ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse14932020.pdf
https://doi.org/10.30534/ijatcse/2020/14932020

The Model to finance the Cyber Security of the Port Information System

Lakhno V.A.[1],Malyukov V.P.[2], Satzhanov B.[3], Tabylov A.[4], Osypova T. Yu.[5], Matus Yu.V.[6]
[1]National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine, lva964@gmail.com
[2]National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine, volod.malyukov@gmail.com
[3]Department of Maritime and land transport, Caspian state university of technology and engineering named after SH. Essenov, Aktau, Kazakhstan, Satzhanov1959@mail.ru
[4]Department of Maritime and land transport, Caspian state university of technology and engineering named after SH. Essenov, Aktau, Kazakhstan, abzal.tabylov@bk.ru
[5]National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine, t_osipova@nubip.edu.ua,
[6]National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,umatus@ukr.net

ABSTRACT

The article presents a model for the module of the computer system for supporting solutions in the process of analysis and selection of rational financing strategies in the means of cyber security of the port information system. The model is based on the tools of the theory of multi-step games. In the course of the study, a solution was obtained enabling the person making the decision to adequately assess the financial risks associated with the loss of financial resources, if the strategy was chosen erroneously. A theoretical solution of a bilinear multistep game of quality with several terminal surfaces is performed. The results of experiments performed in the course of checking the adequacy of the model and its operability are exemplified by the example of choosing a rational financing strategy in the means of cyber protection of the port information system in the seaport of Aktau (Kazakhstan). It is established that the proposed solution for the system of supporting decisions in the field of financing of cyber security means of port information infrastructures allows removing uncertainty when accounting for the financial components of cyber defense strategies at any ratio of parameters describing the financing process.

Key words: Port information systems, cybersecurity, game theory, multi-step game of quality, financing strategies, risks, solution support system.

1. INTRODUCTION

A huge resource of cybernetic and telecommunication facilities is concentrated at the objects of maritime infrastructure [1]. These funds are designed to address a variety of functional tasks in water transport management systems, freight turnover, organizational and economic planning, etc. [1, 2]. One of the most complex components of this infrastructure is the port information system (PIS) [1, 3]. The objects of cybersecurity of PIS are [3, 4]: information content, technical means of data collection, storage and transfer, premises in which hardware and software facilities are located, etc. Features of the objects subject to cyber protection in many ports are the territorial distribution of PIS elements. In addition, PISs unite in a single system a large number of various technical means with a high intensity of information flows between modules and a variety of categories of users.

The realities of operation of offshore facilities and companies, including PISs of large ports, have shown the need to create an effective tool for supporting decision-making on the financing of cybersecurity means for such port infrastructures. In this sense, the urgency of developing the necessary tools - the solution support system (SSS) for financing cybersecurity PIS is expedient in the form of a special software application adapted for a specific task. This will improve the effectiveness of decision-making by port management and relevant services responsible for cybersecurity and security of information that is processed and stored in PIS. In the face of the increasing complexity of cyberattack scenarios for information infrastructures in maritime transport, including PISs, one of the most important tasks, facing the exploitation services, is the task of ensuring their cyber protection. One of the options for solving the problem associated with the assessment of risks in the process of financing PIS cyber defense is the implementation of the SSS [5, 6]. Such systems allow making rational decisions on investing financial resources in the cyber defense of PIS.

2. REVIEW AND ANALYSIS OF PREVIOUS STUDIES

Many studies [1, 3, 4, 7] indicate that enough attention is not given to cybersecurity of PISs and port IT

infrastructure, in particular, telecommunication systems (TCS).

In this study, the game theory apparatus is used, namely, a multi-step quality game [8]. The following designations have been adopted: $(P1)$ –Protector of PIS and TCSs of the port (player No. 1); $(P2)$ – computer attacker (player No. 2 –hacker). In the process of solving the problem, there are many strategies of players 1 and 2. Accordingly, the defender analyzes the possibility of investing his financial resources in the cybersecurity of PIS and TCS of the port (hereinafter all the text is all – PIS), and the hacker has the opportunity to overcome the boundaries of protection with the help of its financial resources. Given two terminal surfaces, for the defender and the hacker, respectively [7, 8]. The goals of the defender and hacker lead the dynamic system with the help of their management strategies to their terminal surface. We believe that the financial strategy is chosen by the hacker at will and does not depend on the defender's financial strategies. If the interaction time of players 1 and 2 is limited to one step, then the solution obtained can be referred to one-step games in the class of mixed strategies [8,9].

