MRNTI 73.34.81

M.M. Abuali[1] – *main author*, ©
M.Sh. Junisbekov[2]

[1]*Master student,* [2]*Cand. Tech. Sci., Professor*

ORCİD [1]*https://orcid.org/0000-0001-7038-436X;* [2]*https://orcid.org/0000-0002-5383-8400*

M.Kh. Dulaty Taraz regional university,
Taraz, Kazakhstan

@ [1]*mukhtaraliabuali@gmail.com,* [2]*d_muhtar@mail.ru*

CYBER SECURITY IN AUTOMATED MARITIME INDUSTRY AND ITS CONSEQUENCES

Abstract. Given article illustrates that the digitalization of the maritime industry improved the connection between the various maritime stakeholders and at the same time opened the maritime industry for the risks and vast consequences of cyber-attacks. This research paper shows the consequences of such cyber attacks to the whole operation of the maritime industry. This investigation paper described various types of consequences that can lead to the breakdown of whole operations in the maritime industry. The written research paper gives some examples regarding the cybersecurity cases in order to show the importance of this aspect for the future development of this sphere.

Keywords: maritime industry, consequences, safety, environmental, cyber threat, digitalization, automation.

Abuali M.M., Junisbekov M.Sh. Cyber security in automated maritime industry and its consequences // Mechanics and Technology / Scientific journal. – 2021. – No.2(72). – P.131-136.

Introduction. Maritime industry includes a provision of goods and services in the fields of shipping, shipyards, shipbuilding and small-scale shipbuilding, port management, infrastructure, logistics, forwarders, lawyers, brokers. Suppliers of products and services for the marine industry focused on developing and manufacturing innovative system solutions. Technologically improved processes apply not only to ships but also to marine equipment, port management, and logistics systems, environmental and safety technologies in the marine industry, as well as techniques for extracting natural resources from the seabed and other areas of the marine industry. It means that digitalization is also affecting this sphere with huge investments and improvements from the side of powerful companies or organizations, which will lead to the revolution of marine transportation. For instance, the adoption of the Global Maritime Distress and Safety System (GMDSS) in 1999 directed to ships that met an emergency during a voyage. This worldwide network obliged all ocean-going vessels of more than 300 Gross Tonnage (GT) to carry radio communication devices on board in order to alert and distinguish the vessel in an emergency [1].

Moreover, the digitalization of the marine industry disclosed an effective way of data exchange between business partners about booking, shipping instructions, loading/unloading operations, money transactions, and details of the Bill of Lading

(BoL). Such an opportunity sprung after an implementation of Electronic Data Interchange (EDI) that nowadays applied in several maritime clusters.

Methods and conditions of the investigation. Today the maritime industry is combining digitalization with Artificial Intelligence (AI). For that purpose, Google and Rolls Royce concentrated their interest in automated shipping and intelligent systems [2].

Additionally, Det Norske Veritas and Germanischer Lloyd (DNV GL) and Kongsberg are concentrating their research on cybersecurity, and especially those companies are on their way to establish a digital platform concerning cybersecurity of database services [3].

Moreover, Maersk and International Business Machine (IBM) are planning to expand their digital trade platform. It was difficult to foresee these designed experiments and innovations in the marine industry at the beginning of the 20th century, while the technological revolution replaced these enigmatic ideas into real cases.

However, developments in new technologies and systems cause this industry to be in tie connection with each sphere and to become vulnerable to cyber attacks without any security. For instance, in 2012, a group of criminals ordered hackers in order to create a syndicate which compromised the service of an Australian cargo tracking system. The cyber-criminalist wanted to know the container that could be suspected from the customs and police side as smuggled goods. With the help of such an IT program, criminals knew the actions of government agencies and started to think about how to act and avoid prosecution [4].

