Cyber security in marine transport: opportunities and legal challenges

Al Ali, Naser Abdel Raheem; Chebotareva, Anna A.; Chebotarev, Vladimir E.

Source / Izvornik: **Pomorstvo, 2021, 35, 248 - 255**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

https://doi.org/10.31217/p.35.2.7

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:187:013908

Multidisciplinary
SCIENTIFIC JOURNAL
OF MARITIME RESEARCH

University of Rijeka
FACULTY OF MARITIME STUDIES

Multidisciplinarni
znanstveni časopis
POMORSTVO

https://doi.org/10.31217/p.35.2.7

Cyber security in marine transport: opportunities and legal challenges

Naser Abdel Raheem Al Ali, Anna A. Chebotareva, Vladimir E. Chebotarev

Russian University of Transport (RUT MIIT), 9b9 Obraztsova str., Moscow, Russian Federation, e-mail: anna_galitskaya@mail.ru

ABSTRACT

In recent years, the number of cyber attacks, virus carriers, and cybercrime on maritime transport facilities has increased significantly. The emergence of new types of maritime vessels, such as autonomous vessels, dependent entirely on information and communication technologies used for passengers, cargo and baggage transportation, requires legal regulation of relations in this area. Therefore, ensuring cybersecurity in maritime transport and the need to adopt appropriate legal norms, standards and measures at both the international and national levels to manage maritime cyber risks are considered one of the most relevant topics for maritime transport. There is no single, systematic integrated approach, unification of requirements and rules in cybersecurity's sphere of maritime transport [15]. In this regard, the authors analyze the issues of ensuring cybersecurity in maritime transport, the legal basis of security: some international documents and national legal acts, regulating cybersecurity in maritime transport, will be considered, as well as the main question of how they are able to meet modern requirements for ensuring cybersecurity in maritime transport.

ARTICLE INFO

Review article
Received 23 June 2021
Accepted 12 September 2021

Key words:
Cybersecurity
Maritime cybersecurity
Maritime transport
Information and communication technologies
Cybercrime and information security

1 Introduction

One of the main features of the modern world is an active application of information and communication technologies (ICT), artificial intelligence, blockchain technology, big data, the internet of things, and other types of the so-called end-to-end digital technologies in all spheres of life, including maritime transport.

Digitalization of maritime transport facilities will become a key element of maritime transport and logistics. The Maritime Transport Review [18] for 2020 rightly notes: 'The pandemic (COVID-19) has shown that difficult times are easier to survive for pioneers, who are embracing the latest technological achievements (such pioneers include commercial enterprises and online platforms, enterprises using blockchain solutions, and external logistics companies operating on the basis of information technology)' [18]. Therefore, the connection of ships and ports to ICT networks requires special legal regulation and strengthening of measures aimed at ensuring cybersecurity.

Nowadays the practical implementation of information technologies and autonomous vessels in the maritime industry is facing the challenge of an appropriate legal framework capable of ensuring cybersecurity in maritime transport, as the existing legal framework at both the international and national levels is not able to meet modern requirements for ensuring cybersecurity of ships and other maritime industry objects. According to experts, little attention is paid to the issues of cybersecurity of marine transport infrastructure facilities of sea vessels [12]. There is still no proper legal mechanism for regulating cybersecurity due to the lack of universal approach to the conceptual apparatus of cybersecurity and international cooperation in this area.

The relevance of this article is to identify the degree of effectiveness of international cooperation in ensuring and strengthening cybersecurity in maritime transport, as well as to determine the capability of existing legal norms to ensure cybersecurity in this area.

The purpose of the research is to conduct a legal analysis of existing international legal acts and provide recommendations on ensuring cybersecurity in maritime transport, as well as to identify challenges and gaps related to the practical implementation of ensuring cybersecurity at sea.

Despite the presence of many scientific papers on maritime security, a comprehensive study of the international legal regulation of cybercrime and ensuring cybersecurity at sea has not been conducted. This fact consequently confirms the scientific novelty of the study.

2 Materials and Methodology

2.1 Materials

The choice of the research topic has been motivated by two factors: 1) most of the scientific works in the field of cybersecurity are devoted to the technical aspect of the study area; 2) very few academic papers highlight the study area within the legal context. The material for the study includes the work of both foreign and Russian authors and researchers in the field of cybersecurity, such as A. Verhelst and J. Wouters. In their study 'Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives' Verhelst and Wouters [19] focus on the factors that complicate the development of norm-setting process in cyberspace and the management of cyberspace in the international dimensionю The experts also consider the UN and EU policy initiative to ensure resilience to cyber threats. The paper examines the EU Network and Information Security Directive of 2016 and the EU Cybersecurity Act of 2019, but the IMO initiative in developing and adopting some resolutions and recommendations is not mentioned in their work [19].

