Journal of Theoretical and Applied Information Technology
15th July 2018. Vol.96. No 13
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FUNDING MODEL FOR PORT INFORMATION SYSTEM CYBER SECURITY FACILITIES WITH INCOMPLETE HACKER INFORMATION AVAILABLE

[1] LAKHNO V., [1] MALYUKOV V. [2]PARKHUTS L., [3]BURIACHOK V., [4]SATZHANOV B., [4]TABYLOV A.

[1]Department of Cyber Security, European University, Ukraine
[2]Department of Information Security, Lviv Polytechnic National University, Ukraine
[3]Department of Information and Cybersecurity, Borys Grinchenko Kyiv University, Ukraine
[4] Department of Maritime and land transport , Caspian state university of technology and engineering named after SH. Essenov, Aktau, Kazakhstan

E-mail: [1]lva964@gmail.com,[1]volod.malyukov@gmail.com, [2]par7@i.ua, [3]v.buriachok@kubg.edu.ua
[4]Satzhanov1959@mail.ru, [4]abzal.tabylov@bk.ru

ABSTRACT

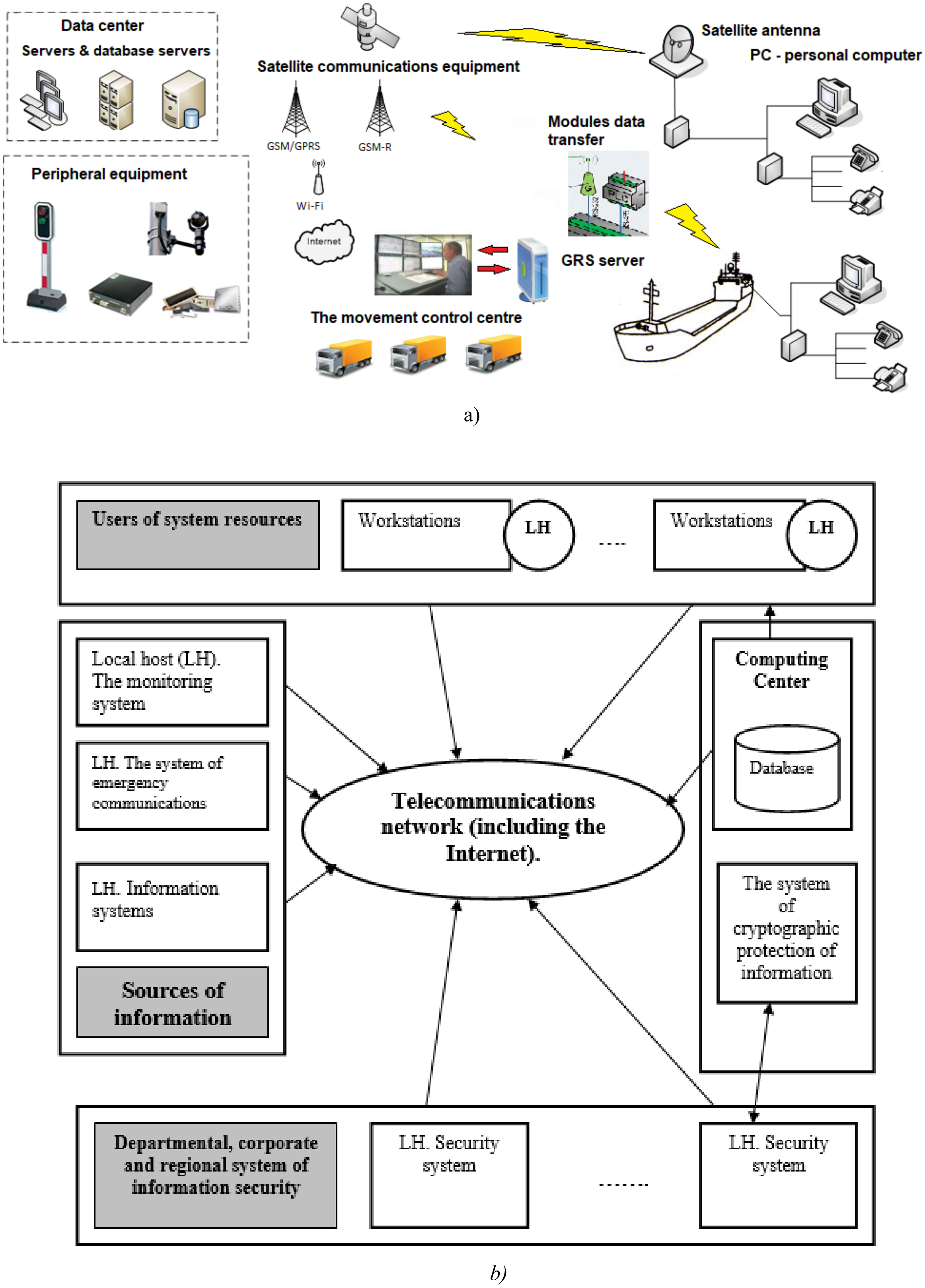
Article describes the model developed for the module of port information system cyber security facilities funding decision making support system. The model is based on multistage game theory toolkit. The solution offered allows an opportunity for managers of information safety systems, particularly port information systems and technologies, to carry out preliminary assessment of financial strategies for development of effective cyber safety systems. The distinctive feature of the model is the assumption that the defending party does not have full information on the financing strategies of the attacking party and on the state of its financial resources used to break cyber security barriers of the port information system. The solution employs mathematical apparatus of bilinear turn-based multistage quality game with several terminal surfaces. A multiple-option simulation experiment was carried out to ensure validity of the model. The results of the experiment will also be described herein. Thus, in the article at the first time, decision of the game was shown for all cases of the correlation of game parameters for the protection side of the port information system (PIS) and hackers seeking to overcome the boundaries of cybersecurity. The solution found in the article will be useful for the created decision support system, in particular, for the situation when the attacker uses a mixed financial strategy of hacking the information system.

