ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIVE INFORMATION TECHNOLOGIES

UDC 004.33(035)

MODEL OF CYBER SECURITY FINANCING WITHIN THE FRAMEWORK OF THE BILINEAR DIFFERENTIAL QUALITY GAME SCHEME

Akhmetov B. B. – PhD, Associate Professor, Rector of the Caspian State University of Technologies and Engineering named after Sh. Yessenov, Aktau, Kazakhstan.

Lakhno V. A. – Dr. Sc., Professor, Head of Department of cybersecurity, European University, Kyiv, Ukraine.

Malyukov V. P. – Dr. Sc., Associate Professor, Professor, Department of Informatics Systems, Mathematics Disciplines, European University, Kyiv, Ukraine.

ABSTRACT

Actuality. There is considered the actual problem of an optimal decision making on financing of information and cyber security means in the conditions of active counteraction to the side of the attackers of information and communication systems of the logistics and situational transport center.

The aim of the work is to develop a model for the decisions support system of the financing process of the information and cyber security means of the logistics and situational transport center in conditions of active counteraction to the attacking party, which differs from existing approaches by solving a bilinear differential quality game with several terminal surfaces.

Method. Solving a bilinear differential quality game, that allows to reflect adequately the essence of the problem, there was used a discrete approximation method. The method allowed not only to find a solution of the bilinear differential quality game with dependent motions, but also became an effective at the software implementation of the decisions support system in the field of financing information and cyber security means for information and communication systems of the protected logistics-situational transport center.

Results. The developed model allows to obtain optimal financing strategies by the cyber security means protection side for information and communication logistics and situational transport centers at any ratio of parameters describing the financing process, no matter how financially the party tries to attack the security perimeters.

Conclusions. In this article there was firstly considered the model within the framework of the bilinear differential quality game scheme for the decisions support system of the process of cyber security means financing for information and communication systems of protected logistics and situational transport centers. For such differential games there were previously developed no effective solution methods. In the proposed solution there were firstly used the differential equations that define the interaction dynamics, describe the dependent motions by means of bilinear functions.

KEYWORDS: cyber security, differential game, optimal strategies, hacking and protection, decision support system.

ABBREVIATIONS

IS – information security;

ICTS – information and communication transport systems;

CS – cyber security;

LSC – logistics and situational centers;

ISS – information security systems;

DSS – decision support system;

GT – game theory.

NOMENCLATURE

g^* – coefficient determining the balance beam;

M_0 – terminal surface for the 1st player;

N_0 – terminal surface for the 2nd player;

r_1 – efficiency of financial resources investments in the means of IS and CS ICTS;

r_2 – efficiency of financial resources investments in the means of overcoming the boundaries of ICST protection;

DOI 10.15588/1607-3274-2018-3-13

R_+^2 – positive orant;

t – time parameter;

u_* – optimal strategy of the 1st player;

U – strategies of the 1st player;

V – strategies of the 2nd player;

x – the value of the financial resource of the 1st player (ICST protector);

y – the value of the financial resource of the 2nd player (hacker);

Z_1 – a set of preferences for the 1st player;

Z_2 – a set of preferences for the 2nd player;

α – the growth rate of the financial resource of the 1st player for the ICTS protection;

β – the growth rate of the financial resource of the 2nd player for the ICTS hacking.

INTRODUCTION

The rapid development of digital technologies in various fields, particularly, in ICTS, stimulate the active development of IS and CS systems. Analyzing the problems of ICTS protection it is advisable to consider the transformation of the situation in the context of actions of two parties (players): party 1 – IS and CS services; party 2 – intruder (hacker). In accordance with [1] the party 2 is regarded as a set of potential threats. As the threats there can be seen both the incompetent actions of individual performers inside the ICTS and the planned targeted cyber attacks. It is noted in works [2, 3] that in such situations the most adequate models describing the behavior of a system with two or more opposing sides are the models based on TI. In fact, if the strategies of both parties 1 and 2, the win/loss for the players (for the cases under consideration) are known then we can talk about solving the problem of rational financing in the IS and CS systems. At the same time, the party 2 (hacker) does not have enough financial resources to overcome the perimeter of the ICTS protection. The reverse problem will be the situation in which the party 1 (the ICTS protector) did not have enough financial resources to protect it.

The object of the research is the process of financing in the means of information and cyber security of the LSC transport and its ICTS.

The aim of the work is the development of a model for the decision support system of the financing process in the means of information and cyber security of the LSC transport, in conditions of active counteraction to the attacking party, which differs from existing approaches by solving a bilinear differential quality game with several terminal surfaces.

1 PROBLEM STATEMENT

One of the most important tasks, facing the services ensuring the ICTS functioning, is the task of their IS and CS. This requires adequate financial investment. In turn, the decision-making on ICTS means investing should be based on procedures that allow financing taking into account all the factors inherent to CS. This is possible if the DSS is developed and implemented, allowing to make optimal (rational) decisions on investing financial resources for the development of ICTS protection tools. There is considered a model for a DSS on a continuous procedure for financing of IS and CS of ICTS in LSC from the penetration of intruders (hackers) into them. The model is based on solving a bilinear differential quality game with two terminal surfaces. Mathematical statement: there are two players that control a dynamic system, given by a system of bilinear differential equations with dependent motions. The sets of strategies of the players U and V are determined accordingly. Two terminal surfaces M_0, N_0 are defined. The aim of the first player is to put the dynamic system using its control strategies to the terminal surface M_0, despite the second player actions. The aim of the second player is to put the dynamic system using its control strategies to the terminal surface N_0, despite the first player actions. The solution is to find a set of initial states of objects and their strategies that allow objects to put the system to that or another surface.

