TRANSNAV
http://www.transnav.eu

the International Journal
on Marine Navigation
and Safety of Sea Transportation

Volume 16
Number 1
March 2022

DOI: 10.12716/1001.16.01.04

Ensuring Cyber Resilience of Ship Information Systems

O. Onishchenko[1], K. Shumilova[1], S. Volyanskyy[2], Y. Volyanskaya[2] & Y. Volianskyi[2]
[1]*National University Odessa Maritime Academy, Ukraine*
[2]*Admiral Makarov National University of Shipbuilding, Ukraine*

ABSTRACT: The Covid-19 pandemic brought a problem related to the inability to timely update security systems on ships during a voyage and the need to encrypt data stored in ship information systems (SISs) and shipping company information systems. The analysis of new types of worldwide cyberattacks showed that they were set off by an increase in the use of remote-controlled autonomous technologies and a spread of telework. It was proved that on ships: a) there are no cybersecurity specialists; b) there is no means of identification of cyber threats and no response plans; c) there is a lack of cybersecurity training for crews; d) encryption of confidential ship data is barely used; e) crew is a vulnerability factor in ship's security. The analysis of cyber incidents allowed us to develop a basic response plan to protect ship control systems. It was demonstrated that the basic plan can be continuously updated and improved in accordance with: a) the real state of ship systems; b) the results of performance analysis of crew actions; c) the emergence of new types of cyberattacks. To improve the security of confidential data in ship information networks theoretical framework for the development of encrypted data search engines with the identification of "dangerous" keywords for the ship information systems (SISs) was proposed. A data exchange protocol, basic requirements for SISs, and an algorithm for detecting "dangerous" keywords in messages were developed. A test search engine on encrypted data was presented, and the main components of the system were highlighted. The functionality of the system was experimentally proved, and the accuracy and speed of search on encrypted data were determined.

1 INTRODUCTION

The COVID-19 recession caused an increase in cyberattacks on information systems around the world. Given that shipping transports 90% of global trade, the maritime industry and maritime transport infrastructure are very attractive targets for cybercriminals. For example, during hybrid wars hackers can disrupt the delivery of supplies to cause massive damage to the country's economy. The Israeli company NavalDome reported a 400% increase in attempted cyberattacks on information systems in 2020. In general, the damage caused by cyberattacks cost the global maritime industry about $200 billion.

A global problem is the inability to update ship security systems when on a voyage or in remote ports, or in the roadstead. Shipowners have to wait for a ship to complete her voyage or call at a port that has the necessary information resources and equipment [20].

Due to social constraints, recession, and abundance of malicious software (ransomware, phishing attacks, social engineering techniques, etc.) shipping companies are not able to sufficiently protect themselves. This forces suppliers, equipment manufacturers, and IT professionals to connect autonomous systems to the Internet to ensure timely maintenance, storage, and distribution of information. Such autonomous systems and processes increase the vulnerability of maritime information networks leading to the possible emergence of new types of cyberattacks.

Operators of coastal and marine networks and systems are usually convinced that a traditional antivirus system protects them against cyberattacks and blame any anomaly on the need to reboot servers, a system error or a system failure. However, individual systems in operational technology (OT) network are insecure because firewall and software only protect information technology (IT) resources. Therefore, individual OT endpoints, critical systems, and components may be sensitive or obsolete, lacking security updates, which increases vulnerability to cyberattacks. "Computers, servers, laptops, tablets, mobile phones and other devices are considered to be endpoints. The lack of reliable endpoint protection made it possible to launch such attacks as Petya, WannaCry, and Bad Rabbit" [9].

Any part of the ship traffic management system, as well as the cargo handling and security system, can become vulnerable. Protecting the entire network from attacks will not solve the vulnerability problem. You need to protect each information system, encrypt its data, and adopt advanced user authentication methods. Unless there is an understanding of the scope and severity of relevant cyber risks, the ship-shore system will be deadlocked – "no vision– no actions". The OT network has no "dashboard" to allow operators to see the status of all systems connected. With vision comes the ability to take adequate actions and respond to cyber threats. Even some baseline monitoring and response plan will make it considerably harder to carry out a "ship shore" cyberattack, and the resilience of the ship's information system needs to ensure the reliability of data storage (commercial, logistics, controlling technical systems, etc.) on ship servers and local devices.