The authors of the research also use the work of Rachel Foote – 'Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities, and Vessels Safe from Cyber Threats' [5]. Special attention was paid to 'Current issues of international legal regulation of the navigation of ships without crew' [6], which addresses the issue of legal provision of cybernetic security of ships without crew. Gavrilov and Dremlyuga rightly note that 'to ensure cybersecurity on these ships, it is necessary to develop a special international treaty that has put a barrier to the commission of cyber attacks and other similar illegal acts' [6]. However, this work only considers ensuring the cybersecurity of ships without a crew, while other objects of the maritime industry are not examined.

The article 'Critical infrastructures cybersecurity and the maritime sector' by Juan Ignacio Alcaide and Ruth Garcia Llave includes interesting research results on the issue of cybersecurity in the maritime area, which is becoming increasingly vulnerable to cyber attacks [1]. Alcaide and Llave have examined the issue of the level of knowledge and training required to study of cybersecurity in the maritime area and its interaction with the entire marine ecosystem. Based on the empirical research data, the scientists have confirmed the lack of general knowledge of experienced maritime transport specialists on the issues of cybersecurity at sea and the need to improve the level of training in the maritime sector.

Ignacio de la Peña Zarzuelo, when exploring the challenges of cybersecurity in maritime transport [20], emphasizes the importance of productive cooperation between the government bodies of all countries with the private sector, both to ensure the proper protection of critical industry infrastructures, as well as to promote the development of new technologies.

Despite the emergence of a number of interesting academic papers in recent years, there is still a great gap in the studies devoted to the cybercrime issues in maritime transport. International and national legal acts of particular states, official materials of the International Maritime Organization (IMO), and UNCTAD Reviews of Maritime Transport have formed the legal database for the current research.

2.2 Methods

The methodological basis of the research is based on the methods of analysis, generalization, scientific abstraction, comparative legal method, technical legal method, and interpretation method.

3 Results

A serious challenge for an integrated approach to the world maritime cybersecurity is the creation of a single conceptual apparatus in this area. The presence of diverse and unrelated terminology does not contribute to the maritime industry's awareness of cyber threats and its effective cyber defense system.

It is revealed that the problem of legal regulation of cybersecurity in maritime transport in modern international law and in national legislation is one of the urgent issues directly related to the security of the world community as a whole. The different approaches of states to the definition of cybersecurity, the types of cybercrime and the problems of ensuring cybersecurity have entailed an increase in the number of cyber threats and cyber attacks on vital important objects, including marine objects.

In order to ensure an efficient international cooperation in the field of maritime cybersecurity, it is vitally important to strengthen the role of IMO in maritime cybersecurity issues by developing and adopting the necessary measures, standards, regulations, and guidelines to combat cyber threats and cyber attacks, which could be formulated and implemented with an aim to protect vulnerable ship systems and various types of information technologies used in ports, marine structures, ships, and other elements of the maritime transport system. IMO Member

States are required to immediately adopt appropriate legal instruments to implement the Resolution MSC.428 (98) 'Maritime cyber risk management in safety management systems' [13], which is currently the only official document at the international level requiring maritime administrations of IMO Member States to ensure that cyber risks are taken into account in ship safety management systems. The issue of qualification of cyber attacks on the objects of the maritime industry as a serious punishable criminal act in the national criminal legislation is also very relevant.

After analyzing specific measures to counter cybercrime and the activities of the relevant state structures, the authors of the research have come to the conclusion that in most of the countries the systematic counteraction to cybercrime at sea is not conducted at all.

Organizational and legal measures are needed to establish national and international units to counter cybercrime, as well as to establish a special center to assist in neutralizing the consequences of cyber attacks at sea.

Based on the analysis of the doctrine, existing regulatory legal acts and state practices in the field of cybersecurity in maritime transport, the article advocates for the adoption of an international treaty on cybersecurity, which will establish an agreed conceptual framework, the basis for legal regulation of cybersecurity, including in maritime transport, and the establishment of a specialized international body within the IMO to combat cybercrime in the maritime industry.