3. THE PURPOSE

In [1-3] it is noted that many companies represented in the market of informatization and automation in the maritime segment are forced to pay close attention to the cyber defense of IT infrastructure from hacking by intruders. In [4, 5] it was shown that the decision to finance cybersecurity in maritime transport is a constant task. However, the lack of many works, and in particular [10-12], is the lack of realistic recommendations for developing strategies for financing the cyber security of IT infrastructures in maritime transport. In particular, there are no studies suggesting models that take into account strategies for active financial counteraction to hackers who can attack PISs. A separate direction is the work devoted to the application of various expert [13] and solution support systems [14, 15] for the selection of financing strategies for cybersecurity in various fields [10], and in transport, in particular [6]. The drawback of these studies [13, 12] is the lack of unambiguous modeling results. Many models [14, 15] do not allow finding effective recommendations and strategies for financing cybersecurity means for complex information objects, in particular PISs. The models proposed in [14-17] also do not allow assessing the risk of losing financial resources by the side of cyber defense. Models based on game theory for evaluating financing in cybersecurity systems were proposed in [14, 18-20]. However, the authors do not take into account many factors, for example, the change in the financial components of the attacking party. Eliminate this shortcoming in previous studies of different authors; it is possible due to the application of methods of the theory of differential and multi-step games of quality with several terminal surfaces [21, 22].

This will improve the effectiveness of forecast calculations for assessing the risks of financial losses in cybersecurity. Thus, as the analysis of the performed studies has shown, the problem of further development of models for SSS in the tasks of financing PISs as one of the components of critical infrastructures of many states remains relevant [1, 4, 5].

4. METHODS AND MODELS

As it was shown in the introduction, the PIS defender needs financial resources. The attacking party (hacker) can also attract financial resources to hack into the components of PISs. For example, in 2012, hackers [1] used special scanners to read 9-character PIN codes, which are used to carry out operations with containers in DP World systems [1, 2].

The following variables are used:

$x1(0)$ – financial resource of the defender of PIS;

$x2(0)$ – financial resource of hacker;

S_1 – set of initial states $(x1(0), x2(0))$ of financial resources of the PIS defender and hacker;

T – time interval – $\{1,..., T\}$;

T^* – a bunch of $\{0,1,...,T\}$;

$1/T$ – the risk of achieving the goal by only one player, i. or defender or hacker, respectively, for another player

$1/T$ – the risk of not achieving the goal

$p1$ и $p2$ – financial strategies of the defender and hacker, respectively;

r_1 – this is a factor that takes into account the financial resource of the hacker spent on hacking PISs (we believe that the unit of the financial resource of the defender has been spent on cyber defense of PIS s);

r_2 – a coefficient that takes into account the financial resource of the defender to protect PISs (a hacker's financial resource unit was used to break the PIS);

R_+^2 – Positive orthant;

$\alpha(t)$ – Coefficient of change in the financial resources of the PIS defender;

$\beta(t)$ – Coefficient of financial resources of a hacker.

The risk of achieving a goal by only one player can be interpreted as a risk to the player to lose his financial resource. I.e. the risk for the defender to finance the cybersecurity of PISs and not achieve the goal, resulting in PISs being hacked. And for the hacker to finance in hardware or software hacking and not achieve their goals.

In the moment $t(0)$ the defender multiplies the value $x1(0)$ by $\alpha(t)$ and selects a value $p1(t)$ $(p1(t) \in [0,1])$. i.e. the share of the defender's resource is determined $\alpha(t) \cdot x1(t)$, allocated to them at the time t.

Similarly, for a hacker – $(p2(t) \in [0,1])$. I.e. the share of the financial resource of the hacker is determined $\beta(t) \cdot x2(t)$, allocated to them for breaking the PIS at the time t.

The dynamics of changes in financial resources of players can be described by such a system of discrete equations:

$$\begin{cases} x1(t+1) = \alpha(t)\cdot x1(t) - p1(t)\cdot\alpha(t)\cdot x1(t) - \\ - r_2\cdot p2(t)\cdot\beta(t)\cdot x2(t); \\ x2(t+1) = \beta(t)\cdot x2(t) - p2(t)\cdot\beta(t)\cdot x2(t) - \\ r_1\cdot p1(t)\cdot\alpha(t)\cdot x1(t). \end{cases} \quad (1)$$

Consequently, at an arbitrary time t may be performed by one of the conditions shown in table 1.

Values $x1(T), x2(T)$ show the result of financing in the cyber defense of PISs over a time interval $[0,T]$, in the framework of a multi-step positional game with complete information [7, 8, 19]. According to previous studies [7, 8, 19], the process of financing PIS cybersecurity generates the tasks: from the point of view of the first player-ally; From the point of view of the second player-ally [7, 8, 19].