Keywords: *Cyber Security, Port Information System, Game Theory, Decision Making Support System, Financial Strategy Selection.*

1. INTRODUCTION

The importance of marine transport operations for contemporary society is not to deny. According to official statistics [1] from year to year from 80 to 90% of all the goods are transported by sea and river transport. The scale of implementation of modern information technologies and systems in maritime transport increases year after year. Gone are the days the ships at sea represented an autonomous computerization and automation object [2]. Nowadays on-board systems and port information systems (hereinafter PIS) may be of interest as a target for a cyber attack by various hacking groups, (Figure 1). At the same time, as noted [3, 4] the problem of cyber security of sea and river transportation facilities, particularly PIS, is especially acute. Thus, according to the report [5], maritime cyber security issues cause little or no concern [5, 6].

Thus, in the context of a consistent trend for the increased number and complexity of cyber attacks in maritime transport (in a less degree river transport) industry, in combination with a lack of a proper strategy of financing of information protection systems and cyber security (IPS and CS) at sea, there is possibility for new dangerous cyber incidents or actual attacks, which pose potential danger and risks associated with the loss or discreditation of information.


Data center
Servers & database servers
Peripheral equipment
Satellite communications equipment
GSM/GPRS
GSM-R
Wi-Fi
Internet
Satellite antenna
PC - personal computer
Modules data transfer
GRS server
The movement control centre
Users of system resources
Workstations
LH

Workstations
LH
Local host (LH). The monitoring system
LH. The system of emergency communications
LH. Information systems
Sources of information
Telecommunications network (including the Internet).
Computing Center
Database
The system of cryptographic protection of information
Departmental, corporate and regional system of information security
LH. Security system

LH. Security system

a)

b)

Figure 1 : PIS elements categories as objects of cyberattacks

All of the aforesaid preconditions significance of the investigations aimed at development of new models, in particular for intelligent decision making support systems for selection of best finance strategies for information protection systems and PIS and maritime transport cyber security systems, in general.

2. STATEMENT OF THE PROBLEM

The purpose of the article is to develop a model for intelligent decision making support system module for selection of best finance strategies for information protection systems and port information system cyber security systems as an integral part of digital components of marine transport and critical information infrastructures of many states.

3. LITERATURE REVIEW

Many researchers [7, 8] have noted that there is a tendency for increased financial input from criminal groups and event states [9] into hacker attacks.

Complexity of contemporary cyber attacks, in particular those related to transport, gave rise to a blizzard of investigations related to intellectualization of computations in the area of decision making support in various practical aspects of information protection and cyber security of various information systems and technologies.

Simultaneous investigations are carried out for development of new methods and models for support of making decisions on selection of strategies of IPS and CS funding. [10] states that making decisions on cyber security financing is a permanent task. At the same time, according to the analysis of a number of recent works [10-12] one common drawback in this investigation segment is the lack of comprehensive techniques for development of IPS and CS financing strategies, including those for PIS. Besides, the models [13, 14] describing strategies of investment into cyber security of information systems and technologies do not cover situations where there is uncertainty about the financial strategies of the attacking party. Also there are no specific recommendations in the research works that contain the description of various expert systems [15, 16] and decision making support systems [17, 18] for selection of IPS and CS financing strategies. In addition, many of such works have one common drawback which is the lack of definitive modeling results. The models suggested in [19, 20] do not provide the possibility for evaluation of the risk of loss of financial resources by the defending party. The models suggested in [21] are based on the game theory for evaluation of efficiency of investments in IPS and CS. Nevertheless, the authors did not take into account such a parameter as the change of financial components of the attacking party.