Cybersecurity should be considered at all levels as an integral part of the safety culture necessary for the safe and efficient operation of a ship with training of personnel, who needs to be aware of technological hazards and threats, and how to deal with them in attack cases, playing a key role in ensuring cybersecurity at sea.

4 Discussion

4.1 Ensuring cybersecurity in maritime transport

The efficiency of the application of information technologies and autonomous vessels in maritime transport directly depends on ensuring cybersecurity, occured not only from illegal actions and cyber threats of hackers, pirates, terrorists, and etc., but also from unintentional actions, such as negligence, software system failure, and a lack of awareness. Therefore, with the introduction of such technologies and vessels, we should expect an aggravation of the problem of ensuring their cybersecurity [10].

The maritime industry is actively using internet-related technologies (electronic maps, virtual navigation tools, and satellite technologies), the threat of cyber attacks continues to grow, and most port facilities and ships are not sufficiently prepared for cyber threats.

Today the problem of ensuring cybersecurity in maritime transport is connected with the fact that many existing international and national legal acts on the maritime industry do not contain norms, regulating issues of ensuring cybersecurity in the field of maritime transport due to the lack of a unified, systematic, and integrated approach to the unification of requirements and rules. For instance, there is no transport center for cybersecurity in Russia. Neither the regulations of the Ministry of Transport of Russia, nor the regulations of the Federal Agency for Maritime and River Transport (in Russian – 'Rosmorrechflot') contain anything on maritime cybersecurity [15].

To ensure cybersecurity in the maritime industry, it is necessary to organize work on the harmonization of existing legal norms and the adoption of new measures, rules, mandatory norms to regulate the issues of cybersecurity.

Chronis Kapalidis, a cyber expert on maritime cybersecurity, in his introduction speech to the Hellenic American Maritime Forum, held in 2019, spoke about the possible cybersecurity challenges, facing shipping, and stressed that in order for smart shipping to become widespread, three elements must be taken into account. The first is an efficiency, which is expressed in an increase in the amount of profit. The second element is a reliability, and the third element is safety and security (the core element). A certain technology has already been laid for most of these 'ingredients'. 'The situation will only get worse due to the growing cyber addiction. There is a cyber element in everything we do' [8]. He has also rightly pointed out that in order for the maritime industry to become more active and secure, it is necessary to launch investing in cybersecurity, and undoubtedly, investing in cybersecurity will benefit this industry, so from the moment of the introduction of ICT in the construction of new ships and other objects of the maritime industry, it is vitally important for cybersecurity to become a part of the entire 'construction'.

Cybersecurity should be considered at all levels in the company, from top management on land to personnel on board, as an integral part of the safety culture required for the safe and efficient operation of the ship. The training process plays a key role in ensuring cybersecurity at sea, the crew and the passengers should be aware of technological hazards and threats, and have a good knowledge of how to deal with such challenges in case of possible attacks.

4.2 The legal regulation of cybersecurity in maritime transport

Thus, the international maritime legal framework basically consists of the following key agreements: Convention on the High Seas (1958), Convention on the International Regulations for Preventing Collisions at Sea (1972), International Convention for the Safety of Life at Sea or SOLAS (1974; Consolidated edition with amendments, dated January 1, 2020), International Convention on Maritime Search and Rescue (1979), the United Nations Convention on the Law of the Sea (UNCLOS, 1982), International Convention on SALVAGE (1989), International Ship and Port Facility Security Code or ISPS Code (2002).

According to these legal documents, the requirements for ensuring the safety of navigation are conventionally divided into the following groups: technical requirements related to the design, construction and equipment; navigation requirements related to the organization of the navigation of the ship; qualification and medical requirements related to the crew of the ship; requirements for the safety management system; requirements related to the threats of piracy and terrorism [7].

The norms of these conventions provide an interpretation of the general requirements for ensuring maritime security, and they have absolutely nothing to say about ensuring cybersecurity at sea due to objective factors since when developing and adopting these agreements, there was practically no introduction of ICT in all spheres of human life, so there was no need to consider the ensuring cybersecurity at sea and its regulation.

The Convention on the High Seas (1958) obliges each State-Party to take the necessary measures to ensure safety at sea. Such measures include: the use of communication signals and collision prevention; manning and working conditions of ship crews; the design of ships' equipment and their seaworthiness [2].