It should be recognised that a ship information system (SIS) is a complex technical system and its behaviour is described by nonlinear interconnections and complex interactions with the environment [2, 7, 10]. SIS has specific features: nonlinearity, heterogeneity, uncertainty, stochasticity, and cyclicity [11]. The variety of types of ships has led to the fact that the structures of modern SISs differ significantly, and developers face a number of serious problems related, in particular, to conducting a qualitative and quantitative analysis of systems efficiency in the initial stages of design.

When synthesizing modern SISs, it is necessary to take into account the following factors and parameters: a) complexity – a holistic approach to automation of technological processes on a ship; b) efficiency – speed of processing and availability of SIS data; c) flexibility – the ability to quickly change the configuration or functional sets of SISs depending on external environment; d) distribution – a multilayer structure and hierarchy of SIS servers; e) interconnection with other networks – the ability to import and export data arrays in widely accepted data exchange formats; f) data openness.

The last point is of particular importance and forms a serious contradiction – the need to increase the degree of openness for external users and the need to protect your information. A modern SIS or shipping company system must have mechanisms for sharing its data over the Internet – price lists, a list of services, ads, inside information, etc. It is clear that developers do not make all data publicly available and therefore special emphasis should be placed on protection SISs to prevent unauthorized access to business data, technical services, control and identification systems, and ship devices [6], for proper organization of information access levels.

The relevance of the research topic is connected with the global crisis and social distancing measures that prevent IT specialists from being mobile in the maritime sector and upgrading and maintaining critical ship OT systems promptly. Such a situation makes operators neglect security protocols and therefore ship's control systems and information networks become vulnerable to hacker attacks.

2 LITERATURE REVIEW AND PROBLEM STATEMENT

The research [18] by the maritime cybersecurity company CyberOwl presented at the CyberSecure at Sea conference showed the results of a survey of 120 IT specialists on cargo shipping. It has been demonstrated that most specialists lack understanding not only of the problems of protecting their ship's networks and devices but also of their overall structure. Some of them have poor central visibility. Some identified a lot more opportunities for connecting "shadow" IT on board the ship. CyberOwl reports that virtual blindness and lack of data protection became the current shipping reality.

[22] states that long-term cybersecurity projects are difficult to implement. They are based on comprehensive risk assessment, change of network architecture to improve segmentation, controls updating and risk management analysis. The issues of assessment of cyber risks and cyberattacks consequences on each ship remain unresolved.

As reported on [21], many people still are not able to detect even the simplest phishing emails used by hackers to steal personal and corporate information (via email, messages in social networks, fake websites, etc.). Even charging a smartphone with a USB port via an ECDIS terminal (ECDIS, Electronic Chart Display and Information System) can grant hackers access to the ship's information systems and lead to data leakage.

The reason may be not only the lack of cybersecurity specialists and an up-to-date cyber incident response plan on board but also exposure of confidential information, the lack of even primitive protection. The mentioned challenges may be overcome through risks identification on each particular ship, development of appropriate cyberattack response plans for the crew, and data encryption. This approach is applied in [18], which defines the categories of cybersecurity procedures and necessary actions that can be used to train ship personnel and prevent cyber threats.

A webinar [1], hosted by the Aspen Institute (USA), informed that since the COVID-19 pandemic started, the number of cybercrimes reported to the Crime Complaint Center of the Federal Bureau of Investigation (FBI) has roughly quadrupled. The biggest cyberattacks were carried out by hostile foreign entities or intelligence agencies. The source [4] shows that the main problem is that many people work remotely, so viruses encountered by employees easily spread to their personal devices. The most common websites attacks [12] are malicious code injection (SQL Injection), Path Traversal and Cross-Site Scripting (XSS). This is what leads to data leakage from local networks and individual devices.

The source [17] describes a new type of DDOS attack, which became the biggest in history and caused a 30-minute shutdown of 15% of the global Internet and a number of backbone providers.

This suggests that it would be appropriate to conduct a study devoted to a) the development of a response plan to modern cyber incidents for ship management information systems; b) the improvement of methods for storing and encrypting confidential data on SIS.

3 THE AIM AND OBJECTIVES OF THE STUDY

The study aims to: a) identify areas of vulnerability of maritime information systems to cyber threats, taking into account the likelihood of cyberattacks and their consequences for navigation processes; b) determine the basic processes for monitoring the cyber resilience of information systems and develop a basic response plan for the ship's crew; c) improve algorithms for SIS data encryption.

