Modeling ship cybersecurity using Markov chains: an educational approach

Nataliia Kaminska[1], Lyudmyla Kravtsova[1], Hennadiy Kravtsov[2] and Tatyana Zaytseva[1]

[1]Kherson State Maritime Academy, 20 Ushakov Ave., Kherson, 73000, Ukraine
[2]Kherson State University, 27 Universytetska Str., Kherson, 73003, Ukraine

Abstract

The strengthening of the role of information in the economy, in particular in transport, is accompanied by the growth of cyber threats. The International Maritime Organization has developed and adopted a number of foundational cybersecurity documents that define requirements for cybersecurity management on board ships. These documents oblige the administration of maritime companies to ensure proper consideration of cyber risks and the application of protection methods in security management systems. The development and establishment of relevant uniform rules is an urgent task for both maritime companies and ships. The most promising direction of ensuring information security is, of course, the use of mathematical models. Such models describe the processes of interaction of a cyberspace violator and the protection system, which should take into account possible cyberattacks on the ship and ensure the preservation and inviolability of the ship's information as much as possible. Analysis of research in the field of building mathematical models of processes taking place in cyberspace shows that, firstly, this is a really relevant research direction, and, secondly, at the moment there are many different theories that form the basis of modeling. The authors of this work propose a new approach to the mathematical modeling of the cyber security management system on the ship, namely, the use of the theory of Markov chains, since a cyberattack on a ship can happen at any random moment, and this event does not always depend on cyberattacks that occurred some time ago. Therefore, a model of the cyber security management system on the ship as a subsystem of the enterprise security management system was built using mathematical modeling methods. Such concepts as the state of cyber security of the ship, the probabilistic relationship between the states, regulation of actions according to the state are defined. The mathematical model of the cyber security management system is based on the model of discrete Markov processes, in which the vertices of the digraph of the Markov chain are the cyber security states of the ship. Connections between the states of the ship's cyber security system were investigated using an expert method. The developed model is illustrated on the example of accounting for the state of cyber security of a ship. The considered methods and technologies of the ship's cyber security system are implemented in the educational process of the Kherson Maritime Academy in the distance course "Cyber security of ship computer systems and networks".

Keywords

cybersecurity in maritime transport, Markov chain model, distance course

1. Introduction

Humanity has entered the stage of development, which is called the "age of information technologies" and is characterized by the growth of the role and value of information. The strengthening of the role of information in the economy, in particular in transport, is accompanied by the growth of cyber threats [1, 2]. The European Union, which wants to strengthen cyber and information security measures in its institutions and business companies, drew attention to this problem. In today's interconnected business environment, a single cybersecurity incident can cause extensive damage to an entire organization. The European Commission points out that the context of the COVID-19 pandemic and growing geopolitical challenges have confirmed the need for a common EU approach to cyber and information security. So the European Commission proposed the corresponding uniform regulations. This point of view is supported by the International Maritime Organization (IMO), which has developed and adopted a

CTE 2023: 11th Workshop on Cloud Technologies in Education, December 22, 2023, Kryvyi Rih, Ukraine
natalikamkam@gmail.com (N. Kaminska); limonova@ukr.net (L. Kravtsova); kgmkherson@gmail.com (H. Kravtsov); zaytseva1966sunny@gmail.com (T. Zaytseva)
0000-0002-9975-7403 (N. Kaminska); 0000-0002-0152-635X (L. Kravtsova); 0000-0003-3680-2286 (H. Kravtsov); 0000-0001-6780-719X (T. Zaytseva)

number of documents on cybersecurity [3]. These documents oblige the administration of institutions and enterprises to ensure proper consideration of cyber risks in security management systems.

The maritime industry needs specialists who can adequately monitor the situation at all facilities that may be targeted by a cyberattack by cybercriminals. One of the requirements related to the aggravation of cybersecurity caused by the total digitalization in all spheres of human activity is to ensure the training of maritime specialists in the basics of cybersecurity on a sea vessel. As emphasized by the IMO, effective cyber risk management must embed a culture of cyber risk awareness at all levels, and ensure a holistic and flexible cyber risk management regime. In June 2017, the IMO Maritime Safety Committee adopted Resolution MSC.428(98) on the management of maritime cyber risks in safety management systems [3]. The resolution calls on the administration of ship companies to ensure the accounting of cyber risks in the existing information security management systems on the ship.

In 2019, the International Chamber of Shipping jointly with BIMCO prepared "The Guidelines on Cybersecurity Onboard Ships. Version 4" [4], which contains general updates of best practices in the field of cyber risk management, and as a key feature includes a section with improved guidance on the concept of risk management. The most significant differences of the fourth version include the inclusion of sections devoted to the participation of top management in cyber risk management; distribution of duties and tasks within the company; quantitative threat assessment; detection of vulnerabilities, including when visiting courts and remote access; assessment of the probability of cyber danger; impact assessment; interrelationships of factors affecting risks; development of detection measures.

In November 2020, the International Chamber of Shipping, in cooperation with BIMCO and Witherbys, released the second edition of the "Cybersecurity Workbook for use on board ships". The workbook provides ship crews with practical tools for identifying cyber threats and protecting vulnerable onboard systems. The International Chamber of Shipping in the workbook considers that at the operational level, the disadvantage of the digital revolution is the growing vulnerability of the operator to cyberattacks. As internet connectivity on board becomes more common, ship systems are increasingly digitized and integrated, and ships are now a target for hackers worldwide, it is critical that the entire crew has an idea of how and when cyberattacks can occur.

The International Organization for Standardization and the International Electrotechnical Commission developed and published the standard ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. This document provides guidance to assist organizations to:

- fulfill the requirements of ISO/IEC 27001 concerning actions to address information security risks;
- perform information security risk management activities, specifically information security risk assessment and treatment.