The Convention on the International Regulations for Preventing Collisions at Sea (1972) contains rules concerning the choice of safe speed, maneuvering, lights, sound devices, distress signals, and etc.

The International Convention for the Safety of Life at Sea or SOLAS (1974; Consolidated edition with amendments, dated January 1, 2020) is of great importance for the safety of navigation and the safety of life at sea. It contains a special list of provisions on the technical readiness of the vessel for navigation, on the design of ships, the necessary rescue equipment, vessel's fire safety, requirements for machinery and electrical equipment of ships, as well as for the operation of vessels with a nuclear power plant. The Convention establishes requirements for fire protection, the supply of ships with lifeboats (rafts), and other floating life-saving equipment.

SOLAS's chapter V 'Safety of navigation' contains 21 rules: reports on hazards, the meteorological service, the ice reconnaissance service, the establishment of ship traffic separation schemes, disaster reports, navigation equipment, rescue signals, navigation publications, manning (the requirement for the implementation of the Resolution A. 481 (XII) on 'Principles of safe manning of ships'), etc.

The Rule V/8-1 on 'Ship reporting systems' had been added to this chapter. The introduction of such systems contributes to the safety of human life at sea, the safety and efficiency of navigation, and the protection of the marine environment. Ship message systems are used to ensure the collection of information or the exchange of it through radio messages. This information allows to obtain data applied for various purposes, including search and rescue, prevention of marine pollution, elimination of the consequences of oil pollution, and weather forecasts.

Since January 1, 2020 new amendments to SOLAS convention have entered into force. Among them are the norms, aiming to prevent accidents with lifeboats. The changes relate to maintenance, thorough inspections, operational tests, routine, and major repairs of lifeboats, rafts, launching devices and disconnecting mechanisms [22].

The list of suppliers of marine satellite communication systems is expanding. Amendments to SOLAS's Chapter IV and some codes provide for the installation of the 'recognized mobile satellite services' for the transmission of distress signals at sea and for communication in case of disaster. Previously, the rules have prescribed the installation of 'Inmarsat's satellite communication systems.

It should be noted that such provisions and rules can be applied to the implementation of information technologies on ships, but it is necessary to amend the adopted and existing agreements and include new rules on the operation of autonomous vessels and on ensuring cybersecurity at sea.

The United Nations Convention on the Law of the Sea or UNCLOS (1982) contains provisions regulating the safety of navigation, ship traffic and liability arising from a collision of ships, and also obliges states to take all necessary measures to ensure safety at sea. According to paragraph 4 of UNCLOS's Article 94, such measures include the following rules:

- each vessel before registration, and later at appropriate intervals, must be inspected by a qualified state inspector and have on board such maps, nautical publications, navigation equipment and instruments as are necessary for the safe navigation of the vessel;
- each vessel must be headed by a captain and officers of appropriate qualifications (in the field of navigation, navigation, communications, ship machinery and equipment), and the crew must correspond to the type, size, mechanisms, and equipment of the vessel in terms of qualification and number;
- the captain, officers and, to the extent necessary, the crew must be fully familiar with the applicable international rules on the protection of life at sea, collision prevention, prevention, reduction and control of marine pollution and radio communication and must comply with such rules.

Most of above-mentioned agreements contain provisions on the legal status of the captain, his or her official rights and duties, imposed for the fulfillment of international obligations, embodied in the international conventions. According to these agreements, the legal status of the captain is based on his or her authority to manage the ship and the crew, including navigation, taking all required measures to ensure the safety of navigation, maintaining order on the ship, preventing any damage/harm to the vessel and the people on board, as well as to the cargo. In addition, the captain is the representative of the shipowner and the cargo owner in relation to transactions and

claims related to the needs of the vessel, cargo, and shipping itself [16]. Much attention is paid to the duties of the captain who has noticed a danger: first of all, he/she is obliged to transmit information about the accident to all vessels nearby, as well as to the competent government authorities/bodies to which he/she can establish contact.

The provisions of these agreements relating to the captain and crew in the implementation of information technology and autonomous vessels undoubtedly require changes and additions to determine the legal status of the person and the duties of those who will perform the duties of the captain on these vessels to transmit a message about the danger posed to ships at sea, and who will be responsible for ensuring the cybersecurity of navigation of these vessels. It is clear that these provisions cannot be applied to autonomous vessels, since there is no need in the presence of a captain and crew on such vessels.