2 LITERATURE REVIEW

In recent years, there has been a tendency to replenish traditional mathematical approaches to the selection of compatible hardware and software systems for CS and IS [4, 5]. In the context of the problem there was carried out the analysis of the literature data for works using the games theory [6] choosing the means of CS. A general approach to the use of TI for the analysis of interactions between participants of the protection process and attackers was presented in [7, 8]. The authors did not cover all the interests of the decision-making parties. In work [9] there was proposed the TI apparatus for the problems of selecting the protection means against unauthorized access. The work was not implemented in the format of completed recommendations. In work [10] there was carried out a review and analysis of game-theoretic methods in the problems of IS and CS providing. The authors were limited by simulating the total cost of ISS without taking into account the behavioral strategies of the parties. In work [11] there were considered the models of step games in cases of incomplete information prior to the construction of protection mechanisms from DoS / DDoS attacks. A certain disadvantage of the work is the fact that in order to find a successful strategy for the player 1 (an information protector) it requires experimentally to collect statistics on the types of ISS. In work [12] there was considered a final non-cooperative game with at least one balance situation with mixed strategies of the parties. The authors do not give any data on how to find the balance situation by standard TI methods.

DOI 10.15588/1607-3274-2018-3-13

As the performed analysis of the latest researches in the field of TI application for determining the strategies of parties 1 and 2 has shown the problem of further development of models for the ISS in the tasks of financing process control in the means of the IS and CS of LSC transport and its protected information and communication systems remains relevant.

3 MATERIALS AND METHODS

Here is a mathematical model for the ICTS protection means financing. In task 1 the confederate player is treated for the protector, the enemy player is treated for the hacker. And vice versa – in task 2, the confederate player is treated for the hacker, and the enemy player is treated for the protector. The first player seeks to protect his ICTS for LSC [13]. The second - to hack the ICTS. For this purpose, both players need financial resources. We assume that for a given period of time $[0,T]$ (T is a real positive number) the first player has $x(0)$ financial resources, while the second player has $y(0)$. These parameters determine the predicted, at $t=0$, amount of financial resources that players 1 and 2 have to achieve their goals. At the initial moment of time t the first player multiplies the value $x(0)$ by the coefficient (rate of change, growth) $\alpha(t)$. Then, the player 1 selects a value $u(t)$ $(u(t)\in[0,1])$ that determines the share of the resource $\alpha(t)\cdot x(t)$ of the 1st player allocated by him at the CS at time t. Similarly, at time t the player 2 multiplies the value $y(t)$ by the coefficient (rate of change, growth) $\beta(t)$. Next, the player 2 selects a value $v(t)$ $(v(t)\in[0,1])$ that determines the share of the resource $\beta(t)\cdot y(t)$ of the second player's allocated by him for ICTS hacking at time t.

Let denote by r_1 the effectiveness of financial resources investment in the means IS and CS of ICTS. In fact, r_1-coefficient that shows how much financial resources a hacker will need to hack the IS (in our case, ICTS), for the protection of which there was expended the unit of financial resource of the first player. Let designate by r_2 the effectiveness of financial resources investment in IS hacking tools (ICTS). Or r_2-coefficient that shows how much financial resources an ICTS protector will need if there was expended the resource unit on hacking. Then the dynamics of financial resources changes of the first and second players is given by the following system of differential equations:

$$\frac{dx}{dt}=-x(t)+\alpha(t)\cdot x(t)-u(t)\cdot\alpha(t)\cdot x(t)-r_2\cdot v(t)\cdot\beta(t)\cdot y(t); \quad (1)$$

$$\frac{dy}{dt}=-y(t)+\beta(t)\cdot y(t)-v(t)\cdot\beta(t)\cdot y(t)-r_1\cdot u(t)\cdot\alpha(t)\cdot x(t). \quad (2)$$

Then at the moment t it is possible to fulfill one of three conditions: 1) $x(t)>0,\ y(t)=0$; 2) $x(t)=0,\ y(t)>0$; 3) $x(t)>0,\ y(t)>0$. If the first condition is fulfilled, then we will say that the financing procedure for the CS systems is completed. And the ICTS hacker has not enough financial means to overcome the protection. If the second condition is fulfilled, then we will say that the procedure for financing the CS systems is completed and the protection side did not have enough financial resources for its efficient organization. If the third condition is fulfilled, the procedure for CS financing systems CRB continues further.

The values $x(T), y(T)$ show the CS systems financing result on the planned interval $[0,T]$.

The IS and CS financing systems process is considered within the framework of a positional differential game with complete information. [14] In this case, the process generates two tasks: from the point of view of the first confederate player and the second confederate player [2]. Because of the symmetry we confine the problem statement from the point of view of the first confederate player. The second problem is solved similarly. Let denote T^* by the set $[0,T]$.

Definition. The pure strategy of the first confederate player is the function $u: T^*\cdot[0,1]\cdot[0,1]\to[0,1]$, that puts the state of the position $(t,(x,y))$ the value $u(t,(x,y)): 0\le u(t,(x,y))\le 1$.