The Kherson State Maritime Academy is deservedly considered the flagship of maritime education in Ukraine. This status was preceded by very painstaking and long work of the management, teachers, and employees of the academy, connected with the formation of the strategy of its formation, the introduction of a competence approach to the training of marine specialists [5, 6, 7, 8, 9]. The great reward for this is the recognition of academy graduates on the world labor market, their competitiveness and demand by leading crewing companies. But such a level must be constantly confirmed, updating and modernizing both the material and technical base and the sailors' training programs. First of all, this means that the academy bears full responsibility for the level of knowledge, skills and abilities that the graduate received during his studies, taking into account all the latest trends and requirements of international crewing.

2. Relevance of research and problem statement

There are enough articles devoted to the problems of cybersecurity in maritime transport, methods of analysis and forecasting of cybercrimes, the authors of which are, as a rule, experienced sailors who have encountered the problem of protecting and preserving information in practice. Thus, Lahno

[10] emphasized that in order to increase the information security of transport systems, it is necessary to conduct research aimed at the further development of methods and models for recognizing cyber threats to the transport information and communication environment (ICT) and making decisions with vaguely specified input information. The author also offers methods of intelligent recognition of threats on a wide class of tasks of quantitative and qualitative recognition of cyberattacks. As Captain Emil Muccin [11] noted, the US executive branch stated that the cyber threat is one of the most serious problems in the field of economy and national security. Unauthorized access by cybercriminals leads to a new area of potential threats that go far beyond physical piracy. This definitely needs to be recognized and appropriate action taken to assist ship owners and operators in maintaining ship information systems, which also includes an understanding of cyberattack analysis and forecasting techniques. Vilskyi [12], Semenov [13] paid a lot of attention to cybersecurity in maritime transport in their works. Chiappetta [14] provides an overview of the main implications associated with cyber threats and shipping.

Bateman [15] examined security threats and vulnerabilities in the modern shipping industry. In this context, various types of cyberattacks that ships face, as well as real incidents, were discussed. Considered possible countermeasures that can mitigate potential cyberattacks and make the shipping industry more cyber-secure, such as implementing a new security standard that reduces the number and scale of cyberattacks.

The relevance of the issue of cybersecurity is given a lot of attention by the media. For example, the head of the European Crime Agency warned of the growing risk of cyberattacks being used by organized crime groups to enable them to trade drugs [16]. The media reported that in February 2017, hackers took control of the navigation systems of a German-owned 8.250 TEU container ship en route from Cyprus to Djibouti for 10 hours [17].

One of the fundamental studies is the book by Foote [18], which explores cybersecurity in the marine transportation. The article by Coq [19] is devoted to modeling the cybersecurity system in maritime transport.

There are general provisions and standard requirements for the organization of cybersecurity on a ship. But it is the shipping companies that are responsible for ensuring the security of the information system. Therefore, the search and implementation of an effective ship cybersecurity system is an important and urgent task. The purpose of this work is to describe, develop, and implement a ship cybersecurity model into the educational process of the Kherson Maritime Academy.

3. Results and discussion

3.1. Description of the ship's information security system

Today, cybersecurity is one of the priorities in the national security system of Ukraine and the whole world [20, 21, 22]. Operators of ships and port facilities use computers and cyber-dependent technologies for navigation, communication, design, transportation of cargo, ballast, security, environmental control and many other purposes, so the share of cyber risks in the total volume of vulnerabilities faced by the maritime transport system is constantly increasing. This certainly indicates the need for training maritime industry specialists in this direction. Therefore, the list of disciplines of the training program for future sailors includes the course "Cybersecurity of shipboard computer systems and networks", the purpose of which is a comprehensive analysis of the sources of cyber threats, the goals of cyberattacks, methods of forecasting and protection against possible manifestations of danger, as well as improving the safety of sailors, the surrounding environment, ship and cargo. Cybersecurity issues, including in maritime transport, are dealt with by specialized companies, as ignoring or underestimating these issues can lead to loss of trust of potential customers, financial losses, as well as such consequences as physical damage to the ship's security system, loss of confidential information, including commercial or proprietary data, and generally criminal activity, installation of ransomware and much more.

In order to better systematize cases of cyberattacks in the maritime industry, we propose to use a mathematical apparatus that will allow, on the basis of research and mathematical calculations, to

determine the state of the ship's information security based on a probabilistic approach to modeling the occurrence of cyber threats taking into account their types.

First, we need to decide which of the system modules that can be attacked by attackers, we will investigate. Therefore, we will conduct a structuring of cybersecurity according to the degree of its consequences, the goals of cyberattacks, and their sources. At the same time, an important element in this process is the human factor, since most incidents are initiated by the actions of the ship's personnel. But it must be emphasized that the adjustment of the ship's control systems, its Internet networks, monitoring of cyberattacks of any direction are handled by special services, highly qualified specialists who have access to all systems and the appropriate authorization for actions aimed at preventing cyberattacks or eliminating their consequences. The aim of the specified course "Cybersecurity of ship computer systems and networks" is to teach future sailors elementary rules of conduct related to the use of Internet networks on ships, interfaces of cargo management systems, bridge systems, ship traffic management systems, as well as the operation of ship communication systems systems vulnerable to external cyberattacks.

The International Maritime Organization refers to cyber-vulnerable ship systems [3]:

- running bridge systems;
- cargo handling and management systems;
- engine, machine and power supply control systems;
- access control systems;
- passenger service and management systems;
- ship's public Internet networks intended for use by passengers;
- administrative systems and networks;
- communication systems.

That is, the fact of the ship's great vulnerability to a planned attack is obvious.

First of all, let's list the most common cyber vulnerabilities that can be identified both on board already existing and some new ships:

- outdated and non-updated operating systems;
- outdated or completely missing anti-virus software and anti-malware software;
- ineffective network management and use of administrator accounts and passwords;
- shipboard computer networks that do not have means of border protection and network segmentation;
- danger from safety-critical equipment or systems connected to shore systems;
- lack or incomplete access control for third parties, including contractors and service providers.

But the global threat is defined by cyberattack vectors through or in the maritime environment.