The reality of cybercrime and the threat of maritime transport confirm the need to develop a special international treaty and legal mechanisms to prevent crimes and cyber attacks on maritime transport and ensure the cybersecurity of maritime transport. The existing international agreements on cybercrime, such as the Budapest Convention on Cybercrime of 2001, the Arab Convention and the Draft Convention on International Information Security of 2011 are aimed at solving more general problems of combating cybercrime. Therefore, the proposed special international treaty should contain provisions not only on bringing to justice those responsible (perpetrators) for attacks on computer systems or computer information, but also on establishing and monitoring compliance with unified minimum standards and requirements for cybersystems in order to ensure the safety of maritime navigation [6].

In 2017 within the IMO framework a number of legal documents on cybersecurity in the maritime industry (IMO 2017) were developed and adopted. These include:

- Recommendations for managing cyber risks in the maritime industry;
- Cyber Risk management in maritime security management systems, Resolution MSC. 428 (98);
- Recommendations for cybersecurity on ships.

Annex No. 10 of the Resolution MSC.428 (98) provides recommendations for the maritime administrations to ensure that cyber risks are properly addressed in safety management systems no later than the first annual verification of the company's Compliance Document after January 1st, 2021. This resolution is currently the only document at the international level that requires the maritime administrations of IMO member states to ensure that cyber risks are taken into account in ship safety management systems. Therefore, many vessels in foreign ports, starting from January 1st 2021, may face the risk of sanctions for non-compliance with the IMO recommendations on cybersecurity. The failure to comply with the cybersecurity recommendations may result in the charterer's refusal of a commercial contract. Marine cargo insurance rates are likely to differ for ships that comply and do not comply with the cybersecurity recommendations, and cyber incidents at the ship / port interface will be viewed through the lens of the cybersecurity recommendations [15].

These recommendations note that cyber technologies have become necessary for the operation and management of a variety of systems that are important for the safety of navigation and the protection of the marine environment. The recommendations also define the 'maritime cyber threats' as risks to a technological resource from potential circumstances or events that may lead to disruptions in the transportation of cargo and passengers, the safety of navigation or the safety of a ship, due to damage, loss or compromise of information related to navigation, the maintenance and development of cyber systems, as well as intentional and unintentional cyber threats [11].

The recommendations indicate that vulnerable ship systems may include: navigation bridge systems; cargo handling and management systems; engine, machine and power management systems; access control systems; passenger service and management systems; vessel's public Internet networks intended for passenger use; administrative systems and networks, and communications systems.

This list is not exhaustive and is intended as a recommendation to the organization. These recommendations can serve as a model to classify these actions or omissions as illegal acts at the national level and to include these actions into criminal legislation as punishable crimes against cybersecurity in the maritime industry.

The IMO Principles for Effective Risk Management in the Maritime Industry are based on five elements: to identify, to protect, to detect, to respond, and to recover [17; 18]. However, to be effective, these elements must be reflected in the general legal culture of all those involved in maritime transport safety. Nowadays safety culture issues are contained in the International Code of Safety Management (ISM Code). The purpose of this code is to create an international standard for the safe management and operation of vessels and the protection of the environment. It also establishes that the ship-owner or other authorized person, who has committed to the operation of the ship, undertakes to establish a safety management system and implement an acceptable policy to achieve the safety objectives.

In 2016, the Baltic and International Maritime Council (BIMCO) and several other influential maritime associations issued the 'Guidelines on Cybersecurity Onboard Ships' and in December 2020 BIMCO together with maritime industry organizations, published the 4th version of the Guidelines on Cybersecurity Onboard Ships [25]. The 2016 Guidelines outlines the basic concept of cybersecurity awareness, which includes six related steps: identify a threat; identify vulnerabilities; assess risk exposure; develop protection and detection measures; develop con-

tingency plans; and respond to cybersecurity incidents. In addition, the Guidelines state that each organization should know and apply any existing security measures, as well as the possibilities and limitations of these measures, while each company should conduct an internal risk assessment to identify potential threats and examine existing systems and procedures. This self-assessment should be accompanied by a third-party assessment to find any additional threat vectors missed during the self-assessment. The Guidelines suggests implementing a multi-level approach focused on both technical and procedural aspects. This Guidelines has served as the basis for the adoption of Resolution MSC.428 (98). The second edition of the Guidelines includes information on insurance issues, recommendations for effective network isolation, as well as new practical recommendations for connecting a ship to the shore interface, as well as managing cybersecurity when a ship enters a port and when communicating with coastal organizations.

