Manuscript received March 21, 2018; revised October, 2018. DOI: 10.24425/123547

Modeling of the Decision-making Procedure for Financing of Cyber Security Means of Cloud Services by the Medium of a Bilinear Multistep Quality Game with Several Terminal Surfaces

Valery Lakhno, Berik Akhmetov, Volodimir Malyukov, and Timur Kartbaev

***Abstract*—The model is developed for the intellectualized decision-making support system on financing of cyber security means of transport cloud-based computing infrastructures, given the limited financial resources. The model is based on the use of the theory of multistep games tools. The decision, which gives specialists a chance to effectively assess risks in the financing processes of cyber security means, is found. The model differs from the existing approaches in the decision of bilinear multistep quality games with several terminal surfaces. The decision of bilinear multistep quality games with dependent movements is found. On the basis of the decision for a one-step game, founded by application of the domination method and developed for infinite antagonistic games, the conclusion about risks for players is drawn. The results of a simulation experiment within program implementation of the intellectualized decision-making support system in the field of financing of cyber security means of cloud-based computing infrastructures on transport are described. Confirmed during the simulation experiment, the decision assumes accounting a financial component of cyber defense strategy at any ratios of the parameters, describing financing process.**

***Keywords*—cloud infrastructures, cyber security, multistep quality game, optimum financing strategy, risks, decision-making support system**

I. Introduction

CLOUD infrastructures are subject to the same risks and threats, as traditional networked ones.

Owing to rapid development of information and communication technologies on different types of transport and increasing data volume, many transport companies began to increasingly transfer their information and calculations to clouds [1]. At the same time, in [2, 3] it is noted that the cloud platforms of hosting providers became an attractive target for cybermalefactors. For example, disclosure of personal user information, a trade secret and other data in a cloud, can potentially lead to severe financial and reputation losses for hosting providers. Therefore, service providers of cloud-based computing and data storage try to provide the due level of cyber defense to minimize risks and cyberthreats. If ensuring physical security is based on strict control of access to infrastructure components, the network safety still remains a problem section in perimeters of cyber defense of cloud infrastructure for many intellectual transport systems (ITS). In particular, one of the ways to enhance efficiency for the ITS is a better interaction with services on the wide area network, for example, with services of electronic cards and satellite pictures, access to the electronic schedule, etc. is. Under the conditions of more sophisticated cyber attacks to transport cloud infrastructures, one of the major tasks, facing operation services, is an issue of ensuring their cyber defense. It, in turn, leads to the necessity of financial investment into the cyber security systems (CSS) of cloud infrastructures on transport (CIST). One of the drawbacks of the previous research is the fact that authors generally investigated numerical values of metrics for expected losses, when modeling risks of cyber security. One of the options to tackle these issues and, in particular, to assess the risks, connected with financing of CIST CSS, is introduction of the intellectualized decision-making support systems (IDMSS) [4]. Similar systems allow to make rational decisions on investing in the CIST protection tools development. It should be noticed that the mathematical aspect of the IDMSS in cyber security issues [5, 6] is expressed in different models and algorithms, giving the specialists a chance to intellectualize the support of decision-making. In the article the model for IDMSS, according to the discrete procedure of the CIST CSS financing, is offered. The model is based on the decision of a bilinear multistep quality game with two terminal surfaces.

The work is performed within grant financing of the AP05132723 project "Development of Adaptive Expert Systems in the field of Cyber Security of Crucial Objects of Informatization" (Republic of Kazakhstan).

V. Lakhno is Head of the Department of cybersecurity, European University, Kyiv, Ukraine (e-mail: Valss21@ukr.net).

B. Akhmetov is Rector of the Caspian State University of Technologies and Engineering named after Sh. Yessenov, Aktau, Republic of Kazakhstan (e-mail:berik.akhmetov@kguti.kz).