Because of symmetry, we confine ourselves to the problem from the point of view of the first player-ally. The second problem is solved similarly.

Table 1: Conditions for modeling the dynamics of changes in the financial resources of the PIS defender and hacker in situations of different players' strategies.

№ conditions	Mathematical interpretation	Note
1	$x1(t)\ge 0, x2(t)<0$	The process of financing PIS cyber defense has been completed. The cracker did not have enough financial resources to overcome the defense.
2	$x1(t)<0, x2(t)\ge 0$	The process of financing PIS cyber defense has been completed. The defender did not have enough financial means to ensure the protection of PISs.
3	$x1(t)<0, x2(t)<0$	The process of financing PIS cyber defense has been completed. The players do not have enough financial resources (in the context of achieving their goals).
4	$x1(t)\ge 0, x2(t)\ge 0$	The process of financing PIS cyber defense continues.

Property: for initial states S_1 there is a strategy of the PIS defender, which, for any implementation of the hacker strategy, "leads", in one of the moments t, the state of the system $(x1(0), x2(0))$ to the one in which condition (1) is fulfilled, see Table 1. Also, the hacker does not have a strategy that can "lead" to the fulfillment of conditions (2) or (3), at one of the preceding moments.

Property: for initial states S_1, there exists a strategy of the PIS advocate, which, for any implementation of the hacker's strategy, "leads", at one point t, the state of the system $(x1(0), x2(0))$ to the one at which condition (1) is fulfilled, see Table 1. Also, the hacker does not have a strategy that can "lead" to the fulfillment of conditions (2) or (3), at one of the preceding moments t.

The strategy (financial component) of the defender, having this property, is called optimal [8, 9]. The solution of Problem 1 is to find the set of preferences of the PIS defender. Its optimal strategies are also determined.

Similarly, the task is from the point of view of the hacker. These are symmetric problems. The solution of Problem 1 is found using the theory of multi-step quality games with complete information [7-9, 19].

Consider the process of finding the set of "preference" S_1. And also, we define optimal strategies $p1_*(.,.)$ for all relations of game parameters.

Situation 1) $\alpha\le\beta$.

$$S_1^i = \begin{Bmatrix} (x1(0), x2(0)): k(i-1)\cdot\beta\cdot x2(0)\le \\ \le r_1\cdot\alpha\cdot x1(0)\prec k(i-2)\cdot\beta\cdot x2(0) \end{Bmatrix}, i=1,.. \quad (2)$$

Then

$p1_* = \{p1_*(0,(x1,x2)),..., p1_*(i-1,(x1,x2))\}$, and

$p1_*(t,(x1,x2)) = \{[1-(r_2\cdot\beta\cdot x2)/(\alpha\cdot x1)]\}$, for $(x1,x2)\in R_+^2,\ \alpha\cdot x1 > r_2\cdot\beta\cdot x2,$ and is not defined - otherwise; $t = 0,1,...,i-1.$

Here

$k(i) = 1 + r_1\cdot r_2 - (r_1\cdot\alpha\cdot\beta)/(\beta\cdot k(i-1));$

$k_{-1} = 0, k_0 = 1 + r_1\cdot r_2;\ S_1 = \bigcup_{i=1}^{\infty} S_1^i.$

Ray

$$r_1\cdot 2\alpha\cdot x1(0) = \left\{ \begin{bmatrix} 1+r_1\cdot r_2 + \\ +\left((1+r_1\cdot r_2)^2 - c\right)^{0.5} \end{bmatrix} / 2\cdot\beta\cdot x2(0) \right\}$$ is called a barrier [7].

Barrier – the case when from the states $(x1(0), x2(0)): r_1\cdot\alpha\cdot x1(0)\le$

$$\le \left\{ \left[1 + r_1\cdot r_2 + \left((1+r_1\cdot r_2)^2 - c\right)^{0.5} \right] / 2\cdot\beta\cdot x2(0) \right\}$$

defender of PIS cannot reach his goal at some point t,

Where $c = 4 \cdot r_1 \cdot r_2 \cdot \chi,\ \chi = \frac{\alpha}{\beta}, \delta = \frac{\beta}{\alpha}.$

Situation 2) $\alpha \succ \beta,\ r_1 \cdot r_2 \geq 1.$

In this situation, the set of preferences for the defender of PIS S_1 will be the union of a finite number of sets S_1^i or $(N+2)$,