We emphasize that the indicated problem belongs to the field of activity of MTS specialists, that is, the maritime transport system, but the management of each sea vessel and its crew must have a clear idea of all sources and channels of cybersecurity.

This area includes:

- work with ships, which is provided by operational networks of ship management, cargo, navigation and communication systems, other specific functions;
- ensuring the operation of external and internal networks, such as company websites, portals for customers and partners, reservation systems and other commercial operations;
- personnel management, robot and maintenance schedules, legal support and much more;
- a huge range of port operations, such as management of ships entering or leaving the port; control of the work of customs services, immigration, logistics and inventory services;

- management of the flow of ships in ports, canals, systems for determining the location of the ship, navigation and time and many other functions that ensure the safe and efficient movement of ships, cargo, passengers.

Each of the listed points is potentially dangerous from the point of view of the probability of cyberattacks. For example, if a ship carrying a dangerous cargo such as oil, liquefied gas falls under the control of cybercriminals, the consequences can be irreversible. This means that if the ship's management or one of the crew members notices some inconsistencies in the operation of the ship's system or the surrounding transfer of ships, it is necessary to immediately inform the management about the incident.

We will remind that cybersecurity can be defined as a certain superposition of security concepts, policies, management principles, risk management, actions, training, technology, practices, that is, everything that can be used to protect the cyber environment of the existence of the system, taking into account the interest of the organization and the preservation of its assets. A well-planned and implemented cyber defense protects not only the organization's own systems, but also all systems with which the organization's data comes into contact.

The motivation of a cyberattack on a ship system can be schematically presented as follows (figure 1).

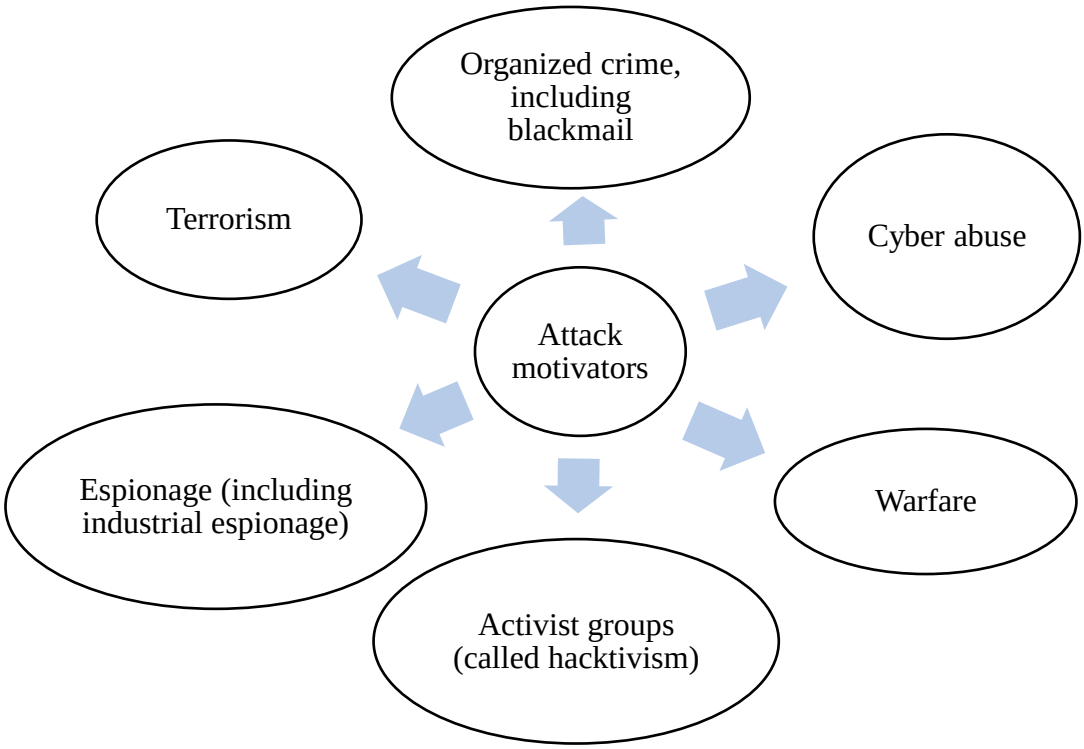


Figure 1: Motivation of a cyberattack on a ship system.

Let's focus on such a widespread and most frequently occurring phenomenon as the misuse of cyberspace, that is, cyber abuse, which includes low-level criminal activities, including vandalism, disruption of systems, damage to websites and unauthorized access to the system. Such actions can be carried out both by not very experienced specialists and by insiders, i.e. employees who have the right to access confidential information of this organization, or by staff or contractors who are dissatisfied for some reason; researchers still get access to the information system without the sanction of the system manager. Although such actions may not always carry any malicious intent, it may be a lack of necessary legal knowledge or ordinary curiosity, but according to the law such actions are considered a criminal offense.

It should be noted that cyberattacks, as a rule, are carried out in stages. The preparation of a cyberattack takes some time, which is determined by the attacker's goal, the reliability of technical

means of cyber risk control, and the degree of updating of the software of the ship's systems. An experienced, trained specialist, who is not a professional system administrator, is nevertheless able to detect criminal attempts, track the most vulnerable key positions and, based on the analysis of the received information, draw conclusions about some criminal interest in the cybersecurity of the ship and its support systems. This will allow you to predict more serious cyberattacks in advance and save time and costs for updating the system.

So, let's assume that the specialist responsible for the cybersecurity of the ship monitors several positions, based on the analysis of which it is possible to claim about attempts to carry out cyberattacks on the ship. First, it can detect the presence of an email from an unknown sender. Such email may contain malicious files or links to malicious websites. Secondly, an experienced specialist will never use the ship's or own computer to communicate on social networks, technical forums, etc., but team members can ignore the ban and open suspicious sites, so it is necessary to track which sites were opened on board the ship with any device. Third, the specialist periodically monitors fake or malicious sites that force or encourage personnel to disclose confidential information.