In our opinion, the drawbacks in many existing approaches to optimization of IPS and CS financing strategies may be eliminated by means of application of the theory of differential and multistage quality games with several terminal surfaces [21, 22]. This approach allows to enhance the efficiency and accuracy of prediction calculations related to assessment of the financial risks associated with IPS and CS, and particularly PIS.

As shown by the analysis of published sources, the general shortcoming of almost all studies devoted to the choice of options for financing MIP (means of information protection) and CS (cybersecurity) strategies is the lack of tools for accurate forecast calculations for assessing the risks of financial losses in the PIS and CS, in particular for PISs.

Thus, according to the analysis of the researches undertaken, the issue of further development of models for decision making support systems (DMSS) in optimization of financing of information protection and cyber security tools for many industrial information systems (in particular port information systems) and technologies continues to be relevant. This is primarily due to insufficient investigation of the situations where there is no full information on the financial state of the attacking party.

4. MODELS AND METHODS

This article covers further development of methods of creation of various modules for the decision making support systems for information protection and cyber security tools (IPS and CS) for information systems of various applications (in particular, port information systems). The article further develops the ideas previously described in [17, 22]. Within the framework of the scheme suggested by the authors there are two parties:

Player 1 – the defender of port information system (DPIS);

Player 2 – hacker.

Both players use financial resources for attainment of their respective objectives [22, 23].

The players have $x(0)$ and $y(0)$ financial resources correspondingly. The interaction time is set as $\{0,1,..., T\}$, where T – is a natural number. Interaction between the Players (DPIS and hacker (hackers)) represents a bilinear multistage turn-based incomplete information quality game. According to [22, 23], the distinction of full information game consists in non-availability to DPIS of the information on the initial financial state of the other player (hacker). At the same time DPIS knows the creation states distribution function $F_0(\cdot)$ of the hacker. The players play in turns. At even points of time DPIS makes a move (the move within the framework of implementation of his own financial strategy of ensuring cyber safety of PIS). Hacker makes moves at uneven points of time.

Given:

1) $t = 2n, x(t), \quad x(t+1)$ – states of DPIS at t, $t+1$;
2) $x_2^{\xi}(t), x_2^{\xi}(t+1)$ – random states of the other player at t, $t+1$.

Thus, states of the players at $t+1$, $t+2$ can be determined based on the following formulae:

$$x(t+1) = \alpha(t)\cdot x(t) - u(t)\cdot \alpha(t)\cdot x(t);$$
$$y^{\xi}(t+1) = y^{\xi}(1) - s_1 \cdot u(t)\cdot \alpha(t)\cdot x(t); \qquad (1)$$
$$y^{\xi}(t+2) = \beta(t)\cdot y^{\xi}(t+1) - \nu(t)\cdot \beta(t)\cdot y^{\xi}(t+1);$$
$$x(t+2) = x(t+1) - s_2(t)\cdot \nu(t)\cdot \beta(t)\cdot y^{\xi}(t+1); \quad (2)$$

where

$u(t), \nu(t) : u(t) \in [0,1], \nu(t) \in [0,1]; s_1 > 0, s_2 > 0.$

4.1. Description of the game

1. at $t \in \{0,2,4,...,2\cdot n\}$ point of time DPIS player multiplies $x(t)$ by coefficient (rate of change, rate of growth) $\alpha(t)$. Then DPIS selects value $u(t)$ $(u(t) \in [0,1])$, which determines the share of resources of DPIS player $\alpha(t)\cdot x(t)$, allocated for protection of the PIS at t moment.

2. States of the players (DPIS and hacker) at $t+1$ moment are determined based on formulae (1) and (2). Therefore, within the framework of implementation of his strategy of PIS hacking player 2 (hacker) has to allocate $s_1 \cdot u(t)\cdot \alpha(t)\cdot x(t)$ financial resources.

3. s_1 parameter (coefficient) described the efficiency of hacker's investments into development or purchase of PIS hacking tools.

4. If the following condition is met:

$$P\left(y^{\xi}(t+1) < 0\right) \ge p_o, \left(0 \le p_o \le 1\right), \qquad (3)$$

DPIS player is deemed to ensure protection of PIS with p_0 probability. In this case DPIS player has used his financial resource. Thus, the process of financing of IPS and CS of the PIS is finished by DPIS player. If condition (3) is not met, DPIS player will continue to further finance IPS and CS.

5. Player 2 (hacker) acts similar to DPIS player in implementation of his financial strategy aimed at breaking through PIS protection. In this case the states of the players will be determined based on formulae (2).