Therefore, the pure strategy of the first confederate player is the function (rule) that puts the state of information (position) at the moment t the value $u(t,(x,y))$. The value $u(t,(x,y))$ determines the share of the financial resource of the player – ICST protector, which he planned to spend for the protection at a time t. Regarding the awareness of the enemy player (within the framework of the positional differential game scheme), no assumptions are made. This is equivalent to the fact that the confederate player chooses his controlling influence based on any information. After defining the strategies in task 1, it is necessary to determine the set of preferences Z_1 for the first player. Therefore, Z_1 – this set of such initial states $(x(0), y(0))$ of financial resources of the defender and the hacker, which has the following property. The property of financial resources of the players: for the initial states there is a strategy of the first player, which for any realizations of the second player strategies put the state of the system in $(x(0), y(0))$ at which the condition 1) will be fulfilled. However, the second player does not have a strategy that can lead to the fulfillment of conditions 2) or 3). The strategy $u_*(.,.)$ of the protector-player that possesses to the states2) or 3) is called optimal. The solution of Problem consists in finding the sets of "preferences" of the protector and his

DOI 10.15588/1607-3274-2018-3-13

optimal strategies. Similarly, the problem is posed from the point of view of the second confederate player.

The solution of the problem 1 is found using the tools of the differential quality games theory with complete information [14, 15], which allows to find it at any ratio of game parameters. We give the solution of the game, i.e. sets of preference Z_1 and optimal strategies for the first player.

The case 1. $r_1 \cdot r_2 = 1, \beta \geq \alpha$. Then we will receive:

$$Z_1 = \left\{(x(0), y(0) : (x(0), y(0))) \in \operatorname{int} R_+^2,\ r_1 \cdot \alpha \cdot x(0) > \beta \cdot y(0)\right\}, \quad (3)$$

$u_*(x, y) = \{1, r_1 \cdot \alpha \cdot x(0) > \beta \cdot y(0)\}, (x, y) \in \operatorname{int} R_+^2$, and is not defined otherwise.

The case 2. $r_1 \cdot r_2 = 1, \beta < \alpha$. Then we will receive:

$$Z_1 = \left\{(x(0), y(0) : (x(0), y(0))) \in \operatorname{int} R_+^2,\ r_1 \cdot \alpha \cdot x(0) > \beta \cdot y(0)\right\}, \quad (4)$$

$$u_*(x, y) = \left\{0, \text{при } \beta \cdot y < r_1 \cdot \alpha \cdot x < a \cdot y, (x, y) \in \operatorname{int} R_+^2\right\},$$

$\left\{1, \text{при } r_1 \cdot \alpha \cdot x > \alpha \cdot y, (x, y) \in \operatorname{int} R_+^2\right\}$, and is not defined otherwise.

The case 3. $r_1 \cdot r_2 \succ 1, \beta \succ r_1 \cdot \alpha \cdot r_2$. Here $u_*(.), Z_1$ are defined in the same way as in Case 1.

The case 4. $r_1 \cdot r_2 \succ 1, \alpha \leq \beta \prec r_1 \cdot \alpha \cdot r_2$. Then we will receive:

$$Z_1 = \left\{(x(0), y(0) : (x(0), y(0))) \in \operatorname{int} R_+^2,\ r_1 \cdot \alpha \cdot x(0) > (r_1 \cdot \alpha \cdot r_2 \cdot \beta)^{\frac{1}{2}} \cdot y(0)\right\}, \quad (5)$$

$$u_*(x, y) = \left\{1, \text{при } r_1 \cdot \alpha \cdot x > (r_1 \cdot \alpha \cdot r_2 \cdot \beta)^{\frac{1}{2}} \cdot y, (x, y) \in \operatorname{int} R_+^2\right\}, (x, y) \in \operatorname{int} R_+^2,$$

and is not defined otherwise.

The case 5. $r_1 \cdot r_2 \succ 1,\ \alpha / (r_1 \cdot r_2) \prec \beta \prec \alpha$.

Here $u_*(.), Z_1$ are defined in the same way as in Case 4.

The case 6. $r_1 \cdot r_2 \succ 1,\ \beta \prec \alpha / (r_1 \cdot r_2)$.

$$Z_1 = \left\{(x(0), y(0) : (x(0), y(0))) \in \operatorname{int} R_+^2,\ \alpha \cdot x(0) > r_2 \cdot \beta \cdot y(0)\right\}, \quad (6)$$

$$u_*(x, y) = \left\{0, \text{при } r_1 \cdot \alpha \cdot r_2 \cdot y < r_1 \cdot \alpha \cdot x < \beta \cdot y, (x, y) \in \operatorname{int} R_+^2\right\},$$

$\left\{1, \text{при } r_1 \cdot \alpha \cdot x > \beta \cdot y, (x, y) \in \operatorname{int} R_+^2\right\}$, and is not defined otherwise.

The case 7. $r_1 \cdot r_2 \prec 1,\ \beta \geq \alpha$.

Here $u_*(.), Z_1$ similarly to Case 1.

The case 8. $r_1 \cdot r_2 \prec 1,\ r_1 \cdot \alpha \cdot r_2 \leq \beta \prec \alpha$.