Therefore, it is necessary to ensure the SIS cyber resilience – to create conditions for the functioning of the system before, during and after a cyberattack, including information attacks. To solve the abovementioned problems, it is necessary to conduct a meta-analysis that will allow using original research data from international IT companies, summarize the results devoted to the cybersecurity problem and protection of systems in OT network.

To achieve this, the following objectives were set:

- carry out a meta-analysis of the maritime information cyberspace context;
- identify prerequisites for the development of a crew`s response plan to information risks and prevention of critical ship safety management systems (SMS) failure;
- improve the SIS data encryption system.

4 THE STUDY MATERIALS AND METHODS

The study uses the following methods: 1) the method of passive monitoring and risk identification in the development of a crew's response plan to information risks; 2) homomorphic data encryption, probabilistic Monte Carlo algorithms – in a cryptographic protection system for data stored on SIS servers (described in section 5).

4.1 *Examination of the vulnerability of maritime information systems from the perspective of cybersecurity of shipping processes*

It should be recalled that cybersecurity aims to protect information systems, networks, and programs from cyberattacks. Based on the analysis of data from cybersecurity experts in the maritime industry (Admiral Makarov National University of Shipbuilding, National University "Odessa Maritime Academy", Positive Technologies company), we will identify critical information systems:

- AIS – Automatic Identification System;
- ECDIS – Electronic Chart Display and Information System;
- VDR – Voyage Data Recorder;
- TOS – Terminal Operating System;
- CTS – Container Tracking System;
- EPIRB – Emergency Position Indicating Radio Beacon;
- GNSS – Global Navigation Satellite System;
- GPS – Global Positioning System.

Literature and Internet sources, maritime practice discovered that the most vulnerable ship systems are: bridge systems; cargo handling systems; engine, machine and power control systems, data storage and processing systems. Access control systems, passenger service and management systems, public Internet networks, administrative systems and networks, and communication systems are also at risk.

It is important to emphasize that any ship as well as all ship navigation equipment and ECDIS systems can fall a victim to a cyberattack, even at sea.

4.2 *Meta-analysis of actual cyber incidents and consequences of cyberattacks for monitoring and analysis*

The summary of cyberattacks notifications for 2017-2021 [8, 15] found that companies do not provide a detailed report on what happened. According to Reuters, little information about successful attacks on ships is publicly disclosed: business owners often cover them up for fear of damaging the image, receiving claims from customers and insurance companies, investigations being initiated. Between 2017 and 2021 Barcelona and San Diego ports were targeted by cyberattacks. Then the same happened to the Australian shipbuilder Austal, the three largest container carriers Maersk, COSCO and MSC, as well as the Shahid Rajaee port in Iran.

Maersk, June 2017 – a major cyberattack on APM Terminals system caused by the NotPetya malware. The attack disrupted the operation of ports and terminals, which sustained losses of approximately $300 million. This system handled more than 100 000 containers per day and was completely paralyzed, which led to failures in the container turnover schedule and huge losses. Maersk container ships stopped at sea and 76 port terminals of the company all over the globe were also stopped.

COSCO, July 2018 – an attack on the company’s digital assets caused the shutdown of email and telephone systems, connections with other regions and took down half of the shipowner’s US network.

MSC, April 2020 – hit by the Ruik ransomware that brought down the MSC website, caused a partial shutdown of servers at the company’s headquarters in Geneva; websites MSC.com and MyMSC became unavailable due to data centre closure. Shahid Rajaee port, May 9, 2020 – a cyberattack on the port terminal hacked the key OT systems. Shipping stopped – computers that regulate ship traffic, trucks and goods crashed.

According to the research by the cybersecurity centre Positive Research [19], the most common attacks on websites are “malicious code embedding” – SQL Injection [12], “breaking out of a directory” – Path Traversal. The common virus Cross-Site Scripting allows accessing the “administration panel”.

5 PREREQUISITES FOR ESTABLISHING BASIC CYBER RESILIENCE MONITORING OF SHIP INFORMATION SYSTEMS

5.1 *Analysis of modern-day cyberattacks to define cyber threat response processes*

Various maritime organizations are active in cybersecurity regulation of the global maritime sector, including IMO (International Maritime Organization), ISO (International Organization for Standardization), IACS (International Association of Classification Societies). But most internet technology professionals admit that they are not aware of the design of ship networks and how they are connected to distributed operational technology networks, to business networks, what vulnerabilities they cause, and how cyber threats spread across them (Figure 1.).