V. Malyukov is with Department of Information Systems and Mathematical Disciplines, European University, Kyiv, Ukraine (e-mail: volod.malyukov@gmail.com).

T. Kartbaev is Head of the Department IT-engineering, Almaty University of Power Engineering and Telecommunications , Almaty, Republic of Kazakhstan (e-mail: Kartbaevt@gmail.com).

II. Research Objective

Application of the CIST and ITS requires the innovative approaches to cyber security management. The multistep quality game with two terminal surfaces is considered in this research [7]. It includes player 1 $(U)-$ a cyberdefender (further the CIST and ITS defender, for instance); player 2 $(U)-$ a malefactor (hacker). Players 1 and 2 manage a dynamic system. The system is set by the system of the bilinear discrete equations with dependent movements. As the players are supposed to

finance the CSS and the means to overcome boundaries of the CIST and ITS cyber defense respectively, it is necessary to find a number of strategies they employ. Two terminal surfaces M_0, N_0 are also set. The purpose of the defender is to bring the dynamic system onto the terminal surface M_0 by means of his management strategies. It is accepted that the hackers financial strategy is arbitrary. The purpose of the hacker to bring the dynamic system onto the terminal surface N_0 by means of his management strategies, whatever are the defenders actions. In the course of the decision-making it is necessary to find the varieties of starting states of the objects and their strategies, which allow them to bring the system onto one or another surface [7]. If the time of interaction of the defender and hacker is limited to one step, we receive the decision of a one-step game in the class of mixed strategies. The decision is made by means of domination methods for infinite multistep games [8].

III. Literature Overview

As it was noted in $[1-3]$ virtually all companies, represented in the cloud computing segment, including transport [4], are forced to pay close attention to cyber defense of the cloud infrastructure from cracking by malefactors. Various "holes" in cyber security are periodically found even in the large companies. To the full extent it is referred to the objects of crucial information infrastructure as well, in particular on transport [1, 4]. It is obvious that CSS financing, including CIST, is a permanent task. In the era of globalization and digitalization of economies, the issue of CSS financing efficiency assessment became one of the first priorities for cyber security services and information protection. In the recent years alone, a large number of publications is devoted to this area of research [3, 4, 6]. The main disadvantage of many works is the lack of real recommendations on the financing strategy development of cloud infrastructures CSS. In particular, it concerns a perspective of the modeling of active financial counteraction to an attacking party. The works, devoted to application of different expert solutions [5] and decision-making support systems [6, 9] for the choice of a CSS financing strategy, became an original direction of publications in this area of research. A lack of these research and as well as the models, offered by the authors in the works [10-12] is the lack of unambiguous results of modeling for the situations, in which financial resources of the attacking party are not limited. It is worth noting that many models, for instance, described in [1315], do not allow to find the effective recommendations and CSS financing strategy of complex informatization objects, in particular transport cloud infrastructure. The results of research, presented in [13-15], do not provide the party of cyber defense with a definite answer to the question: how to develop the strategy, given the attacking party has a financial resource, sufficient for cracking, and the protection has not used its financial resource correctly. It means the mistakes have taken place in the course of forming an expenditure side of the budget on compatible effective CSS. The considered models [14-17] do not allow assessing the risk of financial resources loss by the defense party as well. Ii is possible to eliminate this defect of the previous research by different authors at the expense of application of the theoretical methods of differential and multistep games of quality with several terminal surfaces [7, 18, 19]. The approaches, stated in the works [8, 9, 20], are inapplicable for such differential and multistep games. The theoretical methods of differential and multistep games of quality with several terminal surfaces can be effectively implemented in the intellectualized decision-making support systems [19]. It will certainly increase the efficiency of forecast calculations for the CSS financial losses risk assessment. Taking into account the debatability of the provisions, stated in the works [7, 18, 19, 20], the issue of further development of models for the DMSS in CSS financing tasks is still relevant, and first of all, for the objects of critical information infrastructure, which transport cloud infrastructures can certainly be referred to.