Another accident that demonstrated the cyber vulnerability of the maritime industry happened in February of 2017 when hackers fully managed a container vessel, sailing from Cyprus to Djibouti with 8 250 twenty equivalent units (TEU) containers on board. The steering system of this vessel fully hacked, and control switched to criminals who were in partnership with pirates. They wanted to manage the vessel fully and then direct her to the place where pirates can capture her. However, an incursion of authoritative IT specialists changed this situation into 180 degrees via returning the control to the ship's crew after an accident owner of this container vessel started to install an anti-cyber threat program into the navigation systems of all her fleet.

Results and discussion about investigation. Modern cyberspace and the level of development of information technologies provide unique opportunities for managing the most sophisticated technological processes in various industries such as defence, energy, transport, banking, and maritime logistics.

Unfortunately, the vast potential of these advancements in the IT system of the above-linked sectors increasingly used for criminal purposes. According to Accenture's report in Third Annual Study on the Cyber Resilient, today, only 17% of the world's leading companies are ready to withstand cyber attacks of any type [5].

This figure illustrates the importance of cyber threats for the world's infrastructural development, and the marine industry is not an exception. However, despite this statement, the numbers of cybercrimes are increasing year by year with tremendous consequences in diverse aspects such as economic, environmental, reputational, safety, and operational.

Environmental. Humanity and environment interconnected with each other and taking care of the environment mean the protection of the home. However, mostly the opposite happens, due to the presence of enterprises, chemical plants and exhaust gas emissions air, water and forest are polluting day by day.

The maritime industry is closely related to environmental damages due to the nature of actions that are held on by organizations, companies, and ships. For instance, onboard devices which are regulating emission control, loading, and discharging of ballast water, sewage, or bilge are automated and controlled via remote controls. Those devices could face cyber-attacks and used as a tool to damage the environment and harm human health. Moreover, according to the Houston Chronicle not only the vessels can be a target of cyber criminalists who can destabilize an operation of oil rigs and platforms via infecting them with malware or malicious software [6].

In order to overreach such defects, all equipment shall be well tested and operated by knowledgeable staff.

Furthermore, sea-related environmental issues mostly occur due to the leakage or spill of oil, chemicals into the water after the collision or explosion of tanker vessels. Such incidents could happen due to the penetration into the vessel navigation systems such as GPS, ECDIS, or AIS. These activities could impact the ecosystem of oceans and seas by harming billions of fishes and plants. For instance, an accident that happened in 1989 with M/T Exxon Valdez in Prince William Sound is an excellent example of the sea ecosystem's destruction. This occasion inflicted both financial and environmental costs on Alaska, and the consequences of oil spillage appear nowadays [7].

Therefore, people should take serious measures against environmental pollution of a water ecosystem, including plants and animals. Most vulnerable sectors of the maritime industry should understand the awful repercussion that cyber threats could bring into seas and oceans, including their ecosystem and biodiversity, respectively. In conclusion, minimization of such risks should be discussed and solved by creating unique cybersecurity measures and the implementation of anti-cyber threat actions.

Economical. The next thing which can be inflicted by cyber threats in the marine industry is the economic and financial aspects. Transportation of cargoes and goods decided after the business meetings and conferences where every detail of the voyage discussed.

Nowadays, the majority of negotiations with partners or clients, which include confidential data, money transactions, and payment card details are conducted online with the help of information technologies. Moreover, this action makes them sensitive to cyber threats because of a lack of system insecurity. Furthermore, a possible economic loss should require additional attention from companies' side, which includes maintenance of equipment and system failure, information recovery, installation of a more reliable system; and at the end will increase financial lesion via investing more money into the cybersecurity system [8].

Moreover, according to Arthur J. Gallagher & Co, transportation of cargo was ranked as one of the most cyber-attacked industries with the average financial cost of 3.79 million $ per one medium-sized company. These economical would bring a tremendous social impact on this industry by increasing the number of unemployed seafarers among the world.