As shown in Figure 1., 75% of specialists have no understanding of their ship networks, 38% discovered possibilities to connect “shadow IT”, and 36% lack central visibility into networks and connected devices. Based on the study of cyberattack types published in international materials, as shown in Figure 2., we will identify the most dangerous ones for the global maritime sector.

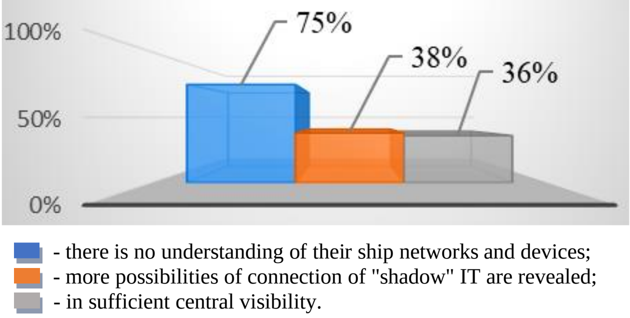

Figure 1. Visibility of ship networks and devices for IT professionals, 2020

The common types of cyberattacks shown in Figure 2. Indicate that the highest proportion of cyberattacks includes: “malicious code injection” – (SQL Injection) – 27%, “breaking out of a directory” (Path Traversal) – 17%, “cross-site scripting” (XSS) – 14%.

Such modern viruses as Bruteforce, Petya, WannaCry, Bad Rabbit are known for causing millions in damages for shipping companies. In 2017, the WannaCry ransomware caused 1 billion dollars in damage and managed to infect 500 000 computers in 150 countries around the world.

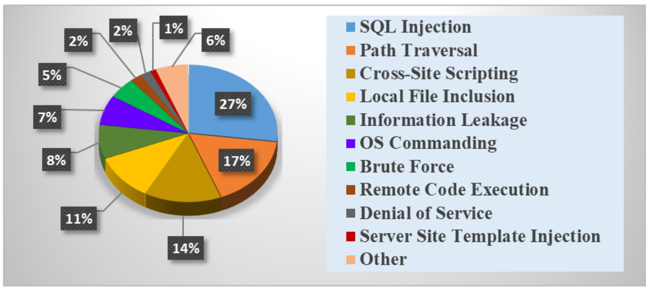

Figure 2. Widespread global cyberattacks on web applications

The Petya virus encrypted database files and data relevant for operating system startup and then demanded a bitcoin ransom. It affected government agencies and companies in Europe, the USA, Australia, Ukraine, India, Russia, and China.

5.2 *Identification of processes for the development of cyber resilience monitoring and response plan*

Taking into account the abovementioned consequences of a cyber security breach, we will highlight the main processes necessary for designing a basic response plan as shown in Table 2.

The developed processes will make it possible to implement a response plan set up to address a certain type of cyberattack, estimate the time required to restore the ship’s control system, and use analysis to demonstrate the efficiency of these processes in reducing cyber risks.

5.3 *Secure data storage and processing on ships*

Encryption – a well-known method used to protect the confidentiality of information. Formerly, all information stored in the SIS was to be encrypted. Modern cryptography provides an extensive set of encryption schemes. At the same time, to ensure the highest SIS security degree all data has to be processed in encrypted form. To solve tasks like these, homomorphic encryption is used. It allows not only performing encryption and decryption of data but also analyzing it without disclosing the contents to anyone [13].

Modern mail servers, such as IMAP servers, file servers, and other storage servers, usually have to be totally reliable. Users need to be sure that their data is not disclosed without their permission, which poses undesirable security and privacy risks. The fundamental problem is that transferring calculations to a data warehouse appears to be very time-consuming, especially if data is encrypted, and many computation tasks over encrypted data previously had no practical solution.