IV. Models and Methods

For the solution of the task, financial resources are required for both players (the defender and the hacker). For example, the hacker can purchase special software for cracking, bribe personnel, resort to phishing or apply DoS/DDoS attacks (other strategies are also possible [11-13]). We accept that for the set time frame $\{1...T\}$ (T - a natural number) the defender has $d\,(0)$ of allocated financial resources, whereas the hacker has $h\,(0)$. These resources predetermine a forecast, at the timepoint , the value of the defender and the hackers financial resources for achievement of the purposes. We note that for a case of comparison of decisions of two games multistep and one-step we will come into coincidence of sets of starting states of financial resources of the defender and the hacker with the following property. Property: a set of the players preferences, proceeding from which he achieves the purpose in steps, matches a set of starting states of financial resources, from which he achieves the purpose in a single step, applying the optimum mixed strategy at optimum counteraction by the other player in the class of mixed strategies with a probability $\frac{1}{T}$. The probability $\frac{1}{T}$ means a risk of the purpose achievement by one player. And, on the other hand, for the other player it means a risk of falling short of the purpose. In the language of "finance" it is interpreted as a risk of financial resources loss by either the defender or the hacker. At an initial timepoint the player (the defender) multiplies a value $d\,(0)$ by a coefficient (rate of change, growth) $a\,(t)$ and selects the value $u\,(t)$ ($u\,(t)\,\epsilon[0,1]$). The later defines a defenders resource share $a\,(t)$ $\times a\,(t)$, spent by him at a timepoint . Similarly, at a timepoint the hacker multiplies a value $h\,(t)$ by a coefficient (rate of change, growth) $\beta(t)$ and selects the value $v\,(t)$ ($v\,(t)\,\epsilon[0,1]$). The later defines a hackers resource share $\beta(t)\,\times\,h\,(t)$, spent by him for cracking the CIST at a timepoint t. Let r_1 be the efficiency of investing funds in CSS. In other words r_1 is the coefficient showing how much financial resources the hacker will need to crack the CIST, which is to be protected by the defender, spending a financial resource unit for this purpose. Let r_2 be the efficiency of investing funds in the means of CIST cracking. In other words r_2 is the coefficient showing how much financial resources the defender will need to protect the CIST, which is to be cracked by the hacker, spending a

financial resource unit for this purpose. Proceeding from all above mentioned, the defender and hackers financial resources change dynamics is set by the following system of the discrete equations:

$$d\,(t+1) = \alpha(t)\cdot d(t) - u(t)\cdot\alpha(t)\cdot d(t) - r_2\cdot v(t)\cdot\beta(t)\cdot h(t) \quad (1)$$

$$h\,(t+1) = \beta(t)\cdot h(t) - v(t)\cdot\beta(t)\cdot h(t) - r_1\cdot u(t)\cdot a(t)\cdot d(t) \quad (2)$$