6. If the following condition is met:

$$P\left(x(t+2) > 0\right) < p_1, \left(0 \le p_1 \le 1\right), \qquad (4)$$

player 2 (hacker) is deemed to be able to challenge cyber security of the PIS. In this case probability of such an outcome is defined as $(1-p_1)$. At this stage the process of financing IPS and CS of the PIS is finished, i.e. DPIS player should analyze the loss and choose a new strategy of financing of IPS and CS.

4.2. Properties of the game

We assume that DPIS player is interested in finding a set of his initial states compliant with the properties set below.

Properties of the game:

1) if the game started from initial states DPIS player may by his controlling actions $u(0),...,u(t) \, (t = 2n)$ ensure cyber safety of PIS with probability exceeding p_0.

2) the financial strategy selected by DPIS player prevents any damage to be caused by the hacker with probability exceeding $(1-p_1)$.

3) the variety of the states described in paragraphs 1 and section "Properties of the Game is the *variety of preference of DPIS player* (or player 1 in general).

4.3. Selection of optimal financial strategies of the port information system defending party

Let us introduce the following designations:

Φ – variety of one-dimensional random variable distribution functions;

$2n$ – even natural number next to T;

$T^* = \{0,2,...,2n\}$ – variety of even natural numbers.

The following definition is introduced based on the above. Pure strategy of DPIS player $u(.,.,.)$ – is function $u(.,.,.)$: $T^* \times R_+ \times \Phi \to [0,1]$, where $u(t,x,F) \in [0,1]$, $(F \in \Phi)$.

Therefore, DPIS player's strategy is the rule which allows DPIS to calculate (based on the data available) the financial resources to be allocated for IPS and CS, particularly for PIS.

Player 2 (hacker) is free to choose his financial strategy $v(.)$ based on any information on the purpose of attack (PIS).

Player 1 (DPIS) and player 2 (hacker) have different objectives and follow different financial strategies to obtain their objectives.

DPIS player's objectives:

1) to find the variety of preference;

2) to determine the strategies which will allow to meet the conditions required for termination of PIS IPS and CS financing process.

DPIS strategies which meet the properties specifies will be deemed optimal [23, 24].

The game model described herein (formulae 1-4) is the decision making task under risk [19, 24, 25]. At the same time our model is a bilinear turn-based multistage quality game with several terminal surfaces. Finding the varieties of preference of DPIS player and his optimal strategies depends on a number of parameters.

The following values have been introduced to describe the variety of preference of DPIS:

$$c(0) = \inf\{c'\},\ d(0) = \inf\{d'\},$$
$$F_0(c') \geq p_0,\ F0(d' \geq p_1). \tag{5}$$

The variety of preference of DPIS and the optimal strategy shall be found for $T = 1,3,...$

Let us introduce designations for varieties of preference:

$V_1^T(p_0, p_1)$ – variety of preference of DPIS of which he successfully completes IPS and CS financing procedure for PIS using T moves.

Provided $T = 1$,

$$V_1^1(p_0) = \{x(0) : s_1 \cdot \alpha \cdot x(0) \geq c(0)\}.$$

Therefore, an optimal strategy of DPIS player may be represented as follows:

$$u_*(1,x,c) = \begin{cases} 1,\ for\ s_1 \cdot \alpha \cdot x \geq c; \\ 0,\ otherwise. \end{cases} \tag{6}$$

Table 1 provides a more convenient presentation of various occurrences, conditions and varieties of preference that may arise for DPIS during the game.

Table 1: Variation of game parameter correlation occurrences

Occurrences	**Variety of preference, optimal strategies**
1. $p_0 = p_1$.	
1.1. $\alpha > \beta$.	$V_1^T(p_0, p_0) = \left\{ \begin{matrix} x(0) : c(0) \leq s_1 \cdot \alpha \cdot \left(\frac{\alpha}{\beta}\right)^k x(0); \\ c(0) > s_1 \cdot \alpha \cdot \left(\frac{\alpha}{\beta}\right)^{k-1} x(0) \end{matrix} \right\}$ where $T = 2k + 1 \leq 2k_0 + 3$. $V_1^{2k_0+s}(p_0, p_0) = \left\{ \begin{matrix} x(0) : c(0) > s_1 \cdot \alpha \cdot \left(\frac{\alpha}{\beta}\right)^{k_0+1} x(0); \\ c(0) \leq \left(\alpha / (s_2 \beta) \right) x(0) \end{matrix} \right\}$, $V_1^T(p_0, p_0) = \varnothing$. For $T = 2k + 1 \geq 2k_0 + 7$. Optimal strategy $u_*(n,x,c) = \begin{cases} 1,\ for\ s_1 \cdot \alpha \cdot x \geq c; \\ 0,\ otherwise. \end{cases}$