Then we will receive:

$$Z_1 = \left\{(x(0), y(0) : (x(0), y(0))) \in \operatorname{int} R_+^2,\ \alpha \cdot x(0) > r_2 \cdot \beta \cdot y(0)\right\}, \quad (7)$$

$$u_*(x, y) = \left\{0, \text{при } r_1 \cdot \beta \cdot r_2 \cdot y < r_1 \cdot \alpha \cdot x < \alpha \cdot y, (x, y) \in \operatorname{int} R_+^2\right\},$$

$\left\{1, \text{при } r_1 \cdot \alpha \cdot x \geq \alpha \cdot y, (x, y) \in \operatorname{int} R_+^2\right\}$, and is not defined otherwise.

The case 9. $r_1 \cdot r_2 \prec 1,\ \beta \prec r_1 \cdot \alpha \cdot r_2$. Здесь $u_*(.), Z_1$ are defined in the same way as in Case 8.

The task from the point of view of the second confederate player is solved similarly.

The sets of preference (cones) from the point of view of the second confederate player "join" to the sets of "preference" of the first confederate player. These sets are divided among themselves by the balance beams. The balance beams have the property if the pair $(x(0), y(0))$ belongs to the beam, then the players have strategies that enable them to be on the balance beam for all subsequent moments of time. This can allow, at given $(x(0), y(0))$, to find the relations to the interaction parameters, under which the pair $(x(t), y(t))$ will be located on the balance beam.

4 EXPERIMENTS

The computational experiment was conducted in the PTC Mathcad 4 environment. The software module for the DSS «SSDMI» is also implemented in the RadStudio (Delphi) environment, see Fig. 1 [16]. As the initial data there was accepted the technical task data for the development of protected LSC transport of Ukraine and the Republic of Kazakhstan.

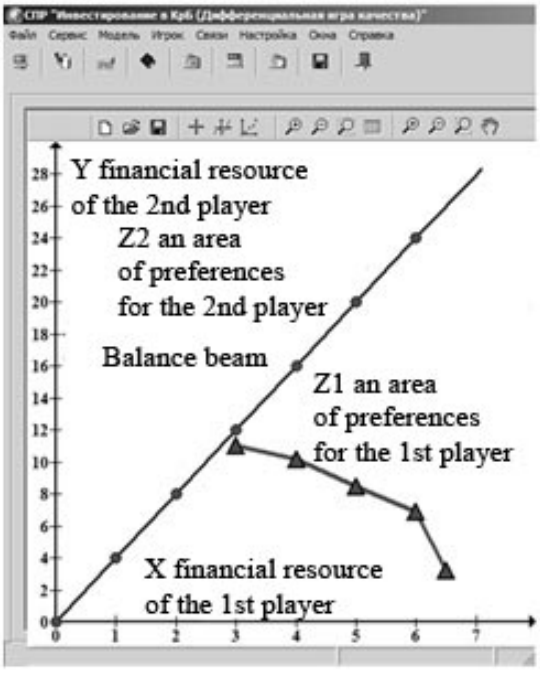

Figure 1– General view of the DSS module of the CS means financing process for the bilinear differential game quality scheme

5 RESULTS

Table 1 and Fig. 2–5 show the results for 4-x test calculations during the computational experiment. There

DOI 10.15588/1607-3274-2018-3-13

were considered situations when two players control a dynamic system. The purpose of the experiment is to determine the set of strategies of the players U and V. There are also considered the cases when the players' strategies deduce them on the corresponding terminal surfaces M_0, N_0. In the course of the experiment, there are found sets of initial states of objects and their strategies that allow objects to bring the system to one or another terminal surface. On the plane, the axis X is the financial resources of the 1st player. Axis Y – financial resources of the 2nd player. The area under the beam – Z_1 (the "preference" area of the first player). The area above the beam – Z_2 (the "preference" area of the second player).

Table 1 – Computational experiment results

Calculations	Modeling results					g^*
	$x(0),y(0)$	$x(1), y(1)$	$x(2),y(2)$	$x(3),y(3)$	$x(4),y(4)$	
1	3,11	4,10.2	5,8.5	6,7.3	6.5,3.2	4
2	5,10.5	4.2,11	3.7,11.2	2.8,12.3	1.6,13.1	2
3	5,15	4.2,12.6	3.4,10.2	2.8,8.4	1.3, 3.9	3
4 (in comparison to MathCad)	3,11.3	4,10.5	5,8.9	6,7.9	6.5,3.6	4