Table 2. Processes of building a basic plan for responding to cyber threats of the ship SISs

Processes	Necessary actions
1. Identification of the incident, cyber threat, vulnerability	Description of the threat, incident, including automatic collection and aggregation of data from a set of monitoring sources. It allows you to quickly identify system cross-links and analyze information, identify and rank risks, and visualize potential losses from cyber attacks.
2. Assessment of the degree of danger	Quantitative assessment of incidents and threats. Creating a registry of cyber incidents and vulnerabilities. Identification of areas of vulnerability of systems. Measurement of system failures and detection of abuse of usage policy. This will help identify incorrect system configuration or suspicious system behavior. Therefore, this process visualizes a vulnerability to deploying a new server or adding a new link, mobile application, or web service. It will also give an idea of the quality of staff training for cyberattacks.
3. Determining the level of and protection of critical systems	Priority actions: detection of a cyber threat or cyber incident, minimization of the probability of their occurrence, restoration of the OT system. This will reveal the interdependence between critical systems control open access ports. Protection against the next generation of threats: update of anti-virus protection, the presence of high-level firewalls – application-level proxy servers (firewall). Regular updating of system data with the introduction of new cybersecurity products. Mandatory certification of devices and equipment used by the pilot, checking the tablets for the absence of unnecessary (undeclared) electronic implants and prompt review (review) of the program code by the control service.
4. Isolation. Documentation	Isolation of "infected" equipment and immediate notification of authorities, shore services and crew about the incident. Ensuring unimpeded access to officials and competent authorities to restore the system as soon as possible. Attracting the help of experienced IT consultants. Using a backup database outside the internal platform. Documenting the incident: recording the time of its occurrence to detect infected systems and data leakage. Involvement of forensic scientists. Surveys of persons involved in the cyber incident.
5. Analysis of cyber resilience	Early detection of cyberattacks to prevent burglary and prevent failure of critical ship management systems. Will protect marine systems by: identifying areas of vulnerability; risk ranking; identification and authentication of all users; visualization of potential losses from possible cyberattacks; determining the unity of the pilot service, shore services and AIS.

One solution to this problem in SISs includes receiving files from a server and their decryption. Another solution is to leave all data on the server and develop a search algorithm for encrypted data using methods for indexing each element or sequential scanning without indexing. The disadvantage of indexes is that their storing and updating requires a significant amount of time. Also, this method is not adequate for read-only data. Thus, the best option is to perform a sequential scan without element indexing. This method appeared in modern cryptography for searching on encrypted data and can be modified for SISs (Figure 3.).

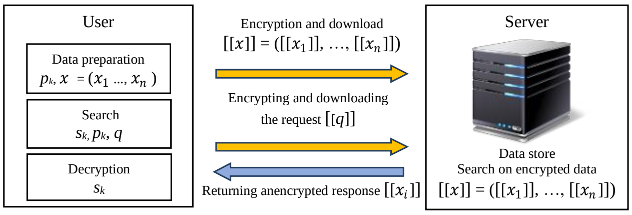
User
Data preparation
$p_k, x = (x_1 ..., x_n)$
Search
s_k, p_k, q
Decryption
s_k
Encryption and download
$[[x]] = ([[x_1]], …, [[x_n]])$
Encrypting and downloading
the request $[[q]]$
Returning anencrypted response $[[x_i]]$
Server
Data store
Search on encrypted data
$[[x]] = ([[x_1]], …, [[x_n]])$

Figure 3. Search scheme on encrypted data

For searchable encryption systems it is crucial to demonstrate their ability to preserve the confidentiality of user data and prevent information leakage from SISs. Therefore, the resilience of encryption systems to possible internal or external attacks on an unreliable server as to be tested. The server should not be able to learn anything about the original data from the encrypted text or search process. Data breach statistics [16] are shown in Figure 4.

We would highlight the main security features [16] each searchable encryption system must support: a) controlled searching – unauthorized users should not be able to perform server search [3, 5]; b) hidden query – a technique that hides an unencrypted query from an untrusted server; c) query isolation – in the search process the server should know nothing, except the search results. If there is a match between the query and the index, the server can locate the related documents and return them to the data user.

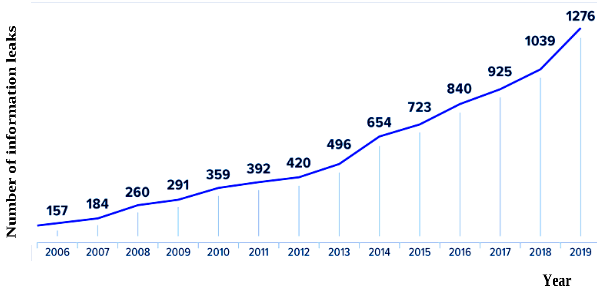

Figure 4. Annual number of information leaks in the world

An algorithm for searching over encrypted data on the SIS server is introduced (Figure 5.).