Where $N : k(i) \succ r_1 \cdot r_2 \cdot \chi,$
$i = 0,..., N-1; k(N) \leq r_1 \cdot r_2 \cdot \chi,$

$$S_1^i = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : k(i-1) \cdot \beta \cdot x2(0) \leq \\ \leq r_1 \cdot \alpha \cdot x1(0) \prec \\ \prec k(i-2) \cdot \beta \cdot x2(0) \end{pmatrix} \right\},$$

$$i = 1,..., N+1; \quad (3)$$

$$S_1^{N+2} = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : r_1 \cdot r_2 \cdot \beta \cdot x2(0) \leq \\ \leq r_1 \cdot \alpha \cdot x1(0) \prec \\ \prec k(N) \cdot \beta \cdot x2(0) \end{pmatrix} \right\}. \quad (4)$$

Optimal financial strategy [8, 9, 22] $p1_* = (p1_*(0,(x1,x2)),..., p1_*(N+1,(x1,x2))))$ I defined in the following way:

$p1_*(0,(x1,x2)) = \{0,$ at $(x1,x2) \in R_+^2, \alpha \cdot x1 > r_2 \cdot \beta \cdot x2,$ and is not defined - otherwise $\}$,

$p1_*(t,(x1,x2)) = \{[1-(r_2 \cdot \beta \cdot x2)/(\alpha \cdot x1)],$ at $(x1,x2) \in R_+^2, \alpha \cdot x1 > r_2 \cdot \beta \cdot x2$, and is not defined - otherwise; $t = 1,..., N+1\}$.

Situation 3) $\alpha \succ \beta,\ r_1 \cdot r_2 \prec 1.$

In this situation, the many preferences of the PIS S_1 advocate will also be the union of a finite number of sets. Or $(N + i_* + 2)$ sets,

Where $N : k(i) \succ \chi, i = 0,..., N-1; k(N) \leq \chi;$ i_* – the minimal nonnegative integer defined by the inequality $k(N) \cdot (\delta)^{i_*+1} \prec r_1 \cdot r_2.$

Then

$$S_1^i = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : k(i-1) \cdot \beta \cdot x2(0) \leq \\ \leq r_1 \cdot \alpha \cdot x1(0) \prec \\ \prec k(i-2) \cdot \beta \cdot x2(0) \end{pmatrix} \right\},$$

$$i = 1,..., N+1. \quad (5)$$

If $i_* = 0,$ then

$$S_1^i = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : k(i-1) \cdot \beta \cdot x2(0) \leq \\ \leq r_1 \cdot \alpha \cdot x1(0) \prec \\ \prec k(i-2) \cdot \beta \cdot x2(0) \end{pmatrix} \right\}, \quad (6)$$

$i = 1,..., N+1;$

$$W_1^{N+2} = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : r_1 \cdot r_2 \cdot \beta \cdot x2(0) \leq \\ \leq r_1 \cdot \alpha \cdot x1(0) \prec \\ \prec k(N) \cdot \beta \cdot x2(0) \end{pmatrix} \right\}.$$

Optimal strategy is defined, as in situation 2 (expressions 3 and 4).

If $i_* > 0,$ then

$$S_1^{N+1+j} = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : k(N) \cdot (\delta)^j \cdot \beta \cdot x1(0) \leq \\ \leq r_1 \cdot \alpha \cdot x2(0) \prec \\ \prec k(N) \cdot (\delta)^{j-1} \cdot \beta \cdot x2(0) \end{pmatrix} \right\}, \quad (7)$$

$i = 1,..., i_*;$

$$S_1^{N+1+i_*} = \left\{ \begin{pmatrix} x1(0), x2(0): \\ : r_1 \cdot r_2 \cdot \beta \cdot x2(0) \leq \\ \leq r_1 \cdot \alpha \cdot x2(0) \prec \\ \prec k(N) \cdot (\delta)^{i_*} \cdot \beta \cdot x2(0) \end{pmatrix} \right\}. \quad (8)$$

Optimal strategy $p1_* = (p2_*(0,(x1,x2)),..., p1_*(N+1+i_*,(x1,x2)))$ in this case is defined as follows:

$p1_*(i,(x1,x2)) = \{0,$ at $(x1,x2) \in R_+^2, \alpha \cdot x1 > r_2 \cdot \beta \cdot x2,$ otherwise it is not defined; $i = 0,..., i_*\},$

$p1_*(i,(x1,x2)) = \{[1-(r_2 \cdot \beta \cdot x2)/(\alpha \cdot x1)],$ at $(x1,x2) \in R_+^2, \alpha \cdot x1 > r_2 \cdot \beta \cdot x2, \quad i \geq i_* + 1$ otherwise it is not defined; $t = 1,..., N+1.$

Situation 4) Defender's sets of preference when limiting his financial resources:

$$S_1^* = S_1 \cap \begin{Bmatrix} (x1(0), x2(0)): \\ :(x1(0), x2(0)) \in R_+^2, \\ x1(0) \le Q \end{Bmatrix}, \quad (9)$$

Where Q – the maximum value of the financial resources of the defender on the means of cybersecurity of PIS.

