MRNTI 73.34.81

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

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

ORCID [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*

https://doi.org/10.55956/GIWK9768

CURRENT CYBERSECURITY STATE OF AUTOMATED PROCESSES IN THE INTERNATIONAL AKTAU SEAPORT

Abstract. This work examines the current state of the system for protecting the seaport of Aktau from possible cyber threats. The need to test the systematic approach of the port of Aktau against possible cyberattacks by introducing a modernized system that can ensure the security of vulnerable clusters is described. Recommendations are presented aimed at identifying the importance of cybersecurity for other maritime clusters of Kazakhstan's industry.

Keywords: Aktau port, cybersecurity, cyber threats, current cybersecurity state, possible cyber-attacks, SecureTower LDP.

Abuali M.M., Junisbekov M.Sh. Current cybersecurity state of automated processes in the international Aktau seaport // Mechanics and Technology / Scientific journal. – 2021. – No.3(73). – P.58-62. https://doi.org/10.55956/GIWK9768

Introduction. The world is relying more on technology than ever before. Numerous applications of technology have become a fundamental part of shipping, providing real information and effective communication around the world, instantaneously. Digital technology has advanced and increased exponentially in recent years; information technology (IT) and operational technology (OT) frequently connected to the world wide web than ever before, and the shipping industry cannot escape this reality [1].

At the same time, these systems are very vulnerable to cyber-attacks. Each hack can cost shipowners millions of dollars and even ruin the countries' economy by penetrating major container terminals or ports; cybercriminals can disrupt the regional and national supply chain, including port operations. For instance, in June 2017, the consequences of the cyberattack on Maersk brought losses of about $250-300 million. The attack directed to APM Terminals, which were processing more than 100 thousand containers per day. This action resulted in to completely paralyze of the system and led to failures in the container turnover schedule and huge losses. To continue the operation daily, the company invested in 4.000 new servers, 45.000 new PCs, and 2.500 applications [1].

The digitalization of 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. So, this research paper is directed

to evaluate the cyber-security state and preparedness of Aktau port to possible cyber threats.

Methods and conditions of the investigation. Aktau port located on the Eastern coast of the Caspian Sea and is the only seaport of the Republic of Kazakhstan intended for international transportation of various types of cargo such as dry cargo, crude oil and petroleum products. Initially, Aktau became a strategic organization in 1963 when there was a necessity in the transportation of uranium and crude oil. The operation of the full complex port started after the construction of four dry cargo births and two breakwaters. Moreover, the Union of Soviet Socialist Republics (USSR) aimed to enlarge the port area and in 1969-1986, built four oil loading berths and a ferry terminal. After reconstruction, oil became the primary type of cargo turnover with an annual figure of 7 million tons, while indicators of dry cargo traffic did not exceed 300 thousand tons per year. Furthermore, destruction of the USSR made Aktau port as a significant strategic object in the maritime industry of sovereign Kazakhstan. In 1999, the Aktau seaport underwent a complete reconstruction, which was a turning point in the history of its development.

In these days, Aktau seaport managed by the national company "Kazakhstan Temir Zholy" and acts as a significant logistic chain between Europe and China. Development in IT Technologies via creating new infrastructural conditions to the maritime industry of Kazakhstan increased the reputation of port Aktau among other Caspian seaports in terms of quality, variety and availability of port services. For instance, Aktau port has an integrated management system that combines three systems: quality management system, environmental management system and occupational safety and health management system [3].

Automated systems of Aktau international seaport. Aktau port after its modernization became a high level interconnected strategic organization via port's facilities with port operations such as introduced security system of SOLVO Company in terms of the automated gate and automated billing. A Solvo.Gate is a control system for the checkpoint and handling of vehicles, forklifts, tractors at a terminal or in the port area. It allows employees to reduce the time spent by vehicles at the terminal, as well as the number of container stops during loading/unloading. This system also automatically shows the UN number of each container during the checkpoint process and distinguishes the ship arrival.