Then at a timepoint t accomplishment of one of four conditions is possible:
$1) d(t) \geq 0, h(t) < 0$. If this condition is true, it implies that the procedure of CSS financing is complete. At the same time, the CIST hacker did not have enough financial resources to overcome protection;
$2) d(t) < 0, h(t) \geq 0$. If this condition is satisfied, then the procedure of financing of CSS is complete. The CIST defender did not have enough financial resources for protection.
$3) d(t) < 0, h(t) < 0$. If this condition is satisfied, then the procedure of CSS financing is complete. However, the defender of CIST and the hacker did not have enough financial resources to achieve their purposes.
$4) d(t) \geq 0, h(t) \geq 0$. If the fourth condition is satisfied, then the CIST CSS financing procedure is to be continued further. The values $d(t), h(t)$ show the CSS financing result at an interval [0,T] Financing of the CIST CSS is considered in our work within the scheme of a position multistep game with the complete information [7, 8, 19]. Within this scheme, the CIST CSS financing process generates two tasks: 1) from the point of view of the first allied player; 2) from the point of view of the second allied player [7, 8, 19]. Owing to symmetry, we will be limited to consideration of the task from the point of view of the first allied player. The second task is being solved similarly. Let T be a set $\{0, 1..., T\}$
$Definition$. The strict strategy of the first allied player is a function $u : T \cdot [0,1] \cdot [0,1] \to [0,1]$, which puts the value $u(t,(d,h)) : 0 \leq u(t,(d,h)) \leq 1$. to the information status (or position) $(t,(d,h))$ The strict strategy of the first allied player is a function which puts the value $u(t,(d,h))$ to the information status at a timepoint . This value determines a financial resource share of the defender which he was going to spend for the CSS at the moment t.There are no assumptions concerning the opposing players awareness (within the scheme of a position multistep game). It is equivalent to assumption that the opposing player selects his own managing influence on the basis of any information. Having chosen a strategy in the task 1, we determine a set of the first players "preference" W_1. Also W_2 is a set of such starting states $(d(0), h(0))$ of the defender and hackers financial resources, which have the property, formulated below. $Property$: for the starting states W_1 there is the defenders strategy which, for any implementations of the hackers strategy, "brings", at one of timepoints t, a system status $(d(0), h(0))$ to the one which satisfies the condition (1). At the same time, the hacker has no strategy which can "lead" to accomplishment of the conditions (2) or (3), at one of the previous timepoints. The defenders strategy (financial component) having the specified property is to be called $optimum$. The solution of the task 1 consists in finding of a set of the defenders preference and his optimum strategy. The task from the point of view of the hacker is similarly set. Owing to the symmetry of task setting, it is enough to be limited to the solution of the task 1, as the solution of the task 2 is found in the same way. The solution of the task 1 is found by means of tools of the theory of multistep quality games with the complete information [79, 19]. These tools allow finding the solution at any ratios of game parameters. The solution, i.e. sets of "preference" W_1 and optimum strategies $u*(.,.)$ at all ratios of game parameters, is shown in the article.

Case a) $\alpha \leq \beta$.

$$W_1^i = \{(d(0),h(0)) : k(i-1)\cdot\beta\cdot h(0) \leq r_1\cdot\alpha\cdot d(0) \prec k(i-2)\cdot\beta\cdot h(0)\}, i = 1,.. \quad (3)$$

$$u_* = \{u_*(0,(d,h)),...,u_*(i-1,(d,h))\},$$
$$u_*(t,(d,h)) = \{[1-(r_2\cdot\beta\cdot h)/(a\cdot d)]\}, for(d,h)\epsilon R_+^2 \quad (4)$$

$d > r_2\cdot\beta\cdot h$ and is not provided otherwise;$t = 0, 1, ..., i-1$
Where

$$k(i) = 1 + r_1\cdot r_2 - (r_1\cdot\alpha\cdot\beta)/(\beta\cdot k(i-1)); k_{-1} = 0, \quad k_0 = 1 + r_1\cdot r_2; \quad (5)$$

$$W_I = \bigcup_{i=1}^{\infty} W_I^i \quad (6)$$

The beam

$$r_1\cdot 2a\cdot d(0) = \left\{\left\lfloor 1 + r_1\cdot r_2 + ((1+r_1\cdot r_2)^2 - 4\cdot r_1\cdot r_2\cdot\alpha/\beta)^{0.5}\right\rfloor/2\cdot\beta\cdot h(0)\right\} \quad (7)$$

will be a barrier [7]. The barrier is a case, when from the statuses

$$(d(0),h(0)) : r_1\cdot\alpha\cdot d(0) \leq \left\{[1 + r_1\cdot r_1 + \left((1+r_1\cdot r_1)^2 - 4\cdot r_1\cdot r_2\cdot\tfrac{\alpha}{\beta}\right)^{0.5}]/2\cdot\beta\cdot h(0)\right\} \quad (8)$$