Similarly, there are sets preference for the hacker. In the same way, task 2 is solved from the point of view of the second player, an ally.

Because of the symmetry of the statement of problems, it is sufficient to solve problem 1. Graphical interpretation of the solution results allows us to represent R_+^2 in the plane $(x1(0), x2(0))$ in the form of three sets. The sets obtained are cones with a vertex at a point $(0,0)$.

The set 1 adjoining the axis is a set of preferences for the PIS defender. The set 2 is the set preference for a hacker. The set 3 is neutral (from the point of view of the PIS advocate and hacker). If $x1(t) \ge 0, x2(t) \ge 0$ conditions for any moment t rays will be fulfilled, which are the boundaries of sets, are given by the coefficients. Coefficients are combinations of parameters that determine the dynamics of financing for the cybersecurity of PISs and its break-in.

5. RESULTS OF COMPUTATIONAL EXPERIMENTS

During the simulation, information was used on the configurations of specific information systems and technologies in maritime transport, see Table 2.

Computational experiments were performed in the previously described DSS (Decision Support System) module "SSDMI" [4, 6, 19, 21], and control computational experiments in the Mathcad package .

Objectives of the experiments:

1) determine the sets of strategies of players 1 and 2;

2) assess the risks associated with the loss of players of their financial resources to protect PISs and hacking the perimeter of cybersecurity;

3) check the adequacy of the model.

The results of three computational experiments are shown in Fig. 1.

The designations adopted in the figure:

1) the equilibrium beams (for three computational experiments) are shown in the figure with lines with round markers;

2) under the rays of balance and above them are the so-called zones of players' preference. It is accepted that under the corresponding rays there is a zone of "preference" for the PIS defender. Above the rays is shown the zone of "preference" of hacker's financial strategies, which tries to overcome the boundaries (perimeters) of PIS cybersecurity;

Table 2: Specific information systems and technologies for maritime transport, requiring financing in cybersecurity

Designation	Use
AIS (Automatic Identification System)	Automatic identification system. It serves for the transfer of the ship's identification data (including its cargo), information about its condition, current location and course. The device works by transmitting signals in the VHF band between vessels, floating relays and shore AIS-gateways that are connected to the Internet.
TOS (Terminal Operating System)	IT-infrastructure of the port. It serves the purposes of automation of the processes occurring with cargoes in the port (loading, unloading, inventory, monitoring of traffic on the port territory, optimization of warehousing, etc.). It can be either a product of a specific developer or an aggregate of individual systems performing various tasks.
CTS (Container Tracking System)	A system that allows you to track the movement of containers through GPS (less often than other data transmission channels).
ECDIS (Electronic Chart Display and Information System)	Electronic-cartographic navigation and information system, collects and uses AIS messages, data from radars, GPS and other marine sensors. In the complete set with
Others	[1–3]

3) the trajectories of the defender's and hacker's movements are represented by lines with triangular markers (for the defender the dotted blue line with triangular markers without shading, for the hacker – dotted green line with triangular markers with solid fill). Accordingly, the trajectories are in the area of preference of the defender and the hacker;

4) solid lines with square markers, shows the restrictions imposed on the financial resources of the defender and hacker (for the defender square markers without shading, for the hacker with solid fill).

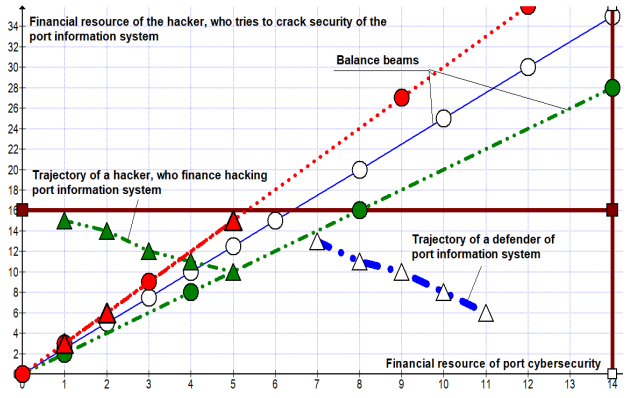

Figure 1: Results of computational experiments on the choice of rational financial strategies of the defender of the port information system (PIS).

