at sea, in which, regardless of the development of systems, a human will play a significant role either as a designer or as a user of the system or subsystems of the complex meta-system for managing cybersecurity in the cold (in maritime transport).

6 CONCLUSIONS

The accumulated research material allowed the preparation of management processes, based on functional requirements that enable the use of a systems approach to ensure cybersecurity in maritime transportation which finally is prepared safety metasystem management at sea (in maritime transportation). It was rooted out in the fact that system is noted that the maritime cybersecurity management system is a system made up of other separate systems interconnected by mutual relationships, which differ in their specifics, but there are common processes that guide maritime stakeholders to carry out their assigned tasks in maritime transportation and are critically important for their success, i.e., planning, establishing, implementing, maintaining and improving.

The accumulated research material allowed the preparation of management processes, based on functional requirements that enable the use of a systems approach to ensure cybersecurity in maritime transportation.

Attention was paid to the role of systems that constitute the preparation safety management system which is extend to cybersecurity management systems.

The research resulted in preparation the metasystem in which the center, regardless of the level of automation, is a human being who makes decisions, supervises the movement of the ship and monitors the safe operation of the ship, and thus performs management processes. In the metasystem of cybersecurity management, a significant role in building the concept of the system is played by a human being (as a designer), who, with its entire team of competencies, designs the devices, networks, systems, programming, which are then operated by it as a user. Effective cybersecurity systems which consist of alla maritime stakeholders, enable users to work in a secure environment and reduce vulnerabilities by presenting their readiness to repel a possible cyber threat as well as a physical one. However, the author understands that the proposed solutions are new and carry a kind of subjectivity. Therefore, a concept with consideration of the metasystem in different perspectives: the user, the designer and the external environment of the system is indicated. Thanks to such an arrangement, it was possible to obtain the very essence of competence needs in building a safety environment for the strategic transport of cargo, as well as its reception in a Polish port.

The time of digital transformation in shipping, where tradition meets modernity, is haggard with all sorts of disruptions. The situation creates a sense of unfamiliarity with the changes taking place, uncertainty in a new hitherto unexplored dimension. Therefore, the author, in concluding her research, understands that she has not exhausted the topic,and hopes that it will be developed and continued by other researchers. Especially with taking into account in future research the need to maintain a balance between the development of autonomy in shipping, innovation in technological progress and the safety environment, ethics and progress, taking into account the limits of human capability, working in extreme conditions, and the rational use of technology in an environment, where nature sets its laws. It is also important to take into account the fact that humanity will continue to be wise and proactive rather than reactive and be able to skillfully use technological advances for the successful operation of maritime transportation in the maritime cyber domain.

REFERENCES

[1] Bratić K. i in., Review of Autonomous and Remotely Controlled Ships in Maritime Sector, „Transactions on Maritime Science" 2019, Vol. 8(2), s. 253–265, dostępne online: https://ojs.ebujournals.lu/index.php/JIDS/article/view/18 [1.02.2024].

[2] BIMCO i in., The guidelines on cyber security onboard ships, v. 4, dostępne online: https://www.ics-shipping.org/resource/guidelines-on-cyber-security-onboard-ships-version-four/ [10.03.2025].

[3] Ramsay S., Maritime Domain Awareness and Security Imperatives Coastal Security, SP Guide Publications Pvt Ltd, wydanie 2014, access online:: https://www.spsnavalforces.com/story/?id=336 [12/02/2023]

[4] Cyber Security Code of Practice of Ships, Department for Transport GMH, July 2023, London UK, https://assets.publishing.service.gov.uk/media/64c929c0d8b1a71bd8b05e80/code-of-practice-cyber-security-for-ships.pdf

[5] Digital Container Shipping Association (DCSA) implementation guide for cyber security on vessels, v. 1.0, 10/03/2020. https://dcsa.org/newsroom/dcsa-publishes-implementation-guide-for-imo-cyber-security-mandate

[6] Gliszczyński G., Panasiewicz L., Koncepcja modelu metasystemu jako kierunek jako kierunek rozwoju teorii systemów zarządzania, Przegląd Organizacji nr 1(936), 2018, s.25, Towarzystwo Naukowe Organizacji i Kierownictwa, access online: https://doi.org/10.33141/po.2018.01.03 [12.04.2025].

[7] ISO/ IEC 27001:2022 PN-EN ISO/IEC 27001:2023-08 - wersja angielska ,Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania, 2023, access online: https://sklep.pkn.pl/pn-en-iso-iec-27001-2023-08e.html?options=cart

[8] Krawiec J., Cyberbezpieczeństwo. Podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2019

[9] MSC-FAL.1/Circ.3/Rev.2 Guidelines on maritime cyber risk management implemented by MSC.428(98) Maritime cyber risk management in safety management systems, IMO 2017.

[10] Mansouri M., Gorod A., Sauser B., A systems of systems approach to maritime transportation governance, „Transportation Research Record. Journal of the Transportation Research Board", July 2009 r., access online: DOI: https://doi.org/10.3141/2166-08.

[11] Miler R.K., Bezpieczeństwo transportu morskiego, PWN, Warszawa 2015, s.81

[12] MSC 109/5 z dnia 16 września 2024 – Development of a goal-based instrument for maritime autonomous surface ships (MASS), report of the Intersessional MASS Working Group, chapter11.

[13] Publikacja NIST, February 26, 2024, access online: DOI: https://doi.org/10.6028/NIST.CSWP.29.

[14] Regulation (EC) No. 336/2006 of the European Parliament and of the Council of February 15, 2006 on the implementation in the Community of the International Safety Management Code and repealing Council Regulation (EC) No. 3051/95 (OJ L 64, 4.3.2006, p. 1)

[15] Ramsay S., Maritime Domain Awareness and Security Imperatives Coastal Security, SP Guide Publications Pvt Ltd, 2014, access online: https://www.spsnavalforces.com/story/?id=336 [12/02/2023]

[16] Skrzypek E., Hofman M., Zarządzanie procesami w przedsiębiorstwie, Oficyna a Wolters Kluwer business, Warsaw 2010, p. 12, p. 77

[17] Strategiczna koncepcja bezpieczeństwa morskiego Rzeczypospolitej Polskiej, red. M. Biernat, J. Kwaśniewska-Wróbel, M. Skowron, BBN, Warszawa–Gdynia 2017, s.11.