The specialist responsible for cybersecurity also carries out control of external media that can be used to update the software of the onboard system, as well as a mandatory check of the actual data arriving on the ship or transmitted from the ship to the shore.

If an attacker gains access to the system in one way or another, he will try to exploit the entire system in stages. This will lead to an attempt to download scripts, exploits, network scans. In turn, it can install persistent tools or a system access logger.

3.2. Security model of the ship's information system

From the point of view of the theory of random processes, a cyberattack (in any form) is a continuous random variable, because it can happen at any moment. But control by the CySO (Cybersecurity officer) is carried out periodically according to the established schedule, that is, discretely, which indicates the discreteness of the monitoring results. Of course, for a certain period, statistical information is accumulated about all cases of cyberattacks that were detected and tracked. Analysis of this information will help to predict the appearance of the next cyberattack and, if possible, to take measures to prevent it.

A careful analysis of the sources of cyberattacks, which occur most often, allows us to assume that this is a random process that obeys the laws that are called Markov processes in the theory of probabilities (or, more precisely, stochastic processes) [23]. By definition, a Markov process is a random process for which the "future" depends only on "today" and does not depend on "yesterday", i.e., a random process is called a Markov process (or a process without an aftereffect) if for each moment of time t the probability of any state of the system in the future depends only on its state at the present time and does not depend on how the system came to this state.

So-called Markov chains are robust and widely known stochastic modeling tools that can be useful to expert analysts.

Therefore, a random variable X is considered to be a variable determined as the result of a random phenomenon. In our case, the result of the event may be detection of interference in the information system, loss of data (full or partial), failure of the system or its elements. In general, the space of possible results of the implementation of a random variable can be discrete or continuous, depending on this, its behavior corresponds to one or another distribution law, for example, normal (continuous random variable) or Poisson (discrete random variable).

A random process, which is otherwise called stochastic, is defined as a set of random variables that can be represented in the form of an indexed one-dimensional array T, the elements of which are the time moments of the occurrence of an event. If this array is the set of natural numbers, then we have a discrete-time random process, otherwise it will be a continuous-time random process.

Random variables may or may not be dependent on each other at different points in time. Yes, cyberattacks can be carried out by completely different criminals, both individually and by organized, highly qualified groups. But it is also possible that someone carried out a cyberattack, but was not

detected and punished for this crime, so this person will carry out such attacks in the future, and each time improving the methods of attacks and deploying their goals.

In the theory of random processes, various types of models have been studied and are widely used: Gaussian, Poisson, auto-regression, Markov chains, and many others. The choice of the model necessarily corresponds to the essence of the phenomenon under study, an in-depth analysis of its characteristic features, statistical analysis of numerical results. The built model allows you to study the process in more detail, perform analysis and forecast the development of the event, and make a management decision on further constructive actions in a timely manner.

A careful analysis of cybersecurity problems on sea vessels allowed us to assume that the results of observations are subject to the properties of discrete Markov processes. This means that in order to determine the forecast regarding the behavior of the process in the future, there is enough information about the current state of this process, that is, data on its behavior in the past will in no way affect the forecast of the future. It can also be noted that in order to determine the forecast and understand the trend, it is not necessary to have any information about the past. Otherwise, this is called the "out of memory" property.

Thus, discrete-time homogeneous Markov chains, or simply Markov chains, are Markov processes with discrete time and discrete state space. Otherwise, a Markov chain is a discrete sequence of states, each of which is obtained from a discrete state space, which can be finite or infinite, and satisfies the corresponding properties.

Mathematically, we define a Markov chain as follows:

$$X = (X_n) = (X_0, X_1, X_2, \dots, X_n), n \in \mathbb{N},$$

where at each moment of time the process takes a value from a discrete set E such that $X_i \in \mathbb{E}, \forall i \in \mathbb{N}$. Then the sequence of states can be determined by the following ratio:

$$P(X_{n+1} = s_{n+1} | X_n = s_n, X_{n-1} = s_{n-1}, \dots) = P(X_{n+1} = s_{n+1} | X_n = s_n).$$

That is, such a mathematical description reflects the basic essence of the Markov process: the probability distribution of the next state of the system depends only on its current state, but does not depend on the past state.

Of course, at this stage of research, we believe that the process under consideration is a simple homogeneous Markov chain with discrete time. In the course of future research, we will add additional characteristics of the system that more fully describe it, thereby expanding the probabilistic description of the model.

Thus, it is possible to characterize the probability dynamics of the Markov chain. For this, we define only two aspects: the initial probability distribution, that is, the probability distribution at the time $n = 0$, namely, $P(X_0 = s) = q_0(s), \forall s \in \mathbb{E}$, and the transition probability matrix, which provides information about the following states are possible, which can be defined as

$$P(X_{n+1} = s_{n+1} | X_n = s_n) = p(s_n, s_{n+1}) \forall (s_{n+1}, s_n) \in \mathbb{E} \times \mathbb{E}.$$

Such a description allows you to determine the full dynamics of the entire process, which, in fact, is cyclical.

In our case, we will investigate four positions of possible cyberattacks on the system that can be detected during system monitoring. According to the model, it is necessary to determine the probability that the system takes the following state: s_0, s_1, s_2, s_3. Then the formal description of the state will have the following form:

$$P(X_0 = s_0, X_1 = s_1, X_2 = s_2, X_3 = s_3),$$

that is, the result will be the probability of a system's cybersecurity based on an analysis of its previous state.