In order to verify the adequacy of the calculations performed, the testing of the results obtained with the help of the DSS "SSDMI" was also carried out for real projects in the field of cybersecurity of PIS s in Kazakhstan. Earlier, in [6, 22, 23], the acceptable accuracy of the DSS software module "SSDMI" was confirmed in relation to the results of computational experiments.

6. DISCUSSION

In Fig. 1, the following cases are considered: 1) PIS defender, has the advantages of the initial financial resources on the means of cybersecurity (the balance beam $x1(0) = (2.5) \cdot x2(0)$ is shown in a blue solid line with white round markers); 2) the hacker has enough financial resources and, despite their limited initial time, he "brings" the state of the system to the "own" terminal surface (the beam of balance $x1(0) = 2 \cdot x2(0)$ is shown by a green dotted line with green round markers); 3) the situation in which the PIS defender and the hacker, using their optimal strategies, "move" along the line of balance. Thus, case 3 corresponds to the equilibrium financial strategies of players.

In the course of the computational experiments, the effectiveness of supporting decisions on the selection of rational financing strategies in the means of cybersecurity of PISs was confirmed. This work continues a number of publications [6, 7, 22–24], in which theoretical and methodological foundations of the design of the SSS using the theory of games were presented. In particular, bilinear multi-step quality games with several terminal surfaces. The model, in our opinion, eliminates many components of uncertainty in the processes of modeling financial investments in cybersecurity means of PIS. This distinguishes our work from the publications of other authors [13, 19, 25–30].

The revealed shortcoming of the model is the fact that the obtained data of the predictive evaluation when choosing financing strategies in the PIS cybersecurity means did not always coincide with the actual data. The maximum deviation of the results of the simulation experiment from practical data was 10–12%.

In Fig. 2 and 3 the comparative results are shown obtained during the survey of experts independently and with the help of the SSS "SSDMI". For the seaports of Kazakhstan, who took part in testing the SSS, 5 to 7 experts in the field of information security were involved. Experts with experience in the field of cybersecurity and information protection for at least 3 years were involved. Without SSS "SSDMI", analysts filled out questionnaires, assessing the feasibility of using various strategies for financing cyber defense of PISs in Kazakhstan seaports. Also, experts were asked to perform an evaluation using the SSS "SSDMI".

In Fig. 2 the results of the expert evaluation were presented independently (columns without shading) and with the help of the SSS "SSDMI" (columns with hatching) PIS protection parameters of the seaport of Aktau (Kazakhstan). Range of evaluation (by experts and SSS "SSDMI"): 0 - no protection; 1 - absolute protection.

The obtained results show that, without the use of the SSS "SSDMI", experts are more optimistic about the state of PIS protection. However, a standard check using penetration tests has denied expert judgment.

In Figure 3. the histogram of the time comparison (in minutes) expended by the experts themselves (columns without hatching) and using the SSS "SSDMI" (hatching columns) is shown to select rational strategies for financing in the PIS cybersecurity means.

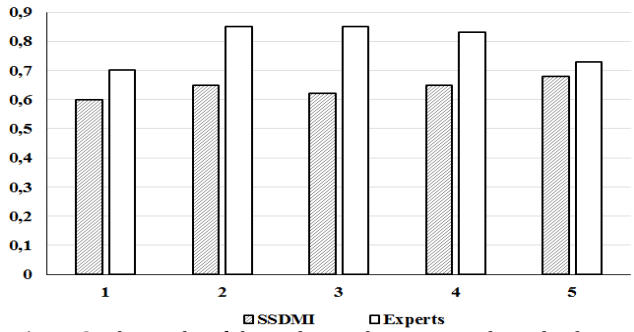

Figure 2: The results of the evaluation by experts independently and with the help of SSS "SSDMI" of PIS protection parameters of the seaport of Aktau (Kazakhstan).

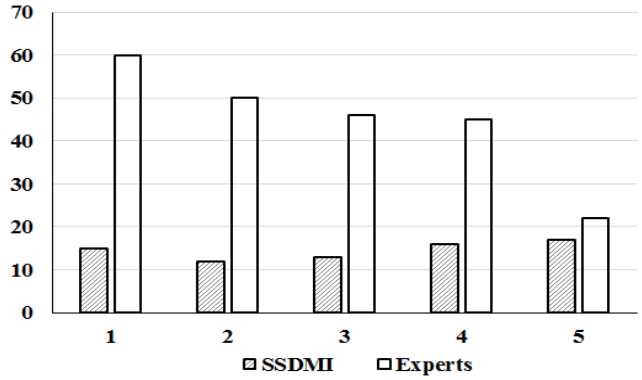

Figure 3: The histogram of time comparison (in minutes), spent by experts independently and with the help of the SSS "SSDMI", to select rational strategies for financing in cybersecurity funds of PIS in Aktau (Kazakhstan).