This algorithm facilitates the checking for the occurrence of certain (for example, "dangerous") keywords on encrypted data. For example, this makes it possible to make up a psychological portrait of a user of the developed system and determine (predict) their further actions without revealing the user's identity. Thus, neither client (data owner) nor their data will be publicly available and the system will be able to clearly identify whether a user is a ship specialist or a hacker.

To implement the developed message passing system with search over encrypted data, Linux Mint 19.3 OS on Virtual Box was used (configuration – 4 cores for the processor, 8 GB of RAM, 60 GB for hard disk space). Clion which supports Cmake projects was used as a development environment. The Helib library was chosen as a library supporting homomorphic encryption.

To test the system, the possibility of obtaining public and private keys from client data on SIS server side was checked. The process is shown in Figure 6. Testing confirmed that a private key obtained on the server side cannot decrypt data encrypted on the client side.

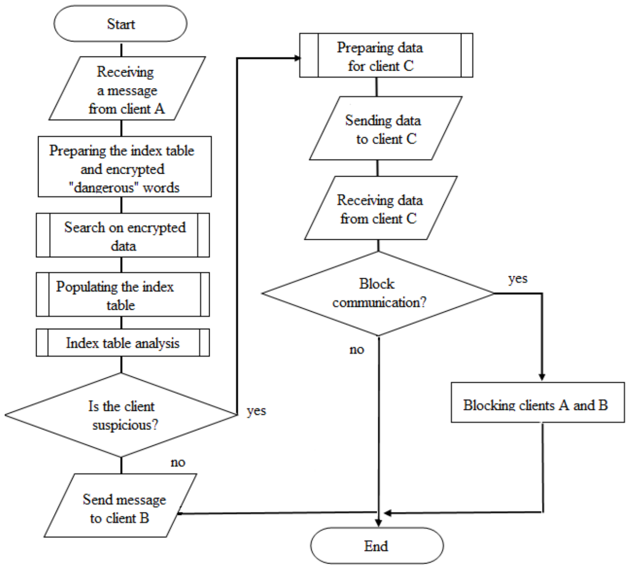
Start
Receiving a message from client A
Preparing the index table and encrypted "dangerous" words
Search on encrypted data
Populating the index table
Index table analysis
Is the client suspicious?
yes
no
Send message to client B
Preparing data for client C
Sending data to client C
Receiving data from client C
Block communication?
yes
no
Blocking clients A and B
End

Figure 5. Flowchart of the algorithm for checking messages for the presence of "dangerous" words

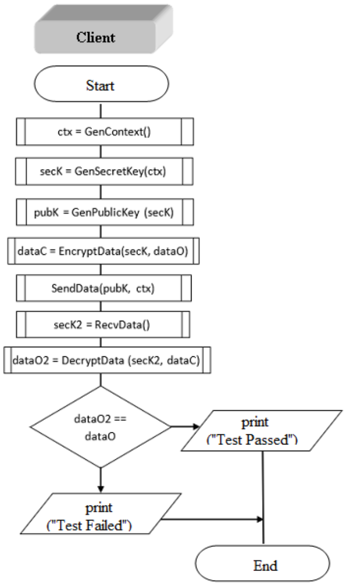

Figure 6. Testing keys during exchange between the client and the ISMS server

The next stage of the testing process was to check the speed of server search for suspicious keywords in a client message. This test is described by the algorithm shown in Figure 7.

A graph in Fig. 8 shows how search speed changes with increasing of data volumes. Theoretically, the search graph should be represented by a logarithmic curve, since it is based on the Binary Raffle Protocol algorithm.

However, given that besides search the results are subject to manipulations, the graph deviates from the theoretical line (deviation does not exceed 5%).