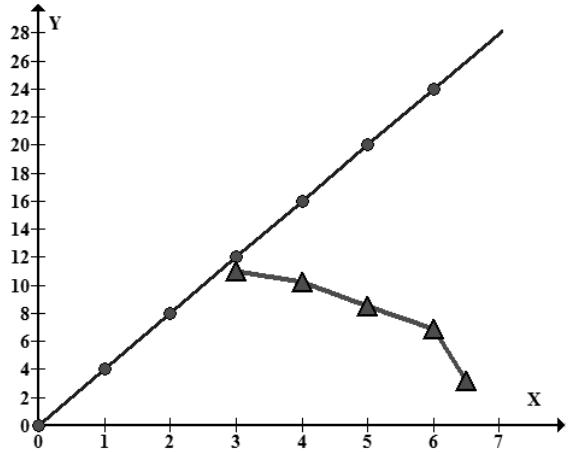

Figure 2 – Computational experiment results 1

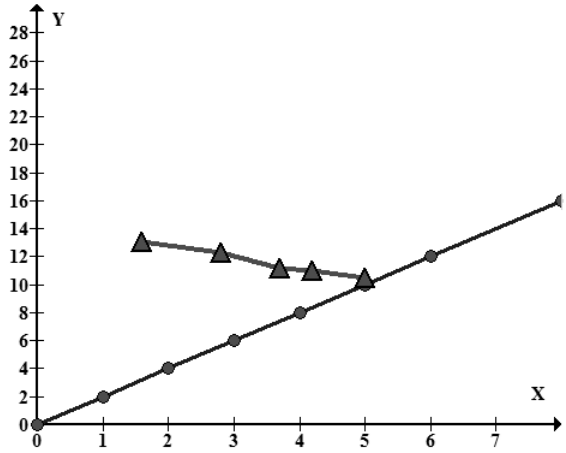

Figure 3 – Computational experiment results 2

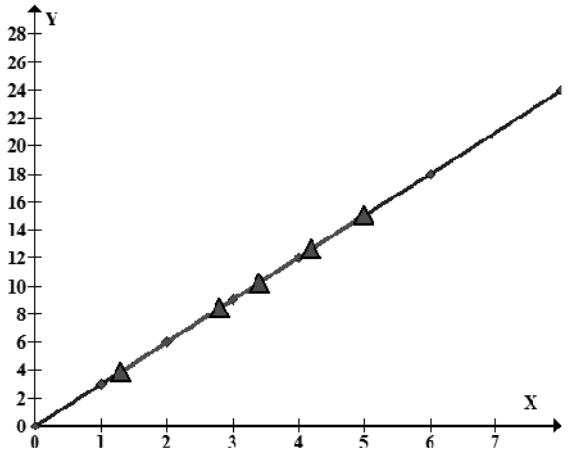

Figure 4 – Computational experiment results 3

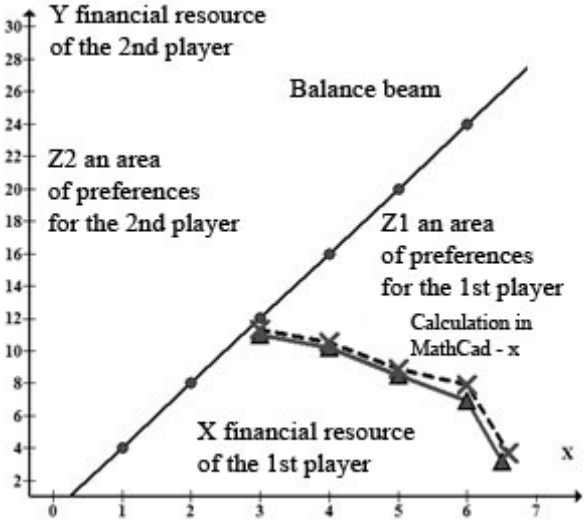

Figure 5 – Computational experiment results in DSS in comparison to MathCad

DOI 10.15588/1607-3274-2018-3-13

The obtained results demonstrate the effectiveness of the proposed approach. During the testing of the model in the PTC Mathcad 4 environment, as well as in the DSS "SSDMI" [16] there was established the correctness of the results.

Approbation of DSS "SSDMI" was carried out for real investment projects in the field of cyber security of Ukraine and Kazakhstan [15, 16].

6 DISCUSSION

Fig. 2 illustrates the situation where the first player has an advantage in the ratio of the initial financial resources, i.e. they are in the set of preferences of the 1st player. In this case, the 1st player, using his optimal strategy, will achieve his goal, particularly, put the state of the system to its "own" terminal surface. Fig. 3 shows a situation in which the 2nd player, using the non-optimal behavior of the first player at the initial moment of time, put the state of the system to the "own" terminal surface. Figure 4 corresponds to the case when the initial state of the system is on a balance beam. And the players, applying their optimal strategies, "move" along this beam. This "satisfies" both players simultaneously and illustrates the "stability" of the system. At small deviations choosing the implementation of the optimal strategy by the 1st player (see the section on which the round and triangular markers coincided) he will reach his goal, but somewhat later. Fig. 5 shows the acceptable accuracy of the software module DSS "SSDMI" in relation to the results of computational experiments in PTC Mathcad 4. The discrepancy does not exceed 2–6%. The proposed model is the process of predicting the results of CS ICTS LSC means investing. The disadvantage of the model is the fact that the data of the forecast estimate obtained through the DSS at the selection investing strategies in CS means do not always coincide with the actual data.

In the course of computational experiments and practical data approbation [15, 16] it was established that the proposed model allows adequately to describe the dependent motions by means of bilinear functions. This provides an effective tool for the participants of the investment process in the CS ICTS LSC means. In comparison with existing models, the proposed solution improves the efficiency and predictability for the investor by an average of 11–15% [8, 9, 11, 17, 18].

CONCLUSIONS

There is proposed a model for the decisions support system of the financing process in the information and cyber security means of the LSC transport, in conditions of active counteraction to the attacking side. The model differs from existing ones by solving a bilinear differential quality game with several terminal surfaces.

The scientific novelty of the results obtained in the article is that for the first time there was considered a new class of bilinear differential games that allowed adequately to describe the process and to find the optimal financing strategies by the cyber security means protection side. The solution was carried out on the example of optimizing the financial components of the strategies for protecting the information and communication systems of the LSC transport at any parameters ratio describing the financing process, no matter how financially acts the party which tries to hack the security perimeters was. A special feature of this approach was the use of a solution based on a bilinear differential quality game with several terminal surfaces.