Table 1: Variation of game parameter correlation occurrences

1.2. $\alpha \le \beta$.	
1.2.1. $s_1 \cdot \alpha \cdot s_2 \le 1$.	$V_1^T(p_0, p_0) = \varnothing$ for $T = 2k + 1 \ge 3$.
1.2.2. $s_1 \cdot \alpha \cdot s_2 > 1$.	
1.2.2.1. $s_1 \cdot \beta \cdot s_2 > 1$.	$V_1^T(p_0, p_0) = \varnothing$ for $T = 2k + 1 \ge 3$.
1.2.2.2. $s_1 \cdot \beta \cdot s_2 \le 1$.	$V_1^3(p_0, p_0) = \left\{ \begin{matrix} x(0): c(0) \le \left(\alpha / (s_2 \cdot \beta) \right) x(0), \\ c(0) > s_1 \cdot \alpha \cdot x(0) \end{matrix} \right\}$ Optimal strategy $u_*(n, x, c) = \begin{cases} 1, \text{ for } s_1 \cdot \alpha \cdot x \ge c; \\ 0, \text{ otherwise.} \end{cases}$ $V_1^T(p_0, p_0) = \varnothing$ for $T = 2k + 1 \ge 5$.
2. $p_0 > p_1$.	$V_1^T(p_0, p_1) = V_1^T(p_0, p_0)$.
3. $p_0 < p_1$.	$V_1^T(p_0, p_1) = V_1^T(p_0, p_0) \cap \left\{ x(0): d(0) c(0) \le \left(\alpha / (s_2 \cdot \beta) \right) x(0) \right\}$.

Ray

$$\left\{ x(0): x(0) \in R_+,\, c(0) \in R_+ \; c(0) = \left(\alpha / (s_2 \cdot \beta) \right) x(0) \right\}$$

will be the barrier [25].

This means that from states $x(0): c(0) > \left(\alpha / (s_2 \cdot \beta) \right) x(0)$ the first player will not be able to attain the objective with $p \ge p_0$. probability. This ray can be called a stochastic ray of balance for financing of PIS protection tools.

Test calculations were made in PTC MathCad 4 for model validation.

5. SIMULATION EXPERIMENT

Purpose of the simulation experiment:

1) to identify the variety of strategies of the players (PIS defending party – player 1) and attacking party (player 2);

2) to assess the risks associated with the loss of players' financial resources used for PIS protection/hack;

3) to assess adequacy of the simulation model.

Outcomes of the three simulation experiments are represented if figures 2–4 below.