Also, next system called SolvoBillingis mostly related to data exchange between the port and its clients. Billing that intended for calculating the cost of responsible storage services rendered for stevedoring companies and logistics operators, maintaining contracts and preparing statements for generating invoices for services rendered. This financial data includes the number of money transactions and bank accounts. All these automated programs are interconnected between each other and those systems can be a subject to cyber-attacks which refers to the term "computer security". For that reason, in 2015, the international port of Aktau implemented the security system of Falcongaze Company that is called SecureTower DLP. This system protects the data related to the provision of logistics services to companies engaged in cargo transportation through the port, as well as the safety of information related to the construction of strategically essential facilities on the territory of the Aktau international commercial seaport.

Research results and discussion. SecureTower DLP system protects such aspects of operational level as prevention data leakage, employee monitoring and risk analysis. Each of them has its significance and impact on smoothing operation of Aktau port. For instance, information that characterized as confidential should not leave the border of an organizations network system, and access to them should be

restricted. To meet these conditions, SecureTower DLP analyzes an inbound and outbound information flow from the organization's network system, taking into consideration the measures mentioned below:

- full control of all communication channels – this action should be done in case of an emergency like penetration or hacking and represents the interception of possible communication channels in the local network system of the port. It can be e-mails, cloud drivers, messengers, USB drivers, printers and even a web activity.

- automatic multi-parameter analysis – this capability allows Aktau port's IS department to protect the seaport's database service as effectively as possible from hot penetration. Because, by implementing this feature, SecureTower DLP will analyze the morphological characteristics of the language, text containing grammatical errors, the information in images, PDF, DjVu files, formalized data and seals in documents.

Next one is employee monitoring that depends entirely on the competence and responsibility of employees. Managers need to see the full picture of the working day, management needs to adjust teams and deadlines, and security needs to identify fraudsters and disloyal employees. Because employees can act as espionage or terrorist and for that purpose, SecureTower DLP decided to establish such an asset.

Last critical aspect of Falcongaze's system is a risk analysis that deals with the creation of the employee's behaviour model and the appointment of an appropriate level of operational risk. The risk analysis module automatically calculates the employee's risk level based on security incidents. Then a list of all employees and their risk levels is generated. Using filters and available data visualization options, you can identify employees who pose a particular risk to the port's operational level.

Nevertheless, SecureTower DLP does not concentrate on the security of the port's cargo handling equipment, ship-to-shore communication and operation of maritime services such as towing, mooring/unmooring and port inspections. It means that all those port facilities could be a subject to cyber-attack from hacker's side. This possible attack leads to economic loss, operational malfunction, loss of reputation, among other Caspian seaports. In order to show the level and state of cyber security system of Aktau port, research did a SWOT analysis table that was demonstrated below [4].

These findings represented that Aktau port does not have a systematic approach in accordance with cybersecurity resilience. Also, research defined that port of Aktau did not consider the present international practices as an examples in their cybresecurity resilience management via SWOT table.

Table

SWOT analysis

Strength:	**Weakness:**
- Majority of data concerning Aktau port considered as confidential that makes it difficult to get; - Presence of SecureTower DLP system that secures the database service, commercial sector and personal data related to stakeholders.	- Lack of unified, systematic and integrated approach regarding the cybersecurity in the maritime industry of Kazakhstan; - Absence of specialized Cyber Resilience Centers in the maritime industry of Kazakhstan; - Aktau port did not implement the recommendations of international organizations and institutions as IET, BIMCO, and IMO. Therefore, the port

	does not have a CSA, CSP and CSO that is directly related to cybersecurity state; - Lack of specialists in the sector of cybersecurity; - There are no drills in term of cybersecurity in Aktau port; - There are still vulnerable sectors in Aktau port such as cargo handling equipment, port services and communication system.
Opportunity: - Creation of Cyber Resilience Committee among Caspian seaports; - Implementation of the Vanguard system into the port facilities and network devices; - To become a member of "Port Authorities Chief Information Officer Cybersecurity Network" organization; - Establishment of Cyber Resilience Center in Aktau port; - To hire professional staff who has experience in the position of CSO.	**Threats:** - Aktau port can lose its reputation among other Caspian seaports; - Absence of emergency drills leads to chaos during a real cyberattack case; - Port employees will not know about their roles and responsibilities during cybercrime due to an absence of CSP and CSO; - Aktau port can become a subject to cyber-attack by one of the organization's members that consider as a government-driven cyber threat; - Membership in Cyber Resilience Committee shifts Aktau port to organize its Cybersecurity method under known systems and programs.