The practical significance of the results is that there was developed a module in the RadStudio programming environment for the decision support system – SSDMI. In "SSDMI" module there is implemented the proposed model, based on the application of methods of the theory of differential games. The developed module, allows to reduce the discrepancies between the forecast data and the real return from investing in CS means. The solution allows to obtain optimal financing strategies by the protection side of cyber security means for ICTS of LSC transport. The software implementation of the DSS module allows to choose the optimal financial component of the protection side strategy at any parameters ratio that describe the financing process, no matter how financially the second party acts, trying to hack the security perimeters.

Further perspectives for the development of this research are the transfer of accumulated experience to the real practice of optimizing investment policy in protected LSC in Ukraine and the Republic of Kazakhstan.

ACKNOWLEDGEMENTS

The work was carried out within the framework of the grant research on scientific and technical projects for 2018-2020 of the Republic of Kazakhstan, registration number AP05132723 "Development of adaptive expert systems in the field of cyber security of critically important information objects".

REFERENCES

1. Manshaei M. H., Zhu Q., Alpcan T. et al. Game theory meets network security and privacy, *ACM Computing Surveys*, 2013, Vol. 45, No. 3, pp. 1–39. DOI: 10.1145/2480741.2480742
2. Grossklags J., Christin N., Chuang J. *Secure* or insure?: a game-theoretic analysis of information security games,*17th international conference on World Wide Web*, Beijing, China, 21 – 25 April 2008 : proceedings.New York, ACM, 2008. pp. 209–218. DOI:10.1145/1367497.1367526
3. Cavusoglu H., MishraB., Raghunathan S. A model for evaluating IT security investments, *Communications of the ACM*, 2004, Vol. 47, No. 7, pp. 87–92.
4. FielderA., PanaousisE., Malacaria P. et al.Decision support approaches for cyber security investment,Decision Support Systems, 2016, Vol. 86, pp. 13–23. DOI: org/10.1016/j.dss.2016.02.012
5. Meland P. H., Tondel I. A., Solhaug B. Mitigating risk with cyberinsurance, IEEE Security & Privacy, 2015, No. 13(6), pp. 38–43. DOI: 10.1109/MSP.2015.137
6. Malyukov V.P. A differential game of quality for two groups of objects, Journal of Applied Mathematics and Mechanics, 1991, Vol. 55, No.5, pp. 596–606.

DOI 10.15588/1607-3274-2018-3-13

7. Lavrent'ev A.V., Zjazin V. P. O primenenii metodov teorii igr dlja reshenija zadach komp'juternoj bezopasnosti, Bezopasnost' informacionnyh tehnologij, 2013, No. 3, pp. 19–24.
8. Bykov A. Ju., Altuhov N. O., Sosenko A. S. Zadacha vybora sredstv zashhity informacii v avtomatizirovannyh sistemah na osnove modeli antagonisticheskoj igry, Inzhenernyj vestnik, 2014, No. 4 , pp. 525–542.
9. Basalova G. V., Sychugov A. A. Primenenie metodov teorii igr dlja optimizacii vybora sredstv zashhity informacii, Izvestija Tul'skogo gosudarstvennogo universiteta, Tehnicheskie nauki, 2016, No. 11(1), pp. 122–128.
10. FielderA., PanaousisE., MalacariaP. etal. Game theory meets information security management, IFIP International Information Security Conference, Marrakech, Morroco, 2–4 June 2014 : proceedings, Berlin, Springer, 2014, pp.15–29. DOI:10.1007/978-3-642-55415-5_2
11. Zarkumova R. N. Primenenie metodov teorii igr pri vybore sredstva jeffektivnoj zashhity, Sbornik nauchnyh trudov Novosibirskogo gosudarstvennogo tehnicheskogo universiteta, 2009, No. 4, pp. 41–46.
12. Gao X., ZhongW., MeiS. A game-theoretic analysis of information sharing and security investment for complementary firms, *Journal of the Operational Research Society*, 2014, Vol. 65, No. 11, pp. 1682–1691. DOI:10.1057/jors.2013.13
13. Lahno V.A. Model' intellektual'noj sistemy upravlenija gorodskimi avtobusnymi perevozkami, *Radio Electronics, Computer Science, Control*, 2016, No. 2, pp. 119–127. DOI: 10.15588/1607-3274-2016-2-15
14. Malyukov V.P. Discrete-approximation method for solving a bilinear differential game, *Cybernetics and Systems Analysis*, 1993,Vol. 29, No. 6, pp. 879 – 888.
15. Lakhno V., Malyukov V., Gerasymchuk N. et al. Development of the decision making support system to control a procedure of financial investment, *Eastern-European Journal of Enterprise Technologies*, 2017, Vol. 6, No. 3, pp. 24–41. DOI: 10.15587/1729-4061.2017.119259
16. Lakhno V. A. Development of a support system for managing the cyber security, *Radio Electronics, Computer Science, Control*, 2017, No. 2, pp. 109–116. DOI: 10.15588/1607-3274-2017-2-12
17. Smeraldi F., Malacaria P. 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, 2014, pp. 8. DOI: 10.1145/2602945.2602952
18. Tosh D. K., Molloy M., Sengupta S. et al.Cyber-investment and cyber-information exchange decision modeling, *High Performance Computing and Communications IEEE 7th International Symposium on Cyberspace Safety and Security (CSS)*, New York, 24–26 August 2015 : proceedings, New York, IEEE, 2015, pp. 1219–1224. DOI: 10.1109/HPCC-CSS-ICESS.2015.264

Received 05.01.2018.
Accepted 24.03.2018.