In addition, a new insurance subsection has been added, providing insurance coverage after cyber attacks, which is an integral part of the risks to which ship-owners are exposed (10.6 – 'Losses arising from a cyber incident').

Therefore, there is an urgent need to adopt legally binding international regulations on cybersecurity in the maritime industry [5].

As Martirosyan rightly points out, 'the current system of international legal norms regulating cybersecurity does not provide comprehensive and effective mechanisms for solving specific problems that arise as a result of various forms of cyber aggression' [9].

Cybercrime in maritime transport can be committed by seizing control over management systems, cyber attacks on ship navigation and propulsion systems, on the cargo handling system and container tracking system in ports and on board the ship (Container Tracking System – CTS), as well as on automated processes, on the Electronic Chart Display and Information System (ECDIS), the site data recorder (Terminal Operating System-TOS), and etc.

Each of these systems is vulnerable in one way or another in terms of cybersecurity in maritime transport. Highly skilled hackers can break into systems applied in the maritime industry, with disastrous consequences. For instance, changing data about a vessel, including its location, cargo information, speed and name; creating 'ghost ships' identified by other vessels as a real ship; sending false weather information to specific vessels to force them to change the course; activating false collision warnings; falsifying signals, and etc. [14]. The subjects of cybercrime in maritime transport include not only hackers, but also pirates and terrorists.

It is advisable to consider creating a special judicial body to deal with cybercrimes or delegating this issue to the International Criminal Court. The existence of such a mechanism to combat cybercrime could contribute to the suppression of such types of crimes.

To sum up, the current system of international legal norms regulating maritime transport security does not provide comprehensive and effective mechanisms for ensuring cybersecurity and for solving specific problems arising from various forms of cyber attacks on maritime transport facilities.

4.3 Legal regulation of cybersecurity in maritime transport at the national level

At the national level, some states have also prepared guidelines on cybersecurity. For example, in 2016 the UK authorities, under the guidance of the Institute of Engineering and Technology, had published the 'Code of Norms and Rules: Cybersecurity of Ports and Port Systems', and later the 'Code of Norms and Rules: Cybersecurity of Ships' – in 2017. Such codes can assist companies in conducting cybersecurity assessments, developing plans to improve cybersecurity, and measures to mitigate and prevent attempted security breaches, along with the IMO Standards and Regulations on Ship Safety [17].

In the United States special attention is paid to the issue of ensuring maritime cybersecurity. In 2018, the National Institute of Standards and Technology published the 'General Principles for Improving the Cybersecurity of Critical Infrastructure'. In October 2018, the FAA Reauthorization Act was adopted. The division 'j – Maritime Security' of this law contains provisions for improving maritime security [4].

The Law supplements the existing acts on maritime security in terms of ensuring maritime cybersecurity. The competence of the subjects involved in its provision has been clarified, and the obligation to analyze cyber threats in the framework of the assessment of the security of a ship or port facility has been introduced. The ship or port facility security plan should be supplemented with provisions for detecting, responding to, and recovering from cyber threats that may lead to transport security incidents. It should be noted that for violation of these requirements, a civil fine of no more than 25 thousand dollars (USD) is provided for each day during which the violation continues. However, the maximum amount should not exceed 50 thousand dollars (USD).

In March 2020 the US Coast Guard had issued a Circular NVIC 01-20 – the so-called guiding principles to the cyber-threats to the facilities, regulated by Maritime Transportation Security Act (MTSA) – 'the Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities' [23].

On October 27, 2020, the US Coast Guard had issued a working instruction CVC-WI-027 'Ship Cyber Risk Management', which provides guidance for Coast Guard Maritime Inspectors (MI) and Port State Control Officials (PSCO) on assessing cyber-hygiene on board ships, as well as options for actions when deficiencies are detected [24].

In the Russian Federation, a unified approach to the legal regulation of maritime cybersecurity has not yet been formed. There are no special regulatory legal acts regulating cybersecurity at sea, and it is not clear which body is authorized to develop state policy and regulation in the field of maritime cybersecurity.

In 2017, the Federal Law 'On the Security of Critical Infrastructure of the Russian Federation' was adopted. However, this law is universal and common for all sectors of the economy and does not take into account the specifics of individual types of transport, in particular, sea transport. It is primarily aimed at protecting significant objects of critical information infrastructure, which includes an exhaustive list of objects: information systems, information and telecommunications networks, automated control systems. Semenov rightly points out that 'for the law, it does not matter significantly in which industry, at which facility the above-mentioned networks and systems are used. The law considers the networks and systems themselves as objects of protection, and not objects by which they are operated' [14, 15].