Also, in 2017 shipping company BW Group Singapore had faced a penetration from hackers' side. The interruption of the computer system of this company caused tremendous economic losses because companies Internet and Intranet were out of use. For that reason, the whole fleet of this company, which includes tankers, bulk carriers, LNG, LPG, and offshore floating units, was left without financial data concerning cargo transportation, destined port, and crew exchange period, inspection time and docking duration [9].

To sum up, profit and revenue have arisen the interest of every shipping and logistics company when there is an opportunity to transport the cargo to the destined point. However, they should not forget that there is also a risk of penetration from outside, which aimed to steal commercial information and transaction of money.

Safety. It is no surprise that the maritime industry faced crucial changes in the last 20 years due to technological improvements and installations. Additionally, the interconnectivity of those automated devices lead this industry into a new revolution, and international legislations urged the majority of world fleet to apply modern aids of navigation in order to safeguard human lives and vessels. However, everything has a weakness, and the shipping industry illustrated it with some cases which appeared in this decade.

Vessels also act as a target for criminals because of equipment that is applying on board of them. This statement proved with an incident that took place in 2016 with 280 South Korean vessels. All those vessels had penetration in their satellite system, and hackers jammed their GPS. After this invasion, some vessels received false information concerning their position and course while GPS of others switched off. Additionally, ships that are on the voyage had the same figures on their GPS receiver as vessels onshore.

The accident, as mentioned earlier, should take universal significance because of fatal consequences, which can lead to loss of human lives and missing shipwreck.

To conclude, the automated shipping industry can be a target of cybercriminals due to the technologies applied on board of vessels.

Reputational. Cybercrime of great shipping companies or huge primary ports could affect sorely to their reputation in the business world due to the lack of trust after becoming a target of cyber criminalists. It means that the partnership between them ended, and they cannot trust commercial information or money transactions for such vulnerable organizations. It can be reached after the hijacking of personal and confidential data through the unsecured service of database system finally could lead to the bankruptcy of companies.

A case regarding this consequence happened at the end of 2017, with one of the most widespread shipbrokers of merchant shipping and offshore industry Clarkson that was hacked by cybercriminals. Cybercriminals jammed the computer system of organization and hijacked all confidential data regarding company clients. After this incident company sent a letter of forgiveness to all victims and installed modern anti-cyber attack IT programs via inviting the best IS specialists of the world.

In conclusion, port administration and company authorities should pay sufficient attention to the cyber-resistance of database service in order to prevent cyber crimes and to maintain its reputation among the partners and clients.

Operational. The last thing which can be defined as a possible consequence of cyber threat is the management of an organization. By management, it declared the operational level of port or administration, which is responsible for the storage of confidential data and commercial information. Also, a possible cyber threat could freeze a smooth operation of port facilities and services such as pilotage, mooring, emergency response actions, tug boat assistance, and offshore installations.

In 2010, a drilling platform in South Korea was penetrated due to the viruses which overrun the computer system and control panels. IT specialists struggled with this problem 19 days and fixed it. The shipping industry has several cases related to oil rigs that were not ready to face the cyber attacks. According to the Reuters report, other oil rig faced such an issue and froze its operation for a whole week. They could not continue their operation due to the insecurity of the IT system and the absence of IS specialists.

As before mentioned in the example, oil rigs are also a subject of cyberattacks. This incident happened in 2013, in one of Houston's oil platforms and related to the un-intentional direct threat, especially negligence of an offshore worker. In order to spend his free time with good feelings, he decided to download some movies from the Internet and did not understand that Universal Serial Bus (USB) Driver contained malicious software, which then disabled operating systems and computers on several oil rigs. Due to this malware, one rig incapacitated from the communication and navigation system. After that, she lost manoeuvrability skills and started to drift due to the crippleness of thrusters resulting in environmental damage and delay of operations.

Conclusion. After all those threats and possible consequences, the issue of cybersecurity became a global problem and aroused the interest of international organizations.