The time spent by experts on data processing with the help of the SSS "SSDMI" is 3.5–4 times less compared to the independent analysis of the expert.

Further perspectives of the development of this research are transferring the accumulated experience to real projects on financing in the means of cybersecurity of port information systems and other IT infrastructure for maritime transport of the Republic of Kazakhstan.

7. THANKS

The work was carried out within the framework of grant financing of the project "International Logistics Center of Aktau Port" (Republic of Kazakhstan). The authors also express their gratitude to the staff of the Department of Marine and Land Transport of the Caspian State University of Technologies and Engineering named after Sh. Yessenov, who participated in the collection of statistical material for computational experiments.

8. CONCLUSION

It is impossible to underestimate the importance of the maritime industry for modern society. According to statistics, at least 85–90% of goods are transported by sea. Information technology in maritime transport, developed in parallel with the progress of technological progress and the digitization of business processes. This makes the problem of cybersecurity of objects in the sphere of maritime transport, and in particular, port information systems (PIS), quite relevant.

The article presents a mathematical model for the decision support system in the process of financing in the means of cybersecurity of the port information systems. The model is based on the theory of games. The novelty of the proposed approach is that unlike existing solutions, a mathematical apparatus of multi-step quality games with several terminal surfaces is used. The result of such a decision is the ability for the end user, for example the seaport administration, or PIS vendor, to assess financial risks when investing in cyber security systems of IT infrastructures in the port.

Computational experiments were implemented, during which the sets of strategies of the PIS defender and hacker were determined. An assessment of the risks associated with the loss of the players' financial resources for the protection of PISs and the cracking of the perimeter of cybersecurity was performed. During the computational experiments it was confirmed that the class of games used in the model allows to adequately describe the financing process in the cybersecurity of PISs. It is also possible to find the optimal financial strategies of the defense side.

The developed model is integrated into the software solution support system, which was previously described in other authors' works.

REFERENCES

1. J. Kramek, **The critical infrastructure gap: US port facilities and cyber vulnerabilities**,*Center for 21st Century Security and Intelligence*, Washington, DC United States, 7 July, 2013.
2. M. McNicholas, ***Maritime security: an introduction***. Butterworth-Heinemann, 2016.
3. S. K. Shah, **The evolving landscape of maritime cybersecurity**, *Review of Business*, vol. 25, issue 3, pp. 28-30, 2004.
4. S.L. Caponi, K.B. Belmont, **Maritime Cybersecurity: A Growing Threat Goes Unanswered**, *Intellectual Property & Technology Law Journal*, vol. 27, issue 1, pp. 15-16, 2015.
5. O. Fitton, D. Prince, B. Germond, M. Lacy, ***The future of maritime cyber security,*** 2015. Online]. Available: http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf
6. V. A. Lakhno, **Development of a support system for managing the cyber security**, *Radio Electronics, Computer Science, Control*, No. 2, pp. 109-116, 2017, DOI: 10.15588/1607-3274-2017-2-12
7. O. Petrov, B. Borowik, M. Karpinskyy, O. Korchenko, V. Lakhno, V. ***Immune and defensive corporate systems with intellectual identification of threats***, Pszczyna :ŚląskaOficynaDrukarska, p. 222 p., 2016.
8. I.A. Krass, V.P. Malyukov, **O sushhestvovaniioptimal'nyhsmeshannyhstrategijdl janekotoryhantagonisticheskihigr**, *Optimizacija*, vol. 20, issue 37, pp. 135-146, 1978. (in Russian)
9. V.P. Malyukov, **A differential game of quality for two groups of objects**, *Journal of Applied Mathematics and Mechanics*, vol. 55, issue 5, pp. 596-606, 1991.
10. A. Fielder, S. Konig, E. Panaousis, S. Schauer, S. Rass, ***Uncertainty in Cyber Security Investments***, [Online]. Available: https://arxiv.org/abs/1712.05893
11. M. Chronopoulos, E. Panaousis, J. Grossklags, **An options approach to cybersecurity investment**, IEEE Access, vol. PP, pp. 1, 2017. DOI: 10.1109/ACCESS.2017.2773366
12. H. Cavusoglu, B. Mishra, S. Raghunathan, **A model for evaluating IT security investments**, *Communications of the ACM*, vol. 47, issue 7, pp. 87-92, 2004. DOI:10.1145/1005817.1005828
13. K. Goztepe, **Designing Fuzzy Rule Based Expert System for Cyber Security**, *International Journal of Information Security Science*, vol. 1, issue 1, pp. 13-19, 2012.
14. M. H. Manshaei, Q. Zhu, T. Alpcan et al., **Game theory meets network security and privacy**, *ACM Computing Surveys*, vol. 45, issue 3, pp. 1-39, 2013. DOI:10.1145/2480741.2480742
15. N. Ben–Asher, C. Gonzalez, **Effects of cyber security knowledge on attack detection**, *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015. DOI: 10.1016/j.chb.2015.01.039
16. J. Grossklags, N. Christin, J. Chuang, **Secure or insure?: a game-theoretic analysis of information security games**, in Proceedings of the *17th international conference on World Wide Web*, Beijing, China, 21 – 25 April 2008, New York, ACM, pp. 209-218.
17. A. Fielder, E. Panaousis, P. Malacaria et al., **Decision support approaches for cyber security investment**, *Decision Support Systems*, vol. 86, pp. 13–23, 2016. DOI:10.1016/j.dss.2016.02.012
18. P. H. Meland, I. A. Tondel, B. Solhaug, **Mitigating risk with cyberinsurance**, *IEEE Security & Privacy*, vol. 13, issue, 6, pp. 38–43, 2015. DOI: 10.1109/MSP.2015.137
19. A. Fielder, E. Panaousis, P. Malacaria et al. **Game theory meets information security management**, in Proceedings of the *IFIP International Information Security Conference*, Marrakech, Morroco, 2–4 June 2014, Berlin, Springer, pp. 15–29.