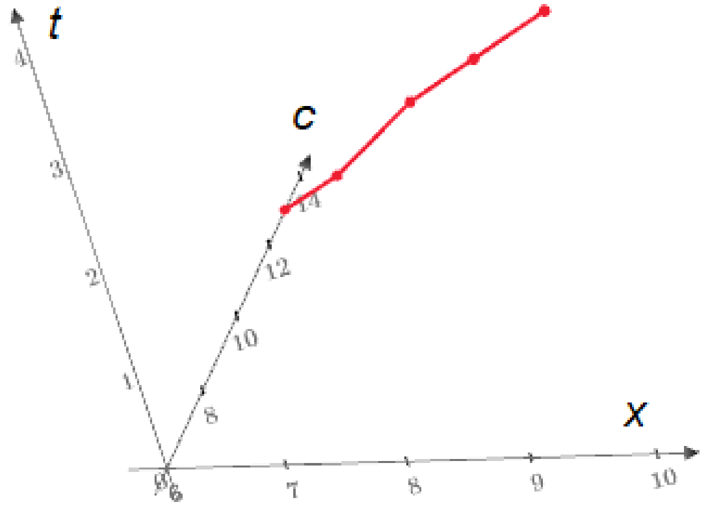


Figure 2 : Outcomes of simulation experiment No. 1

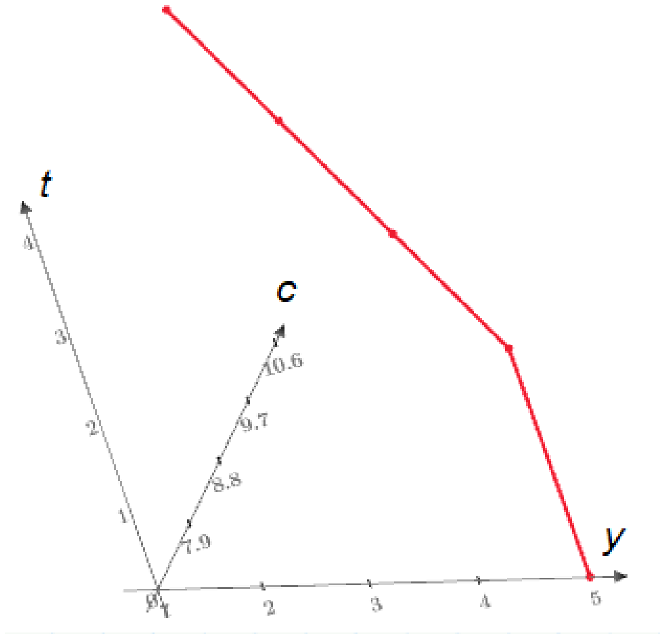


Figure 3 : Outcomes of simulation experiment No. 2

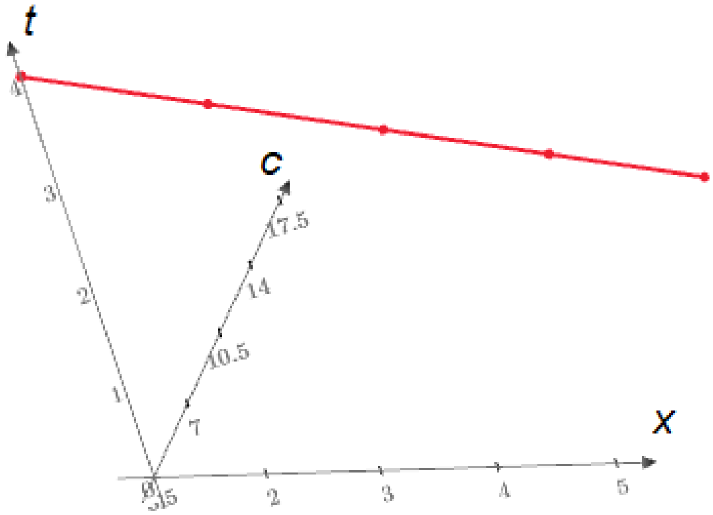


Figure 4 : Outcomes of simulation experiment No. 3

Game solution is given for all the game parameter correlation occurrences. Optimal behavior of port information system defendant can be determined based on the outcomes of the game. In the case reviewed the defending party was not aware of the financial resources of the attacking party. The only function set was the function of distribution of hacker's financial resources. Such a situation may arise in particular when the attacking party employs mixed hacking strategy (financial) with the aim to challenge cyber security of the port information system.

As shown by the results of the computational experiment, the refined model allowed to resolve the contradiction arising in the course of previous research [17, 23]. Namely, refinements in the model take into account all cases when there is not complete information about the financial state of the attacking party (hackers).

Maximum deviation between the outcomes of the simulation experiment and the actual data was 8–12 %.

6. DISCUSSION OF SIMULATION OUTCOMES

We considered a three dimensional positive orthant in three dimensional space $(t, x(0), c(0))$. t time axis goes from zero upwards.

t time will indicate the number of player's moves.

In this three-dimensional orthant we considered a set of planes, extending from (0,0,0) point and perpendicular to plane $(0, x(0), c(0))$. These planes are designated as follows: $c = \left(3.5 - \frac{1}{n}\right) \cdot x.$, for any positive n.

These planes allow to set varieties of preference of the first player in n moves with p_0 probability, i.e. it is deemed that $p_0 = p_1$. For example, $V_1^n(p_0, p_0)$ variety is

$$\{(n, x(0), c(0) : x(0), c(0)) \in$$
$$\in R_+^2, \left(3.5 - {}^{1}\!\!\diagup_{(n-1)}\right) x(0) \leq$$
$$\leq c(0) < \left(3.5 - {}^{1}\!\!\diagup_{(n)}\right) x(0), t = n\}$$

variety.

For $n = 1$ the expression is as follows:

$$V_1^1(p_0) = \{(1, x(0), y(0) : x(0), c(0)) \in$$
$$\in R_+^2, 0 \leq c(0) < (2.5) x(0), t = 1\}.$$

Ray: $c(0) = (3.5) \cdot x(0)$ in $(x(0), c(0))$ plane will be the ray of stochastic balance.

Test calculation 1 (**Figure 2**): (0, x(0), c(0)) = (0, 6, 13.0), (1, x(1), c(1)) = (1, 7, 11.0), (2, x(2), c(2)) = (2, 8, 10.0), (3, x(3), c(3)) = (3, 9, 8.0), (4, x(4), c(4)) = (4, 10, 6.0). Note, that the points are considered in three-dimensional space (t, x, c). Test calculation 1 describes situation there the first player (DPIS or computer system cyber protection party) has an advantage on the second player (hacker) in financial resources. This enables him to control the general path function in three-dimensional space (t, x, c), by driving it to the preferred terminal surface.