References

1. Belmont K.B. Maritime cybersecurity: cyber cases in the maritime environment // *American association of port authorities.* 2016. – Access mode: http://aapa.files.cmsplus.com/SeminarPresentations/2016Seminars/2016SecurityIT/K.%20Belmont%20%20AAPA%20Maritime%20Cybersecurity%20FINAL.pdf
2. Clarkson PLC. Notice of cyber security incident. 2017. – Access mode: https://www.clarksons.com/news/notice-of-cyber-security-incident/
3. IMO. Maritime Security, Cyber security. 2018. – Access mode: http://www.imo.org/en/MediaCentre/HotTopics/piracy/Pages/default.aspx
4. Kongsberg. Kongsberg receives first DNV GL cyber security type approval for its K-IMS system. 2017. – Access mode: https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/66667CD5227C9F21C12581D7002937ED?OpenDocument
5. Rolls-Royce. Rolls-Royce joins forces with Google Cloud to help make autonomous ships a reality. 2017. – Access mode: https://www.rolls-royce.com/media/our-stories/press-releases/2017/03-10-2017-rr-joins-forces-with-google-cloud-to-help-make-autonomous-ships-a-reality.aspx
6. Rose A. Economic consequence analysis of maritime cyber threats // *Issues in the maritime cyber security.* 2017.
7. Saul J. Global shipping feels fallout from Maersk cyber-attacks. 2017. - Access mode: https://af.reuters.com/article/africaTech/idAFL8N1JQ3CO
8. Shauk Z. Malware on oil rig computer raises security fears // *Houston Chronicle.* 2013. - Access mode: https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php
9. Silgado D.M. Master's thesis. World Maritime University. Malmo. Sweden // *Cyber-attacks; a digital threat reality affecting the maritime industry.* 2018. (pp.3-16)

Material received 08.06.21.

М.М. Әбуәлі, М.Ш. Джунисбеков

М.Х. Дулати атындағы Тараз өңірлік университеті, Тараз қ., Қазақстан

АВТОМАТТАНДЫРЫЛҒАН ТЕҢІЗ САЛАСЫНДАҒЫ КИБЕРҚАУІПСІЗДІК ЖӘНЕ ОНЫҢ САЛДАРЫ

Аңдатпа. Мақалада теңіз саласын цифрландыру әртүрлі мүдделі тараптар арасындағы байланысты жақсартатыны және кибершабуылдардың қауіп-қатері мен салдары қарастырылған. Кибершабуылдардың теңіз саласының барлық қызметіне

әсері баяндалған. Теңіз саласындағы барлық операциялардың бұзылуына әкелуі мүмкін әртүрлі салдарлар сипатталған. Осы саланың дамуы үшін маңызды киберқауіпсіздік жағдайлары туралы бірқатар мысалдар келтірілген.

Тірек сөздер: теңіз өнеркәсібі, салдары, қауіпсіздік, қоршаған орта, киберқауіптер, цифрландыру, автоматтандыру.

М.М. Абуали, М.Ш. Джунисбеков

Таразский региональный университет им. М.Х. Дулати, г. Тараз, Казахстан

КИБЕРБЕЗОПАСНОСТЬ В АВТОМАТИЗИРОВАННОЙ МОРСКОЙ ОТРАСЛИ И ЕЕ ПОСЛЕДСТВИЯ

Аннотация. Данная статья иллюстрирует, что цифровизация морской отрасли улучшила связь между различными морскими заинтересованными сторонами и в то же время открыла морскую отрасль для рисков и обширных последствий кибератак. Эта исследовательская работа показывает последствия таких кибератак для всей деятельности морской отрасли. В работе описаны различные виды последствий, которые могут привести к срыву операций в морской отрасли. Приведены ряд примеров, касающиеся случаев кибербезопасности, показывающие важность рассматриваемого аспекта для развития данной сферы.

Ключевые слова: морская промышленность, последствия, безопасность, окружающая среда, киберугрозы, цифровизация, автоматизация.