20. X. Gao, W. Zhong, S. Mei, **A game-theoretic analysis of information sharing and security investment for complementary firms**, *Journal of the Operational Research Society*, vol. 65, issue 11, pp. 1682-1691, 2014. DOI:10.1057/jors.2013.133
21. V.P. Malyukov, **Discrete-approximation method for solving a bilinear differential game**, *Cybernetics and Systems Analysis*, vol. 29, issue 6, pp. 879–888, 1993.
22. V. Lakhno, V. Malyukov, N. Gerasymchuk et al., **Development of the decision making support system to control a procedure of financial investment**, *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 3, pp. 24-41, 2017. DOI: 10.15587/1729-4061.2017.119259
23. V. Lakhno, V. Malyukov, V. Domrachev, O. Stepanenko, O. Kramarov, **Development of a system for the detection of cyber attacks based on the clustering and formation of reference deviations of attributes**, *Eastern-European Journal of Eenterprise Technologies*, vol. 3, issue 9, pp. 43–52, 2017. DOI: 10.15587/1729-4061.2017.102225
24. F. Smeraldi, P. Malacaria, **How to spend it: optimal investment for cyber security**, in Proceedings of the *1st International Workshop on Agents and CyberSecurity*, Paris, France, 06–08 May 2014, New York, ACM, pp. 8.
25. S. Rass, S. König, S. Schauer, **Uncertainty in games: Using probability-distributions as payoffs**, in Proceedings of the *International Conference on Decision and Game Theory for Security*, Springer, Cham, pp. 346-357, 2015. DOI:10.1007/978-3-319-25594-1_20
26. Y. J. Lee, R. J. Kauffman, R. Sougstad, **Profit-maximizing firm investments in customer information security**, *Decision support systems*, vol. 51, issue 4, pp. 904-920, 2011. DOI:10.1016/j.dss.2011.02.009
27. T. Moore, S. Dynes, F.R. Chang, ***Identifying how firms manage cybersecurity investment***, Available: Southern Methodist University, 2015, [Online]. Available: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf
28. M.L. Priyanka, S.Rajeshwari, K.Ashwini. **An Expert model for DNA Based Encryption Technology using Cloud Computing**, *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 8, No.1.3, pp.15–18, 2019. https://doi.org/10.30534/ijatcse/2019/0381.32019
29. B. Madhuravani, N.ChandraSekhar Reddy, K.Sai Prasad, B.Dhanalaxmi, V. Uma Maheswari. **Strong and Secure Mechanism for Data Storage in Cloud Environment**, *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 8, No.1.3, pp.29–33, 2019. https://doi.org/10.30534/ijatcse/2019/0681.32019
30. Akhmetov B., Lakhno V., Tkach Y., Adranova A., Zhilkishbayeva G. **Problems of Development of a Cloud-Oriented EducationalEnvironment of the University,** *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, Vol. 9, No.2, pp. 2196–2203, 2020. https://doi.org/10.30534/ijatcse/2020/196922020