the defender cannot achieve the purpose at some timepoint. Case b) $\alpha \succ \beta, r_1\cdot r_2 \geq 1$. In this case a set of the defenders preference W_1 will be consolidation of a finite number of the sets W_1^i , i.e.$(N+2)$ sets,
where $N : k(i) \succ r_1\cdot r_2\cdot\frac{\alpha}{\beta}, i = 0, ..., N-1; k(N) \leq r_1\cdot r_2\cdot\frac{\alpha}{\beta}$,

$$W_1^i = \{(d(0),h(0) : k(i-1)\cdot\beta\cdot h(0) \leq r_1\cdot\alpha\cdot d(0) \prec k(i-2)\cdot\beta\cdot h(0))\}, i = 1, ..., N+1; \quad (9)$$

$$W_1^{N+2} = \{(d(0),h(0) : r_1\cdot r_2\cdot\beta\cdot h(0) \leq r_1\cdot\alpha\cdot d(0) \prec k(N)\cdot\beta\cdot h(0))\}. \quad (10)$$

The optimum financial strategy $u_* = (u_*(0,(d,h)),...,u_*(N+1,(d,h))$is to be found as follows: $u_*(0,(d,h)) = \{0, for(x,y)\epsilon R_+^2, a\cdot d > r_2\cdot\beta\cdot h\}$, and is not provided otherwise $u_*(t,(d,h)) = \{[1-(r_2\cdot\beta\cdot h)/(\alpha\cdot d)], for(d,h)\epsilon R_+^2, \alpha\cdot d > r_2\cdot\beta\cdot h\}$, and is not provided otherwise; $t = 1, ..., N+1$

Case c) $\alpha \succ \beta, r_1\cdot r_2 \prec 1$. In this case a set of the defenders preference W_1 will also be consolidation of a finite number of the sets W_1^i . i.e. $(N + i_(*) + 2)$ sets, where $N : k(i) \succ \frac{\alpha}{\beta}, i =$

$0, ..., N-1; k(N) \leq \frac{\alpha}{\beta}; i_*$- the minimum integer non-negative number provided by the inequality $k(N) \cdot (\beta/\alpha)^{i_*+1} \prec r_1 \cdot r_2$. There after

$$W_1^i = \{(d(0), h(0) : k(i-1) \cdot \beta \cdot h(0) \leq r_1 \cdot \alpha \cdot d(0) \prec k(i-2) \cdot \beta \cdot h(0))\}, i = 1, ..., N+1 \text{ If } i_* = 0, \quad (11)$$

then

$$W_1^i = \{(d(0), h(0) : k(i-1) \cdot \beta \cdot h(0) \leq r_1 \cdot \alpha \cdot d(0) \prec k(i-2) \cdot \beta \cdot h(0))\}, \quad (12)$$

$$i = 1, ..., N+1; W_1^{N+2} = \left\{d(0), h(0) : r_(1) \cdot r_(2) \cdot \beta \cdot h(0) \leq r_(1) \cdot \alpha \cdot d(0) \prec k(N) \cdot \beta \cdot h(0)\right\}. \quad (13)$$

The optimum strategy listing in this case is just the same as in the case b). If $i_* > 0$, then

$$W_1^{N+1+i} = \left\{(d(0), h(0) : k(N) \cdot (\frac{\beta}{\alpha})^j \cdot \beta \cdot h(0) \leq r_1 \cdot \alpha \cdot d(0) \prec k(N) \cdot (\tfrac{\beta}{\alpha})^{j-1} \cdot \beta \cdot h(0))\right\}, \quad (14)$$

$$i = 1, ..., i_* W_1^{N+1+i} = \{d(0), h(0) : r_1 \cdot r_2 \cdot \beta \cdot h(0) \leq r_1 \cdot \alpha \cdot d(0) \prec k(N) \cdot (\tfrac{\beta}{\alpha})^i \cdot \beta \cdot h(0)\right\}. \quad (15)$$