From the probability theory course, it is known that the formula for the full probability of obtaining the state s_0, s_1, s_2, s_3 takes into account the probability of the next state occurring, provided that the

previous state was realized. But the assumption that the process can be defined as a Markov chain greatly simplifies mathematical calculations, without violating the main trends of the development of events. Then the probabilistic dynamics of the process has the form:

$$P(X_0 = s_0, X_1 = s_1, X_2 = s_2, X_3 = s_3) = P(X_0 = s_0)P(X_1 = s_1 \mid X_0 = s_0).$$

$$P(X_2 = s_2|X_1 = s_1)P(X_3 = s_3|X_2 = s_2) = q(s_0)p(s_0, s_1)p(s_1, s_2)p(s_2, s_3).$$

In this way, it is possible to obtain the full probabilistic dynamics of the process only on the basis of the initial probability distribution q_0 and the transition probability matrix P, that is, the probability distribution at time $n + 1$ relative to the probability distribution at time n:

$$q_{n+1}(s_{n+1}) = P(X_{n+1} = s_{n+1}) =$$

$$= \sum P(X_n = s)P(X_{n+1} = s_{n+1}|X_n = s) = \sum q_n(s)p(s, s_{n+1}), s \in \mathbb{E}$$

Markov chains obey all the rules of actions with matrix forms. If the set of possible final states of the system N is represented as a string vector $E = e_1, e_2, \ldots, e_N$, then the transition probabilities can be represented by an $\mathbb{N} \times \mathbb{N}$ matrix, so that

$$(q_{0,i}) = q_0(e_i) = P(X_0 = e_i)$$

$$p_{i,j} = p(e_i, e_j) = P(X_{n+1} = e_j|X_n = e_i)$$

In other words, with such a description of the process, to obtain relationships between the current and next state of the system, you can use ordinary matrix forms and, accordingly, ordinary actions on matrices, for example, in our case, the rule

$$q_{n+1} = q_n p, q_{n+2} = q_{n+1}p = (q_n p)p = q_n p^2, \ldots, q_{n+m} = q_n p^m.$$

Obviously, such a representation greatly simplifies the process of forecasting the situation, that is, cyberattacks on the ship's information system based on probabilistic data analysis at the present time.

For clarity, you can use the form of the connection in the form of a normalized directed graph, where each node defines a state, and the transition from state i to state j characterizes the probability P_{ij} of the occurrence of such an event (figure 2).

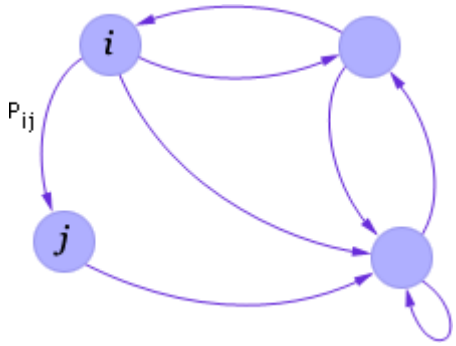


Figure 2: Example graph of the transition from state i to state j.

Consider the generally accepted 4 states of the ship's cybersecurity system $E = (s_0, s_1, s_2, s_3)$, where state s_0 is safe (green zone), state s_1 is the existence of a cyber-threat or cyber vulnerability (yellow zone), state s_2 is the existence of a risk of a cyberattack (orange zone), state s_3 – the presence of a cyberattack (red zone). In accordance with the state of the ship's cybersecurity, the procedure for ensuring it, as well as interaction with the shipping company, is regulated.

Let's consider the states of the ship's cybersecurity system regulated by the Guide on cybersecurity on board ships [13]:

1. **Threats**. In general, there are two categories of cyber threats that can affect companies and courts:
    - untargeted attacks, in which the company or ship systems and data are one of many potential targets,
    - targeted attacks, when the intended target or one of several targets is the company or the ship's systems and data.

Untargeted attacks will most likely use tools and methods available on the Internet that can be used to detect and exploit widespread vulnerabilities that may also exist in the company and on board the ship.

Targeted attacks can be more sophisticated and use tools and methods specially designed to attack a specific company or ship.

2. **Vulnerabilities**. The following are common cyber vulnerabilities that can be found aboard existing ships and some new ships:
    - outdated and unsupported operating systems,
    - uncorrected or unlicensed system software,
    - outdated or missing anti-virus software and anti-malware software,
    - inadequate security settings, including inefficient network management and careless use of accounts and passwords,
    - safety-critical equipment or systems connected to the shore,
    - insufficient control of access to cyber assets, networks, etc. for third parties, including contractors and service providers.
3. **Risks**. Risk assessment of the presence of cyber threats and vulnerabilities can be carried out both by IT specialists on the ship and by the company, which owns the ship. At the same time, it is possible to include penetration tests in critical IT infrastructure to determine whether the actual level of protection corresponds to the desired level specified in the company's cybersecurity strategy.
4. **Attacks**. A cyberattack is an attempt to disable an information system or steal information due to a vulnerability in the device or software. There are several types of cyberattacks:
    - phishing,
    - installation of malicious software,
    - the use of encryption viruses,
    - DDoS and others.

The safety model of the ship's information system using Markov chains is presented in figure 3.

Here, the states of the system $E = (s_0, s_1, s_2, s_3)$ are connected to each other by the transition probabilities P_{ij}, where $i = 0, 1, 2, 3$, $j = 0, 1, 2, 3$. The transition probabilities P_{ij} are set parameters of the model. If the ship company does not define the values of the transition probabilities of the matrix P_{ij}, then an expert method can be used to determine them [24].

3.3. An example of cyberattack analysis and forecasting

So, according to the proposed model, consider the state space of the ship's cybersecurity system as a string vector $E = (s_0, s_1, s_2, s_3)$. Suppose that the system is in the yellow zone, the current information about the events, that is, the probability distribution vector, has the form (based on the previous analysis): $q_0 = (0.3, 0.5, 0.1, 0.1)$, that is, with a probability of 0.3, the return probability was detected in the green zone, with a probability of 0.5, the fact of leaving the system in the yellow zone was recorded, with a probability of 0.1, a transition of the system to the orange zone was detected, and with a probability