The Russian Maritime Register of Shipping has issued a guidelines to cybersecurity, and the provisions of the guidelines have entered into force on January 1st, 2021 [3].

This manual contains recommendations for the design, manufacture, maintenance and testing of ship's computerized systems, as well as recommendations applicable to safety management systems (paragraph 1.1.1). It also provides the interpretation of the requirements for monitoring the ship's cybersecurity in operation and the requirements necessary for the organization of cyber risk management in security management systems. The provisions of this manual have been developed in accordance with the requirements of IMO resolution MSC.428 (98), the provisions of IMO Circular MSC-FAL.1/Circ.3 'Guidelines for the Management of Cyber Risks', IACS Recommendations No. 166-Recommendation on Cyber Resilience.

This guidelines is aimed at reducing the vulnerability of vessels to cyber attacks, malware and, as a result, improving the safety of navigation.

5 Conclusion

Based on the above mentioned materials, we can draw the following conclusions:

1. The issue of maritime safety has always been and remains a key issue.
2. Modern challenges, cyber attacks and threats to cybersecurity in maritime transport in connection with the development and use of ICTs entail the need for progressive development of international law and further codification of international legal norms in the field of countering cybercrime and ensuring cybersecurity in maritime transport.
3. The efforts of states should be directed to the development of special standards and the creation of an international universal and regional mechanism to ensure cybersecurity in maritime transport.
4. The risks associated with the development of information technologies and their implementation in the maritime industry need special management to ensure the protection of cyberspace from these risks.
5. It is important to spread the culture of cybersecurity in all industries, including the maritime industry.
6. It is a matter of principle to recognize cybersecurity as an integral part of national and international security. The Russian initiative on the need to adopt the UN Convention on Cooperation in Combating Information Crime may serve as a basis for the adoption of a full-fledged universal international legal framework for the cooperation in the field of cybercrime and cybersecurity.
7. Effective provision of cybersecurity at sea requires joint efforts of all members of the world community to develop a single conceptual framework, including a universal definition of cybersecurity and its further codification, as well as the development of international criteria defining the signs and types of cybercrime at sea.
8. At the moment most states are not ready to recover from serious cyber attacks in the maritime industry due to the lack of a unified approach to the concept of cybersecurity and a single standard for protecting cyberspace in general. However, in order to eliminate these negative factors, it is necessary for states, international organizations and the private sector to reach a consensus among each other on the need to regulate their activities in cyberspace and adopt an appropriate international treaty that will serve as a model for the adoption of national regulations in this area. The adoption of such a treaty could overcome conflicts and establish a single conceptual framework in the field of cybersecurity in general.
9. The UN, regional organizations and scientific communities are the universal platform for discussing the challenges of cybersecurity and adopting appropriate measures and norms in this field.

Funding: The research is carried out within the framework of the functioning of the laboratory of information technologies in the field of law and economics of the Law Institute of the Russian University of Transport, as well as with financial support from the Russian Foundation for Basic Research (research project 18029-16013 'Research of conceptual approaches to the formation of a system of legal regulation of information security under the great challenges in the global information society').

Author Contributions: Research, Anna Chebotareva; Writing, Anna Chebotareva and Naser Abdel Raheem Al Ali; Verification, Vladimir Chebotarev.

References

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

[2] Consulate-General of the Russian Federation in Busan, Republic of Korea (2020). International legal acts regulating the safety of navigation. Available at: https://pusan.mid.ru/ru/consular-services/informatsiya_dlya_moryakov_kapitanov_i_sudovladeltsev/mezhdunarodno_pravovye_akty_reguliruyushchie_bezopasnost_moreplavaniya/ [Accessed 20 February 2021]

[3] Cybersecurity Guidelines, Russian Maritime Register of Shipping, St. Petersburg, 2021. Available at: https://lk.rs-class.org/regbook/getDocument2?type=rules&d=BD2581FF-C53E-49FB-B8F8-0021E7F08005&f=2-030101-040 (published in Russian).