Conclusion. During the investigation process concerning the preparedness of Aktau port to possible cyber-attacks, it was found that the research did not cover several clusters as seafarers, shipping companies and Kazakhstan's governmental bodies. All those aspects would bring an effective outcome and results in research concerning the importance of the cybersecurity to the maritime industry of Kazakhstan for both official and unofficial bodies.

As before mentioned, Aktau port implemented the system called SecureTower LDP that deals with illegal penetration via highlighting the ways how it secures the database service of the port. In order to have a deeper knowledge of SecureTower LDP, the technical aspects of this system should be discussed with the founders.

Also, some cargo terminals in Aktau port owned by logistic companies and the conversation with the representatives of such companies will give a clear picture about the absence of cybersecurity resilience system in cargo handling equipment of terminals.

Furthermore, shipping companies that are operating in Aktau port such as Kaz-Mor Trans Flot (KMTF) should be assessed about their current cybersecurity state via highlighting the importance of anti-cyber threat program in database service of shipping companies, the willingness of their employees against possible cyberattack, and consequence of the unpredictable cyber threat to money transactions and operational level of the company.

Moreover, as Aktau port considered as government official body, a discussion with state institutions seems significant for further researches. A properly conducted interview would help to collect the information concerning the countries perception

about cybersecurity via highlighting already implemented laws, regulations and legislations. Besides, this body could open a link to the data that reckoned as confidential.

References

1. IMO. Maritime Security, Cyber security. 2018. – Access mode: http://www.imo.org/en/MediaCentre/HotTopics/piracy/Pages/default.aspx
2. Digital Ship. Maersk cyber-attack – a global wake-up call. 2018. – Access mode: https://en.calameo.com/read/003132028fd96d2228608
3. Voetmann M. DP World / Port of Aktau, Kazakhstan – Caspian Sea. *Project Cargo Weekly*. 2017. – Access mode: https://www.projectcargo-weekly.com/2017/08/17/dp-world-port-aktau-kazakhstan-caspian-sea/
4. Zolotykh O. What will happen with the main seaport of Kazakhstan after privatization? *E-magazine Kursiv*. 2019. – Access mode: https://kursiv.kz/news/vlast-i-biznes/2019-04/chto-stanet-s-glavnoy-morskoy-gavanyu-kazakhstana-posle-privatizacii [in Russian].

Material received 28.09.21.

М.М. Әбуәлі, М.Ш. Джунисбеков

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

АҚТАУ ХАЛЫҚАРАЛЫҚ ТЕҢІЗ ПОРТЫНДАҒЫ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕЛЕРДІҢ КИБЕРҚОРҒАНЫС ДЕҢГЕЙІ

Аңдатпа. Бұл жұмыс Ақтау теңіз портын ықтимал кибер қауіптерден қорғау жүйесінің қазіргі жай-күйін қарастырады. Осал кластерлердің қауіпсіздігін қамтамасыз ете алатын жаңартылған жүйені енгізу арқылы Ақтау портының ықтимал кибер шабуылдарға қарсы жүйелі тәсілін тексеру қажеттілігі сипатталған. Қазақстандық өнеркәсіптің басқа теңіз кластерлері үшін кибер қауіпсіздіктің маңыздылығын анықтауға бағытталған ұсыныстар жасалған.

Тірек сөздер: Ақтау порты, киберқорғаныс, кибер қауіптер, қазіргі киберқорғаныс деңгейі, мүмкін кибер шабуылдар, SecureTower LDP.

М.М. Абуали, М.Ш. Джунисбеков

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

СОСТОЯНИЕ КИБЕРБЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ ПРОЦЕССОВ В МЕЖДУНАРОДНОМ МОРСКОМ ПОРТУ АКТАУ

Аннотация. Данная работа рассматривает существующее состояние системы защиты морского порта Актау от возможных киберугроз. Описана необходимость проверки систематического подхода порта Актау в против возможных кибератак путем внедрения модернизированной системы, которая может обеспечить безопасность уязвимых кластеров. Представлены рекомендации, направленные на выявление важности кибербезопасности для других морских кластеров казахстанской промышленности.

Ключевые слова: порт Актау, кибербезопасность, кибер угрозы, текущее состояние кибербезопасности, возможные кибер атаки, SecureTower LDP.