УДК 004.33(035)

МОДЕЛЬ ФІНАНСУВАННЯ У КІБЕРБЕЗПЕКУ В РАМКАХ СХЕМИ БІЛІНІЙНОЇ ДИФЕРЕНЦІЙНОЇ ГРИ ЯКОСТІ

Ахметов Б. Б. – канд. техн. наук, доцент, ректор Каспійського державного університету технологій та інжинірингу ім. Ш. Есенова, Актау, Казахстан.

Лахно В. А. – д-р техн. наук, професор, зав. кафедри кібербезпеки та управління захистом інформаційних систем, Європейський університет, Київ, Україна.

Малюков В. П. – д-р физ.-мат. наук, доцент, професор кафедри інформаційних систем та математичних дисциплін, європейський університет, Київ, Україна.

АНОТАЦІЯ

Актуальність. Розглянуто актуальну проблему прийняття оптимального рішення щодо фінансування засобів інформаційної та кібербезпеки в умовах активної протидії стороні зламувачів інформаційно-комунікаційних систем логістично-ситуаційного центру транспорту.

Мета роботи – розробка моделі для системи підтримки рішень процесу фінансування в засоби інформаційної та кібербезпеки логістично-ситуаційного центру транспорту, в умовах активної протидії нападникам, що відрізняється від чинних підходів рішенням білінійної диференціальної гри якості з декількома термінальними поверхнями.

Метод. При вирішенні білінійної диференціальної гри якості, що дозволяє адекватно показати сутність розглянутої проблеми, використовувався дискретно-апроксимаційний метод. Метод дозволив не тільки знайти рішення білінійної диференціальної гри якості із залежними рухами, а й виявився ефективним під час програмної реалізації системи підтримки рішень в сфері фінансування засобів інформаційної та кібербезпеки інформаційно-комунікаційних систем захищених логістично-ситуаційних центрів транспорту.

Результати. Розроблена модель дозволяє отримати оптимальні стратегії фінансування стороною захисту засобів кібербезпеки для інформаційно-комунікаційних логістично-ситуаційних центрів транспорту при будь-яких співвідношеннях параметрів, що описують процес фінансування, як би фінансово не діяла сторона, яка намагається подолати периметри захисту.

Висновки. У статті вперше розглянута модель в рамках схеми білінійної диференціальної гри якості для системи підтримки рішень процесу фінансування засобів кібербезпеки для інформаційно-комунікаційних систем захищених логістично-ситуаційних центрів транспорту. Для таких диференціальних ігор раніше не було розроблено ефективних методів вирішення. У запропонованому рішенні вперше диференціальні рівняння, що задають динаміку взаємодії, описують залежні рухи за допомогою білінійних функцій.

КЛЮЧОВІ СЛОВА: кібербезпека, диференціальна гра, оптимальні стратегії, злом і захист, система підтримки рішень.

УДК 004.33(035)

Ахметов Б. Б. – канд. техн. наук, доцент, ректор Каспийского государственного университета технологий и инжиниринга им. Ш. Есенова, Актау, Казахстан.

Лахно В. А. – д-р техн. наук, профессор, зав. кафедры кибербезопасности и управления защитой информационных систем, Европейский университет, Киев, Украина.

Малюков В. П. – д-р физ.-мат. наук, доцент, профессор кафедры информационных систем и математических дисциплин, Европейский университет, Киев, Украина.

DOI 10.15588/1607-3274-2018-3-13

МОДЕЛЬ ФИНАНСИРОВАНИЯ В КИБЕРБЕЗОПАСНОСТЬ В РАМКАХ СХЕМЫ БИЛИНЕЙНОЙ ДИФФЕРЕНЦИАЛЬНОЙ ИГРЫ КАЧЕСТВА

Актуальность. Рассмотрена актуальная проблема принятия оптимального решения по финансированию средств информационной и кибербезопасности в условиях активного противодействия стороне взломщиков информационно-коммуникационных систем логистическо-ситуационного центра транспорта.

Цель работы – разработка модели для системы поддержки решений процесса финансирования в средства информационной и кибербезопасности логистическо-ситуационного центра транспорта, в условиях активного противодействия атакующей стороне, отличающаяся от существующих подходов решением билинейной дифференциальной игры качества с несколькими терминальными поверхностями.

Метод. При решении билинейной дифференциальной игры качества, позволяющей адекватно отразить существо рассматриваемой проблемы, был использован дискретно-аппроксимационный метод. Метод позволил не только найти решение билинейной дифференциальной игры качества с зависимыми движениями, но и оказался эффективным при программной реализации системы поддержки решений в сфере финансирования средств информационной и кибербезопасности информационно-коммуникационных систем защищенных логистическо-ситуационных центров транспорта.

Результаты. Разработанная модель позволяет получить оптимальные стратегии финансирования стороной защиты средств кибербезопасности для информационно-коммуникационных логистическо-ситуационных центров транспорта при любых соотношениях параметров, описывающих процесс финансирования, как бы финансово не действовала сторона, пытающаяся взломать периметры защиты.