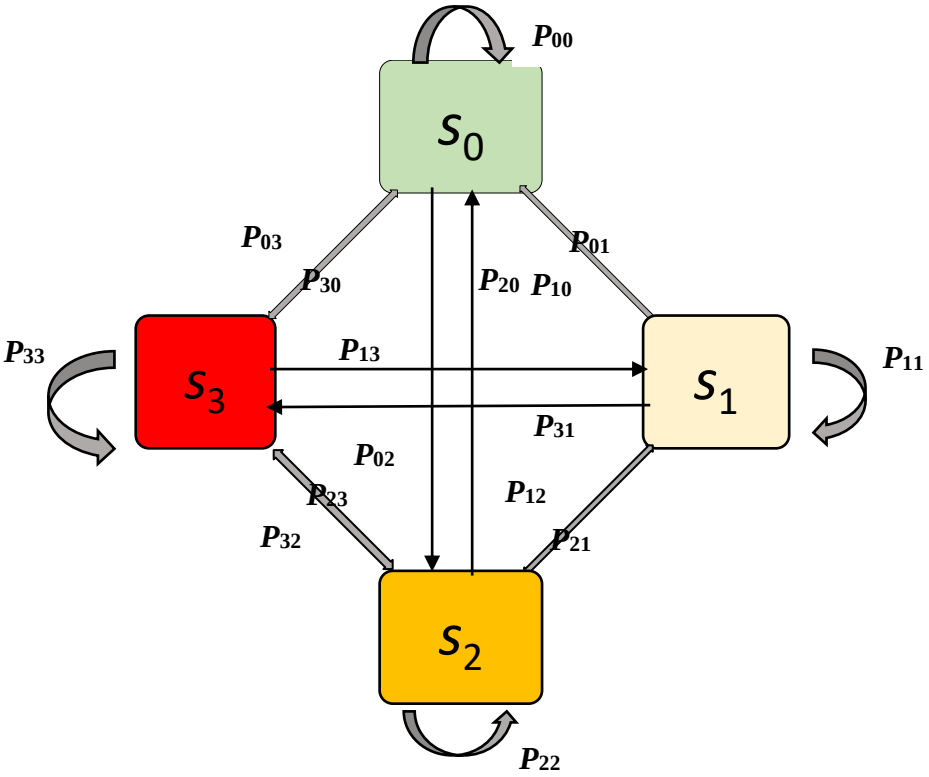


Figure 3: Security model of the ship's information system.

of 0.1, cyberattacks on the ship's information security system were expected. The transition matrix provides information about the probabilities of changing the state of cybersecurity:

$$p = \begin{pmatrix} 0.6 & 0.2 & 0.1 & 0.1 \\ 0.4 & 0.4 & 0.1 & 0.1 \\ 0.2 & 0.3 & 0.3 & 0.2 \\ 0.2 & 0.3 & 0.3 & 0.2 \end{pmatrix}$$

Recall that each line of the matrix is the possible probabilities of events according to the investigated states, the sum of the values in each line is equal to one, that is, the probability of a reliable event. Then, according to the rules of actions with matrix forms, we determine the probability of each state $E = (s_0, s_1, s_2, s_3)$ for the next day:

$$q_1 = q_0 p = (0.3, 0.5, 0.1, 0.1) \begin{pmatrix} 0.6 & 0.2 & 0.1 & 0.1 \\ 0.4 & 0.4 & 0.1 & 0.1 \\ 0.2 & 0.3 & 0.3 & 0.2 \\ 0.2 & 0.3 & 0.3 & 0.2 \end{pmatrix} = (0.42, 0.32, 0.14, 0.12)$$

i.e. with a probability of 0.42 you can expect the system to return to the green zone, with a probability of 0.32 the system remains in the yellow zone, with a probability of 0.14 the system will move to the orange zone and with a probability of 0.12 you should expect a cyberattack on the ship's information security system. Thus, it is most likely to return to the green zone. The probability of remaining in the yellow zone is significant.

Let's pay attention to the fact that the sum of the values of the result line is equal to 1, that is, the probabilistic laws are indeed subject to the laws of matrix algebra. The obtained result makes it possible to predict cases of cyberattacks at the next moment in time, to carry out appropriate work in advance and to warn of possible interventions by intruders.

Let's present the transition matrix more clearly graphically, which makes it possible to visually assess the probability of a change in the state of the ship's cybersecurity system (figure 4).