The optimum strategy $u_* = (u_*(0, (d, h)), ..., u_*(N+1+i_*, (d, h)))$ in this case is found as follows: $u_*(i, (d, h)) = \left\{0, for (d, h) \epsilon R_+^2, \alpha \cdot d > r_2 \cdot \beta \cdot h\right\}$, and is not provided otherwise; $i = 0, ..., i_*$,

$u_*(i(d, h)) = [1 - (r_2 \cdot \beta \cdot h)/(\alpha \cdot d)], for (d, h) \epsilon R_+^2, \alpha \cdot d > r_2 \cdot \beta \cdot h, i \geq i_* + 1$ and is not provided otherwise; $t = 1, ..., N+1$. As it was already noted, the defender possesses limited financial resources. Let Q be the maximum value of a resource. Then a set of the defenders preference at such restriction W_1^* will represent the intersection of the set W_1 and the set $\left\{(d(0), h(0)) : (d(0), h(0)) \epsilon R_+^2, d(0) \leq Q\right\}$. i.e. $W_1^* = W_1 \cap \left\{(d(0), h(0)) : (d(0), h(0)) \epsilon R_+^2, d(0) \leq Q\right\}$ A set of the hackers preference is to be found similarly. At the same time, we assume that he possesses limited financial resources. The task 2 is solved in the same way from the point of view of the second allied player. It allows to provide a positive orthant to the plane $(d(0), h(0))$ in the form of three sets (cones with an apex at the point $(0, 0)$). One set (cone) adjoining an axis , is a set preferable to the defender. The second set (cone) is a set preferable to the hacker. The third set (cone) is a neutral set, from the point of view of both players. Actually, this set characterizes the balance property for the defender and the hacker. The players are dealing with financing of protection and cracking respectively. That is the players have the strategies for the statuses belonging to this set, allowing them to continue as much long as possible the CSS financings and CIST cracking. That means the conditions $d(t) \geq 0, h(t) \geq 0$ will be satisfied for any timepoint . The beams, being the borders of the cones, are set by the means of coefficients. These coefficients represent a combination of the parameters, setting the dynamics of CSS financing process and CIST cracking. Therefore, if the initial values$(d(0), h(0))$ of the defender and hackers financial resources are set, it is possible to vary, for instance, these parameters.

TABLE I
THE RESULTS OF THE SIMULATION EXPERIMENT (SE) AT THE CHOICE OF A STRATEGY FOR TRANSPORT CLOUD INFRASTRUCTURES BY THE DEFENDER AND THE HACKER, FOLLOWING THE EXAMPLE OF UKRAINE AND THE REPUBLIC OF KAZAKHSTAN

Number, IE	Modeling results		
	The financial resource of players is not limited	Limitations imposed on a financial resource of players	
1	(d(0), h(0))= (10.0, 13.2); (d(1),h(1))= (12.0, 11.36); (d(2),h(2))= (14.0, 10.36); (d(3),h(3))= (16.0,8.4); (d(4), h(4)) = (18.0, 6.4).	Q=14 Limitation for a financial resource of the defender	(d(0), h(0)) = (7.0, 13.0); (d(1), h(1))= (8.0, 11.0); (d(2),h(2)) = (9.0, 10.0); (d(3), h(3)) = (10.0, 8.0); (d(4),h(4)) = (11.0, 6.0).
2	(d(0), h(0))= (5.0, 10.0); (d(1),h(1))= (4.0, 12.0); (d(2), h(2))= (3.0, 13.0); (d(3),h(3))= (2.0, 15.0); (d(4), h(4))= (1.0, 17.0).	S=16 Limitation for a financial resource of the hacker	(d(0),h(0))= (5.0, 10.0); (d(1), h(1))= (4.0, 11.0); (d(2),h(2))= (3.0, 12.0); (d(3), h(3))= (2.0, 14.0); (d(4),h(4))= (1.0, 15.0).
3	(d(0), h(0))= (5.0, 20.0); (d(1),h(1))= (4.0, 16.0); (d(2), h(2))= (3.0, 12.0); (d(3),h(3)) = (2.0, 8.0), (d(4); h(4)) = (1.0, 4.0).	Q=7 Limitation for a financial resource of the defender	(d(0), h(0)) = (5.0, 15.0); (d(1),h(1)) = (4.0, 12.0); (d(2), h(2))= (3.0, 9.0), (d(3),h(3))= (2.0, 6.0); (d(4), h(4)) = (1.0, 3.0).