Test calculation 2 (**Figure 3**). Variety of preference of the second player (attacking party). We considered a three dimensional positive orthant in three dimensional space $(t, x(0), c(0))$. In this three-dimensional orthant we considered a set of planes, extending from (0,0,0) point and perpendicular to plane $(0, c(0), y(0))$.

These planes are designated as follows: $y = \left(0.8 + \dfrac{1}{n}\right) \cdot c$ for any positive n. These planes allow to set varieties of preference of the first player in n moves with p_0 probability, i.e. it is deemed that $p_0 = p_1$.

For example, $V_2^n(p_0, p_0)$ variety is

$$\{(n, c(0), y(0) : c(0), y(0)) \in$$
$$\in R_+^2, \left(0.8 + 1/(n-1)\right) c(0) \le$$
$$\le y(0) < \left(0.8 + 1/(n)\right) c(0), t\}$$

variety.

For $n = 1$ the expression is as follows:

$$V_2^1(p_0) = \{(1, c(0), y(0) : c(0), y(0)) \in$$
$$\in R_+^2, 0 \le y(0) < (1.8) c(0), t = 1\}.$$

Ray: $y(0) = (0.8) \cdot c(0)$ in $(c(0), y(0))$ plane will be the ray of stochastic balance.

Test calculation 2 (Figure 3, and Table 2) will have the following outcome: (0, c(0), y(0)) = (0, 5, 7.0), (1, c(1), y(1))=(1, 4, 9.0), (2, c(2), y(2))=(2, 3, 9.5), (3, c(3), y(3))=(3, 2, 10.0), (4, c(4), y(4))= (4, 1, 10.5). The points are considered in three-dimensional space (t, c, y). The situation in test calculation 2 is symmetrical to the situation in test calculation 1. This means that the second player (hacker) has an advantage in financial resources and thus is able to drive the path function to its preferred variety.

The third test calculation will correspond to the movement along the ray of balance (Figure 4): $y(0) = (3.5) \cdot c(0)$. Here we consider the initial task for the first player. **We obtain:** (0, x(0), c(0)) = (0, 5, 17.5), (1, x(1), c(1))=(1, 4, 14), (2, x(2), c(2))=(2, 3, 10.5), (3, x(3), c(3)) = (3, 2, 7), (4, x(4), c(4)) = (4, 1, 3.5, table 2. This test calculation corresponds to the situation where the initial data on the state of the player allow both players to move in path of balanced interaction. This means that the players have the strategies allowing them to move in (x, c) plane along the ray of stochastic balance. The players are not recommended to deviate from their respective optimal strategies, for any player may get into the area of preference of the other player.

Table 2: Results of simulation experiments.

Experiment N.	**t**					**x**					**c**				
1.	0	1	2	3	4	6	7	8	9	10	13	11	10	8	6
2.	0	1	2	3	4	5	4	3	2	1	7	9	9.5	10	10.5
3.	0	1	2	3	4	5	4	3	2	1	17.5	14	10.5	7	3.5

Thus the test calculations confirmed the adequacy of the model and its ability to ensure efficient decision making support in the area of financing of port information system cyber security tools. This work extends from several publications [17, 23] which describe theoretical and methodological framework for development of decision making support systems (DMSS). This article further develops these research works in terms of supplementation of the existing DMSS [4, 23] with simulation models based on bilinear turn-based multistage quality game with several terminal surfaces [23].

On a comparative analysis of similar software products [12, 13, 26], the developed decision support system considers various information systems specifics, such as sea transport. This ensures cost reduction for planning the joint hardware and software data protection performance.

The model proposed herein removed the defects of the decision option which did not take into account all the initial conditions. In particular, at this stage we tried to expand the model by considering the cases where there is no full information available on the financial state of the attacking party (hacker). In this context our model is different from the solutions offered by other authors [9–12].

7. THANKS

This work was performed within the framework of grant financing of the Logistic Center of International Aktau Sea Port project (Republic of Kazakhstan). The authors of this article greatly appreciate the assistance of the staff of Sea and Land Transport academic department of Yessenov State University of Technology and Engineering in collection of statistical material for the simulation experiment.

This work was supported by a grant from the European University of Kyiv.

8. CONCLUSION

Below is the description of the results obtained.

Improvements were suggested to the port information system cyber security financing model previously described. The suggested improved variant of the model differs from the existing models and the original author's solution in that it take into account the lack of full information on the financial state of the attacking party (hackers).

The models provides for the use of dynamic programming method for incomplete data problem solving. Unlike other existing models the suggested one provides for a more effective solving of problems in the scenarios where the information content requires the defending party to spend resources for PIS security.