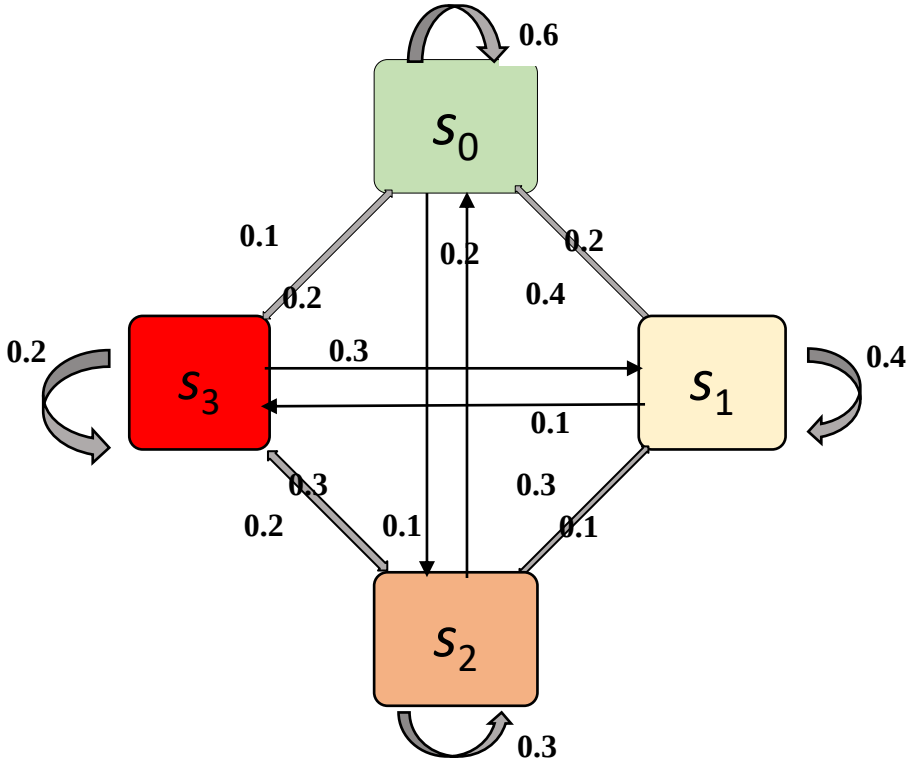


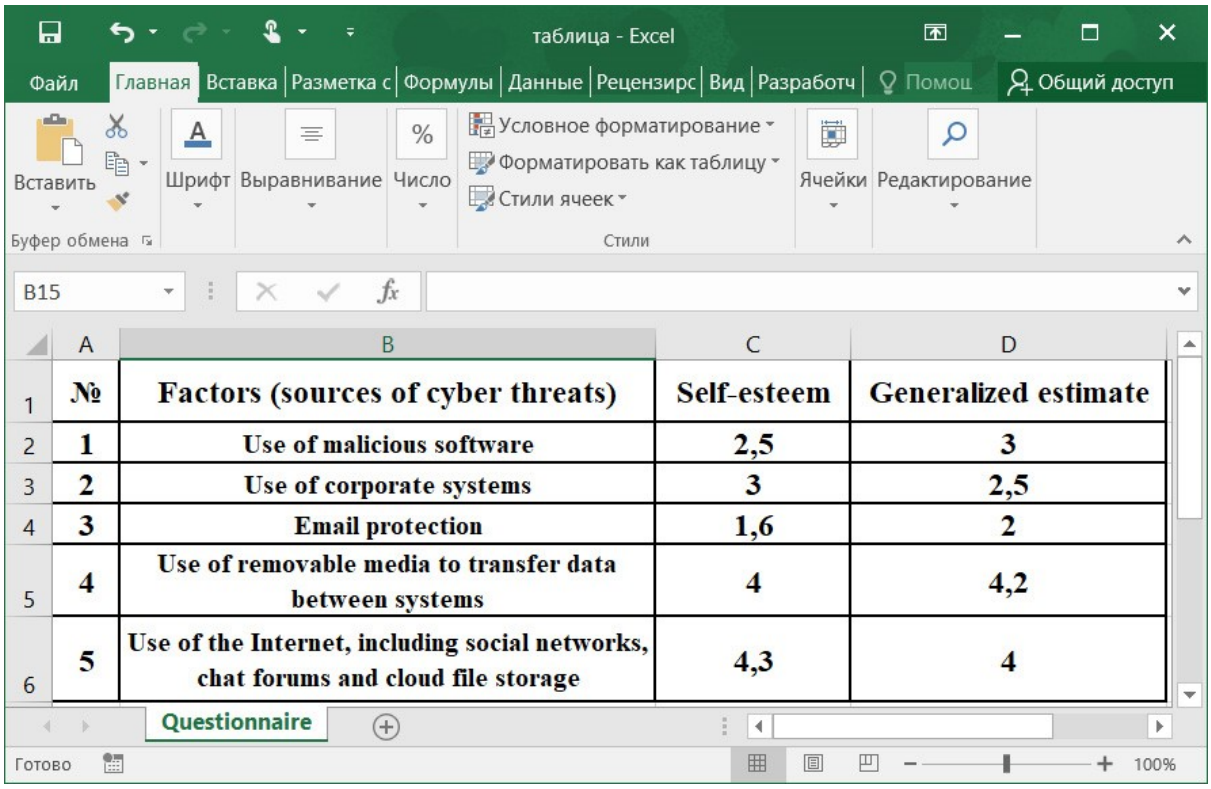
Figure 4: Graphic representation of the transition matrix.

Using the properties of Markov chains, it is possible to reveal interesting and useful results of process research. Yes, it is easy to prove that in our example the chain is aperiodic, does not decompose and all its states are positively inverse. This allows you to calculate the period of return to the current state, that is, for any initial state, the process receives a stationary distribution.

4. Introduction of ship cybersecurity methods and technologies into the educational process

The provided model is implemented in the lecture part of the distance course "Cybersecurity of ship computer systems and networks" [25].

Understanding the importance of ensuring the cybersecurity of the maritime industry, the leading teachers of the Department of Innovative Technologies and Technical Devices of Navigation offered Masters of Shipping subjects of qualification works that are specifically related to the provision of cybersecurity in maritime transport. Masters, especially part-time students, professional sailors who already have sufficient experience working on sea vessels, deliberately chose scientific topics that are currently relevant for those who apply for a leadership position in this field. But for the researchers, the participation of active sailors-shipmasters is also an important factor, as it provides an opportunity to analyze the state of cybersecurity of the ship's information systems directly based on the experience of shipmasters, to understand in detail the most vulnerable objects on the ship from the point of view of cyberattacks, and to prepare students of higher education as best as possible to work as an officer in the ship's crew. It must be noted that according to the plan for the preparation of the diploma thesis, the master's student, being on a flight, i.e. on a ship, must conduct an experiment, the results of which either confirm a scientific hypothesis or refute it. In this work, the hypothesis is that it is possible to mathematically predict the occurrence of an event related to a cyberattack on a ship system. In particular, several master's students, with the permission of the ship's management, were asked to survey crew members about their awareness of possible cyberattacks and methods of countering such



№	Factors (sources of cyber threats)	Self-esteem	Generalized estimate
1	Use of malicious software	2,5	3
2	Use of corporate systems	3	2,5
3	Email protection	1,6	2
4	Use of removable media to transfer data between systems	4	4,2
5	Use of the Internet, including social networks, chat forums and cloud file storage	4,3	4

Figure 5: Fragment of the questionnaire for testing the ability of crew members to protect against external cyber attacks.

phenomena (figure 5).

The results of surveys conducted on different ships with different crews allow to systematize the main mistakes in the use of innovative technologies from the standpoint of their cybersecurity, and to correct the influence of the human factor on the part of the crew to improve the quality of protection against cyber threats during the voyage.