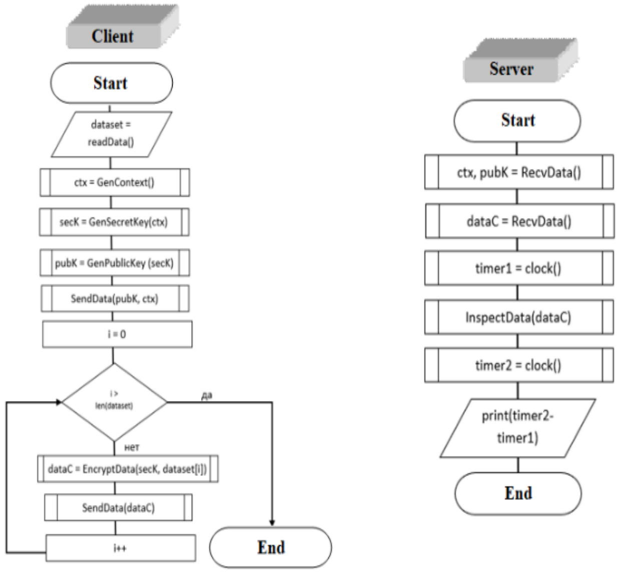

Figure 7. Testing the speed of the search algorithm

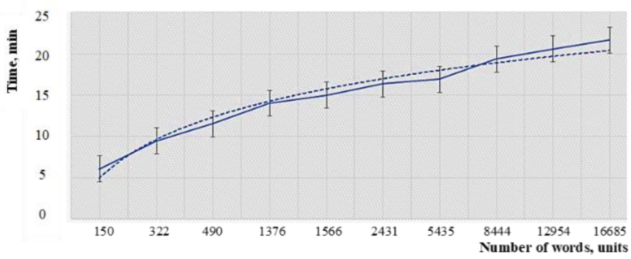

Figure 8. Algorithm running time depending on the number of words

Figure 9 shows the plot of the number of "dangerous" keywords found against the number of such keywords available in data. It can be observed that the error is not permanent but probabilistic. It should also be noted that the user's writing style affects the search of "dangerous" keywords.

Another result of testing was that in some cases certain keywords were not found. The reason is that the homomorphic search scheme uses Monte Carlo probabilistic algorithms, which perform a search based on a set error probability. Here the error value was taken as ε = 2-2, which is the biggest tolerable error for this algorithm.

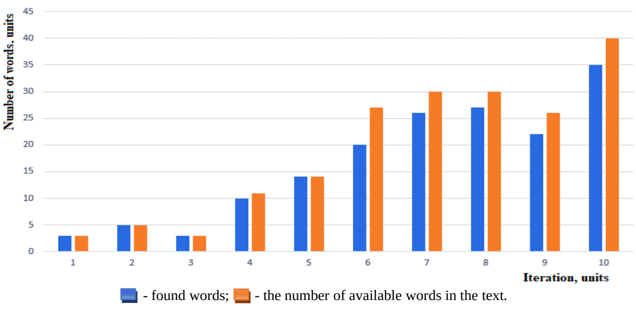

Figure 9. Number of words found and available

The time spent on "dangerous" keywords searching increases with the decrease of error probability. This is not critical when dealing with small data volumes, but as the volume increases, the search speed decreases. However, this does not reduce the practical value of the introduced algorithms for designing dataware and software for storing encrypted data in SISs.

6 DISCUSSION OF RESULTS

The obtained results demonstrate the need to identify [6] and assess risks and identify vulnerable areas of ship systems in terms of information security, encryption of confidential information stored in SISs.

The specific feature of the introduced response plan is that it is easy for ship personnel to understand compared to multi-process and general comprehensive cybersecurity measures. The flexibility of the included procedures allows updating and improving documentation, taking into account new cyber incidents, changes in the state of, for example, ship's power control systems [14], etc.

Further challenges in the development and practical application of this study are related to the lack of public access to information about cyberattacks on each ship, lack of cybersecurity awareness among seafarers, the need to encrypt data stored on ship or company servers, and subsequent erroneous decisions, information leakage. Thus, it creates a problem of incident identification and reduces the quality of systems state monitoring. The difficulty of incident identification and monitoring may arise from the inability to control all connected devices on the ship, risk of ship personnel failure to follow existing security procedures, and lack of response plans that combine shore and sea cyber ecosystems to ensure effective system recovery.

7 CONCLUSIONS

4. The results of the study are based on the analysis of the most dangerous cyberattacks. The survey of international IT specialists showed the lack of awareness among modern companies about protection against cyber threats, dangers associated with leakage of confidential information. Maritime industry practitioners have little knowledge of the complexity of ship and shore information networks. Unintentional actions of the crew were determined to be the most dangerous weakness since it is a seafarer who allows a virus into equipment or clicks on malicious links. The basic response plan introduced in the study allows identifying and assessing risks and can be continuously updated depending on the identified areas of system vulnerabilities.
5. Based on the analysis of existing search engines on encrypted data, the criteria for the development of secure search algorithms for SISs with the use of homomorphic encryption were highlighted. A test search engine on encrypted data was developed, and its main components were identified. Software implementations were made in CLion development environment. The search engine for "dangerous" keywords was tested. The study introduced the solution for further improvement of the algorithm for searching "dangerous" keywords over encrypted data by examining and drawing up "dangerous" keywords rules in order to predict their occurrence in the text, thus allowing taking into account the writing style of each SIS user, reducing the time spent on searching and processing encrypted data. The security of distributed SIS accesskeys was experimentally proved, and the accuracy and speed of searching over encrypted data were determined. The error of the experimental speed curve deviation from the theoretical curve does not exceed 5%.