[4] FAA Reauthorization Act (2018). Available at: https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf. [Accessed 20 February 2021]

[5] Foote, R., 2017*. Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities, and Vessels Safe from Cyber Threats. Cybaris 8 (2):* 231–264. Available at: https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1073&context=cybaris [Accessed 20 February 2021]

[6] Gavrilov, V.V., Dremlyuga, R.I., 2020. Topical issues of international legal regulation of navigation of sea vessels without a crew. Moscow Journal of International Law 2. Retrieved from: https://www.mjil.ru/jour/article/view/361. Accessed 20 February 2021 (published in Russian).

[7] Gutsulyak, V.N., 2017. *Russian and international maritime law (public and private).* Publishing house 'Border', Moscow (published in Russian).

[8] Kapalidis, Ch., 2019. Cyber Security challenges for the maritime industry. Retrieved from: https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/.

[9] Martirosyan, A., 2020. Cybersecurity and International Maritime Law: An Overview of Current International Legal Issues in the Field of Cybercrime. Retrieved from: https://inter-legal.ru/kiberbezopasnost-i-mezhdunarodnoe-morskoe-pravo-obzor-aktualnyh-mezhdunarodno-pravovyh-problem-v-oblasti-kiberprestupnosti. Accessed 20 February 2021 (published in Russian).

[10] McGillivary, P. 2018. *Why Maritime Cybersecurity Is Policy Priority and How It Can an Ocean Be Addressed – Marine Technology Society Journal.* Vol. 52. Issue 5. P. 44–57. Available from: https://doi.org/10.4031/MTSJ.52.5.11.

[11] Nikolskaya, K.Y., Ivanov, S.A., Golodov, V.A., Asyaev, G.D., Minbaleev, A.V., 2017. *Review of modern ddos-attacks, methods and means of counteraction.* Proceedings of the 2017 International Conference 'Quality Management, Transport and Information Security, Information Technologies', IT&QM&IS: 87–89. http://doi.org/10.1109/ITMQIS.2017.8085769.

[12] Positive Technologies (2016) *Cybersecurity in the endless seas. Positive Technologies Blog* https://habr.com/ru/company/pt/blog/303198/ [Accessed 20 February 2021]

[13] Resolution, 2017. MSC.428 (98) *Maritime Cyber Risk Management in Safety Management Systems.* https://ru.scribd.com/document/424994427/MSC-428-98-2017-Maritime-Cyber-Risk-Management [Accessed 20 February 2021]

[14] Semenov, S., 2018. *Cybersecurity of sea and river transport. Transport of the Russian Federation*, 1 (74). (published in Russian).

[15] Semenov, S., 2020. *Maritime cyber security: assessment and solutions.* Available from: http://www.morvesti.ru/analitika/1692/82776/ [Accessed 20 February 2021] (published in Russian).

[16] Skaridov, A.S. 2020. *Law of the Sea. International public maritime law.* Yuriight Publishing House, Moscow (published in Russian).

[17] UNCTAD Review of maritime transport (2018). Available from: https://unctad.org/system/files/official-document/rmt2018_ru.pdf. [Accessed 20 February 2021]

[18] UNCTAD Review of maritime transport (2020). Available from: https://unctad.org/system/files/official-document/rmt2020summary_ru.pdf. [Accessed 20 February 2021]

[19] Verhelst, A, Wouters, J., 2020. *Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. International Organisations Research Journal*, vol. 15, no 2, pp. 105–124 (in English). DOI: 10.17323/1996784520200207.

[20] Zarzuelo, I., 2021. *Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. Transport Policy*. 100: 1–4. https://doi.org/10.1016/j.tranpol.2020.10.001.

[21] The Guidelines on Cyber Security Onboard Ships Version 4. Available at: https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf

[22] A set of important amendments to the International Convention for the Safety of Life at Sea (SOLAS) and various codes enter into force on 1 January 2020. Available at: https://www.imo.org/en/MediaCentre/PressBriefings/Pages/35-SOLAS-EIF-2020.aspx.

[23] Navigation and Vessel Inspection Circular (NVIC) 01-20; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. Available at: https://www.federalregister.gov/documents/2020/03/20/2020-05823/navigation-and-vessel-inspection-circular-nvic-01-20-guidelines-for-addressing-cyber-risks-at.

[24] USCG Office of Commercial Vessel Compliance (CG-CVC) Mission Management System (MMS) Work Instruction (WI). Available at: https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf

[25] The Guidelines on Cyber Security Onboard Ships. BIMCO. Version 4, 2020. Available at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.