5. Conclusions

The authors of the paper proposed a new approach to the mathematical modeling of the cybersecurity management system on the ship, namely, the use of the theory of Markov chains. Cybersecurity was structured according to the degree of its consequences, the goals of cyberattacks, and their sources. Cases of cyberattacks in the maritime industry have been systematized, based on the analysis of which it is possible to assert the types of attempts to carry out cyberattacks on the ship. It is also determined that in the process of carrying out cyberattacks on a ship, the human factor is an important element, since most incidents are initiated by the actions of the ship's personnel. A mathematical method was used, which made it possible, based on research and mathematical calculations, to determine the state of information security of the ship based on a probabilistic approach to modeling the occurrence of cyber threats, taking into account their types.

The cybersecurity system of the ship is described and a model of the cybersecurity of the ship information system is built based on homogeneous Markov chains in discrete time. Four ship cybersecurity states are proposed. Connections between the states of the ship's cybersecurity system were investigated using an expert method. The model is illustrated by an example of a concrete implementation.

The proposed model is implemented in the educational process of the Kherson State Maritime Academy. The distance course "Cybersecurity of ship computer systems and networks" has been developed.

At the next stage, it is planned to expand the range of sources of cyber threats, which will allow to

improve the regulatory actions of crew members in accordance with the state of the ship's cybersecurity system, as well as to conduct a full analytical study of the possibility of creating a cybersecurity space on board the ship.

References

[1] O. Y. Burov, O. P. Pinchuk, A meta-analysis of the most influential factors of the virtual reality in education for the health and efficiency of students' activity, Educational Technology Quarterly 2023 (2023) 58–68. doi:10.55056/etq.435.

[2] A. I. Jony, A. K. B. Arnob, A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset, Journal of Edge Computing (2024). doi:10.55056/jec.648.

[3] IMO, Maritime cyber risk management in Safety Management Systems, 2017. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

[4] M. K. Fraende, Industry publishes new and improved cyber security guidelines, 2020. URL: https://www.bimco.org/news/priority-news/20201223-new-cyber-security-guidelines.

[5] O. O. Dobroshtan, Introduction of cloud computing technologies into the educational process of higher maritime educational institutions, CTE Workshop Proceedings 1 (2013) 125–126. doi:10.55056/cte.162.

[6] M. S. Lvov, H. V. Popova, Simulation technologies of virtual reality usage in the training of future ship navigators, Educational Dimension 1 (2019) 159–180. doi:10.31812/educdim.v53i1.3840.

[7] M. Sherman, A. Yurzhenko, Experimental research on the formation of future ship engineers' communicative competence based on gamification approach, Educational Dimension 3 (2020) 251–266. doi:10.31812/educdim.v55i0.3939.

[8] S. A. Voloshynov, I. M. Riabukha, O. O. Dobroshtan, H. V. Popova, T. S. Spychak, Adaptive learning environment design in the system of future maritime specialits' training, Educational Dimension 5 (2021) 126–143. doi:10.31812/educdim.4722.

[9] L. V. Kravtsova, T. V. Zaytseva, O. M. Bezbakh, H. M. Kravtsov, N. H. Kaminska, The optimum assessment of the information systems of shipboard hardware reliability in cloud services, CTE Workshop Proceedings 9 (2022) 200–215. doi:10.55056/cte.115.

[10] V. Lahno, Ensuring of information processes' reliability and security in critical application data processing systems, MEST Journal 2 (2014) 71–79. doi:10.12709/mest.02.02.01.07.

[11] E. Muccin, Combatting Maritime Cyber Security Threats, 2015. URL: https://www.marinelink.com/news/combatting-maritime393435.

[12] G. B. Vilskyi, Informational risks of navigation, Scientific Bulletin of KhDMA 1 (2012).

[13] S. Semenov, Cybersecurity in the fleet, Maritime security service 1 (2018).

[14] A. Chiappetta, Hybrid ports: the role of iot and cyber security in the next decade, Journal of Sustainable Development of Transport and Logistics 2 (2017) 47–56. doi:doi.org/10.14254/jsdtl.2017.2-2.4.

[15] T. Bateman, Police warning after drug traffickers' cyberattack, 2013. URL: https://www.bbc.com/news/world-europe-24539417.

[16] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos, Cybersecurity challenges in the maritime sector, Network 2 (2022) 123–138. URL: https://www.mdpi.com/2673-8732/2/1/9.

[17] T. Blake, Hackers took 'full control' of container ship's navigation systems for 10 hours – IHS Fairplay, 2017. URL: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay.

[18] R. Foote, Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities, and Vessels Safe from Cyber Threats, Cybaris® 8 (2017) 3. URL: https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1073&context=cybaris.

[19] T. Coq, Cybersecurity by design, 2018. URL: https://www.dnv.com/maritime/publications/paper-security-by-design-complex-vessels/.

[20] D. V. Stolbov, Features of development software for teaching secondary school students the internet security, CTE Workshop Proceedings 3 (2015) 131–134. doi:10.55056/cte.255.

[21] T. Vakaliuk, I. Pilkevych, D. Fedorchuk, V. Osadchyi, A. Tokar, O. Naumchak, Methodology of monitoring negative psychological influences in online media, Educational Technology Quarterly 2022 (2022) 143–151. doi:10.55056/etq.1.

[22] N. M. Lobanchykova, I. A. Pilkevych, O. Korchenko, Analysis and protection of IoT systems: Edge computing and decentralized decision-making, Journal of Edge Computing 1 (2022) 55–67. doi:10.55056/jec.573.

[23] R. Serfozo, Basics of Applied Stochastic Processes, Probability and Its Applications, Springer, Berlin, Heidelberg, 2009. doi:10.1007/978-3-540-89332-5.

[24] M. G. Kendall, Rank correlation methods, Griffin, 1948. URL: https://psycnet.apa.org/record/1948-15040-000.

[25] Distance learning course “Cybersecurity of ship computer systems and networks”, 2023. URL: https://mdl.ksma.ks.ua/course/view.php?id=4029.