This article describes the outcomes of the simulation experiment. Solution of the game is given for all the game parameter correlation occurrences for PIS defending party and hackers who try to break cyber security barriers of the port information system. Optimal variants of behavior of the port information system defending party have been found. Simulation experiment covered the situation where PIS defending party is not aware of the financial resources of the hacker. This may be useful, for example, where the attacking party employs mixed hacking strategy with the aim to challenge cyber security of the port information system. The simulation experiment conducted proves the adequacy of the model offered. Maximum deviation between the outcomes of the simulation experiment and the actual data does not exceed 12 %.

REFERENCES

[1] The 2017 Sea Transport Awards Winners Announced, [Online]. Available: http://www.hellamarine.com/it/blog/case-studies/the-2017-sea-transport-awards-winners-announced.html

[2] M. McNicholas, "Maritime security: an introduction," Butterworth-Heinemann, 2016.

[3] L. Jensen, "Challenges in Maritime Cyber-Resilience," Technology Innovation Management Review, Vol. 5, N 4. p. 35, 2015.

[4] O. Petrov, B. Borowik, M. Karpinskyy, O. Korchenko, V. Lakhno, "Immune and defensive corporate systems with intellectual identification of threats," Pszczyna : Śląska Oficyna Drukarska, 222 p., 2016.

[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] J. Kramek, "The critical infrastructure gap: US port facilities and cyber vulnerabilities," Center for 21st Century Security and Intelligence, 2013.

[7] N. Van der Meulen, "Investing in Cybersecurity," RAND Europe, 2015.

[8] L. A. Gordon, M. P. Loeb, & L. Zhou, "Investing in cybersecurity: Insights from the Gordon-Loeb model," *Journal of Information Security*, *7*(02), p. 49, 2016.

[9] S. L. Caponi, & K.B. Belmont, "Maritime Cybersecurity: A Growing Threat Goes Unanswered," *Intellectual Property & Technology Law Journal*, 27(1), 16, 2015.

[10] B. B. Kelly, "Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform," *BUL Rev.*, *2*, pp. 1663, 2012.

[11] L. A. Gordon, M. P. Loeb, W. Lucyshyn, & L. Zhou, "The impact of information sharing on cybersecurity underinvestment: a real options perspective," *Journal of Accounting and Public Policy*, Vol. *34, No* 5, pp. 509-519, 2015.

[12] A. Fielder, S. Konig, E. Panaousis, S. Schauer, & S. Rass, "Uncertainty in Cyber Security Investments," arXiv preprint [Online].

Available: arXiv:1712.05893, 2017.

[13] L. A. Gordon, M.P. Loeb, W. Lucyshyn, & L. Zhou, "Increasing cybersecurity investments in private sector firms," *Journal of Cybersecurity*, *1*(1), pp. 3-17, 2015.

[14] H. Cavusoglu, B. Mishra, S. Raghunathan, "A model for evaluating IT security investments," *Communications of the ACM*, Vol. 47, No. 7, pp. 87-92, 2004.

[15] K. Goztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security," *International Journal of Information Security Science*, Vol. 1, No 1, pp. 13-19, 2012.

[16] A. Fielder, E. Panaousis, P. Malacaria et al., "Decision support approaches for cyber security investment," *Decision Support Systems*, Vol. 86, pp. 13-23, 2016.

[17] V.A. Lakhno, "Development of a support system for managing the cyber security," *Radio Electronics, Computer Science, Control*, No. 2, pp. 109-116, 2017.

[18] M. N. Manshaei, Q. Zhu, T. Alpcan et al., "Game theory meets network security and privacy," *ACM Computing Surveys*, Vol. 45, No. 3, pp. 1-39, 2013.

[19] A. Fielder, E. Panaousis, P. Malacaria et al., "Game theory meets information security management," *IFIP International Information Security Conference*, Marrakech, Morroco, 2-4 June 2014 : proceedings, Berlin, Springer, pp. 15-29, 2014.

[20] F. Smeraldi, P. Malacaria, "How to spend it: optimal investment for cyber security," *1st International Workshop on Agents and CyberSecurity*, Paris, France, 06–08 May 2014 : proceedings, New York, ACM, pp. 8, 2014.

[21] 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, No. 11. pp. 1682-1691, 2014.

[22] V.P. Malyukov, "Discrete-approximation method for solving a bilinear differential game," *Cybernetics and Systems Analysis,* Vol. 29, No. 6. pp. 879-888, 1993.

[23] 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, No. 3. pp. 24-41, 2017.

[24] R. Isaacs, "Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization", Courier Corporation, 1999.

[25] B. Akhmetov et al., "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity," *Eastern-European Journal of Enterprise Technologies*. No. 1 (2). pp. 4-15, 2016.

[26] V. Lakhno, A. Petrov, Ant. Petrov, "Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport," *International Conference on Information Systems Architecture and Technology*, Springer, Cham, 2017, pp. 113-127.