REFERENCES

1. Apr 19, D.H.K.•, 2020: FBI: Covid-19 Cyberattacks Spike 400% in Pandemic, https://www.msspalert.com/cybersecurity-news/fbi-covid-19-cyberattacks-spike-400-in-pandemic/, last accessed 2022/03/25.
2. Bar-Yam, Y.: General Features of Complex Systems. UNESCO Encyclopedia of Life Support Systems. (2002).
3. Ding, M. et al.: An efficient Public Key Encryption with Conjunctive Keyword Search scheme based on pairings. In: 2012 3rd IEEE International Conference on Network Infrastructure and Digital Content. pp. 526–530 (2012). https://doi.org/10.1109/ICNIDC.2012.6418809.
4. Ferrill, T.: 10 security tools all remote employees should have, https://www.csoonline.com/article/3625882/10-security-tools-all-remote-employees-should-have.html, last accessed 2022/03/25.
5. Goh, E.-J.: Secure Indexes. (2003).
6. Golikov, V.A. et al.: A simple technique for identifying vessel model parameters. IOP Conference Series: Earth and Environmental Science. 172, 012010 (2018). https://doi.org/10.1088/1755-1315/172/1/012010.
7. Kołowrocki, K., Soszyńska-Budny, J.: Reliability and Safety of Complex Technical Systems and Processes. Springer London, London (2011). https://doi.org/10.1007/978-0-85729-694-8_8.
8. Kulesh, S.: NCCC NSDC recorded a new type of DDOS attacks using hacked smart home devices?, https://itc.ua/news/nkczk-snbo-zafiksiroval-novyj-tip-ddos-atak-s-ispolzovaniem-vzlomannyh-ustrojstv-umnogo-doma/, last accessed 2022/03/25.
9. Shumilova, K., Onishchenko, O.: Action planning in comprehensive shipping risk identification. The scientific heritage. The scientific heritage. 49, 1, 40–46 (2020).
10. Tsvetkov, V.Y.: Complex technical systems. International Journal of Applied and Basic Research. 10, 4, 670 (2016).
11. Tugolukov, E.N. et al.: Design of complex systems. Tambov: TGTU (2008).
12. VanMSFT: SQL code injection, https://docs.microsoft.com/ru-ru/sql/relational-databases/security/sql-injection, last accessed 2022/03/25.
13. Volianskyi, Y.: Development of practical implementation of the use of schemes of homomorphic search. Slovak international scientific journal. 48, 1, 7–12 (2021).
14. Volyanskaya, Y. et al.: Determining energy-efficient operation modes of the propulsion electrical motor of an autonomous swimming apparatus. EEJET. 6, 8 (90), 11–16 (2017). https://doi.org/10.15587/1729-4061.2017.118984.
15. Analytical review of the protocols of the Internet of Things, https://www.tssonline.ru, last accessed 2022/03/25.
16. Analytics of the information security industry 2021, https://www.infowatch.ru/analytics/daydzhesty-i-obzory, last accessed 2022/03/25.
17. Attacks on web applications: results of 2018, https://www.ptsecurity.com/ru-

ru/research/analytics/web-application-attacks-2019/, last accessed 2022/03/25.

18. Gaining visibility of your onboard systems: you can’t secure something you can’t see, https://thedigitalship.com/news/maritime-satellite-communications/item/6673-gaining-visibility-of-your-onboard-systems-you-can-t-secure-something-you-can-t-see3, last accessed 2022/03/25.
19. Positive Research Center, https://www.securitylab.ru/lab/, last accessed 2022/03/25.
20. Relevant cyber threats quarter 1 2020, https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/, last accessed 2022/03/25.
21. Ship cybersecurity is in the hands of sailors, https://moryakukrainy.livejournal.com/3843048.html, last accessed 2022/03/25.
22. Vulnerabilities, https://www.securitylab.ru/vulnerability/, last accessed 2022/03/25.