Выводы. В статье впервые рассмотрена модель в рамках схемы билинейной дифференциальной игры качества для системы поддержки решений процесса финансирования средств кибербезопасности для информационно-коммуникационных систем защищенных логистическо-ситуационных центров транспорта. Для таких дифференциальных игр ранее не было разработано эффективных методов решения. В предложенном решении впервые дифференциальные уравнения, задающие динамику взаимодействия, описывают зависимые движения посредством билинейных функций.

КЛЮЧЕВЫЕ СЛОВА: кибербезопасность, дифференциальная игра, оптимальные стратегии, взлом и защита, система поддержки решений.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Game theory meets network security and privacy / [M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, & J. P. Hubaux] //ACM Computing Surveys (CSUR). – 2013. – Т. 45, №. 3. – P. 1–39. DOI: 10.1145/2480741.2480742
2. Grossklags J. Secure or insure?: a game-theoretic analysis of information security games / J. Grossklags, N. Christin, J. Chuang // 17th international conference on World Wide Web, Beijing, China, 21 – 25 April 2008 : Proceedings. – New York : ACM, 2008. – P. 209–218. DOI: 10.1145/1367497.1367526
3. Cavusoglu H. A model for evaluating IT security investments / H. Cavusoglu, B. Mishra, S. Raghunathan // Communications of the ACM. – 2004. – Т. 47, № 7. – P. 87–92.
4. Decision support approaches for cyber security investment / [A. Fielder, E. Panaousis, P. Malacaria et al.] // Decision Support Systems. – 2016. – Vol. 86. – P. 13–23. DOI: org/10.1016/j.dss.2016.02.012
5. Meland P. H. Mitigating risk with cyberinsurance / P. H. Meland, I. A. Tondel, B. Solhaug // IEEE Security & Privacy. – 2015. – Vol. 13, № 6. – P. 38–43. DOI: 10.1109/MSP.2015.137
6. Malyukov V. P. A differential game of quality for two groups of objects / V. P. Malyukov // Journal of Applied Mathematics and Mechanics. – 1991. – Vol. 55, № 5. – P. 596–606.
7. Лаврентьев А. В. О применении методов теории игр для решения задач компьютерной безопасности / А. В. Лаврентьев, В. П. Зязин // Безопасность информационных технологий. – 2013. – № 3. – С. 19–24.
8. Быков А. Ю. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры / А. Ю. Быков, Н. О. Алтухов, А. С. Сосенко // Инженерный вестник. – 2014. – №. 4. – С. 525–542.
9. Басалова Г. В. Применение методов теории игр для оптимизации выбора средств защиты информации / Г. В. Басалова, А. А. Сычугов // Известия Тульского государственного университета. Технические науки. – 2016. – № 11(1). – С. 122–128.
10. Game theory meets information security management / [A. Fielder, E. Panaousis, P. Malacaria et al.] // IFIP International Information Security Conference, Marrakech, Morroco, 2–4 June 2014 : Proceedings. – Berlin : Springer, 2014. – P. 15–29. DOI:10.1007/978-3-642-55415-5_2
11. Заркумова Р. Н. Применение методов теории игр при выборе средства эффективной защиты / Р. Н. Заркумова // Сборник научных трудов Новосибирского государственного технического университета. – 2009. – № 4. – С. 41–46.
12. Gao X. A game-theoretic analysis of information sharing and security investment for complementary firms / X. Gao, W. Zhong, S. Mei // Journal of the Operational Research Society. – 2014. – Т. 65, №. 11. – P. 1682–1691. DOI:10.1057/jors.2013.13
13. Лахно В.А. Модель интеллектуальной системы управления городскими автобусными перевозками / В. А. Лахно // Радіоелектроніка, інформатика, управління. – 2016. – № 2. – С. 119–127. DOI: 10.15588/1607-3274-2016-2-15
14. Malyukov V. P. Discrete-approximation method for solving a bilinear differential game / V. P. Malyukov // Cybernetics and Systems Analysis. – 1993. – Vol. 29, № 6. – P. 879–888.
15. Development of the decision making support system to control a procedure of financial investment / [V. Lakhno, V. Malyukov, N. Gerasymchuk et al.] // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 6, № 3. – P. 34–41. DOI: 10.15587/1729-4061.2017.119259
16. Lakhno V. A. Development of a support system for managing the cyber security / V. A. Lakhno // Radio Electronics, Computer Science, Control. – 2017. – № 2. – P. 109–116. DOI: 10.15588/1607-3274-2017-2-12
17. Smeraldi F. How to spend it: optimal investment for cyber security / F. Smeraldi, P. Malacaria // 1st International Workshop on Agents and CyberSecurity, Paris, France, 06–08 May 2014 : Proceedings. – New York : ACM, 2014. – P. 8. DOI: 10.1145/2602945.2602952
18. Cyber-investment and cyber-information exchange decision modeling / [D. K. Tosh, M. Molloy, S. Sengupta et al.] // High Performance Computing and Communications IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), New York, 24–26 August 2015 : Proceedings. – New York : IEEE, 2015. – P. 1219–1224. DOI: 10.1109/HPCC-CSS-ICESS.2015.264

DOI 10.15588/1607-3274-2018-3-13