V. RESULTS OF SIMULATION EXPERIMENTS

The simulation experiments were executed in the earlier described "SSDMI" module [4, 6, 19, 21], and the control computing experiments in the Mathcad packet. The simulation experiment purposes: 1) determination of a set of players strategies (a CIST (cloud infrastructure on transport) defender and a hacker); 2) modeling of the risks parameters, connected to the loss of players financial resources; 3) determination of a set of players starting states and their strategies which allow the CIST defender or the hacker to bring the system upon one or another terminal surface. The results of simulation experiments are shown in table I and in fig. 1-3.

The beam of balance is shown by a solid line with round markers. Areas in fig. 1-3 are shown: 1) The CIST defenders "preference" is below the beam; 2) The hackers "preference" is above the beam. The values of points, received during the simulation experiment, are presented in table I. The defender and hackers movement trajectories are represented by dotted lines with triangular markers. The trajectories are in the defender and hackers preference area respectively. The solid line with square markers shows the limitations imposed on the defender and hackers financial resources. Financial limitations are not obligatory. Since, if, for instance, cybertroops or intelligence agencies act as the hacker, we assume that their financial

resource is not limited, see table I. For the purpose of checking

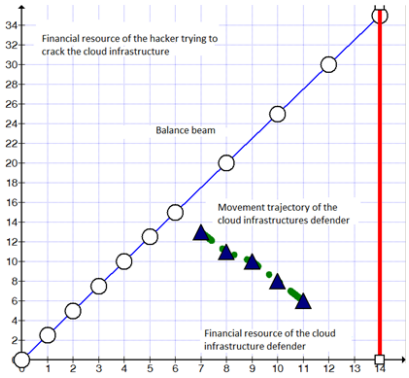

Fig. 1. Results of simulation experiment 1. Trajectory of the CIST defender movement.

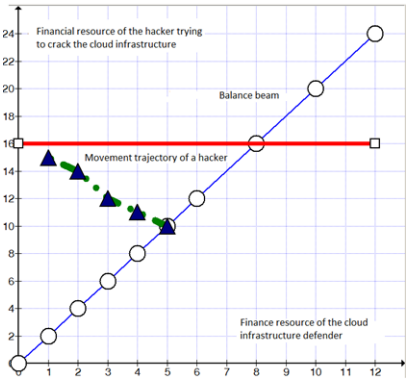

Fig. 2. Results of simulation experiment 2. Trajectory of the hacker movement.

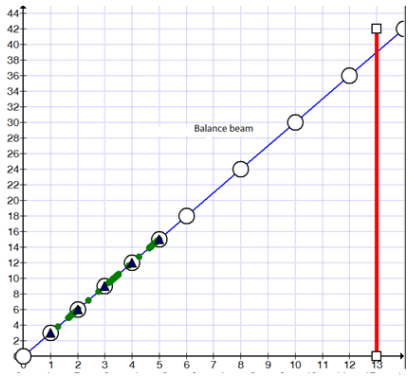

Fig. 3. Results of simulation experiment 3. System ”stability”.

the adequacy of the carried-out calculations, approbation of the results received by the means of ”SSDMI” is also executed for real projects in the field of cyber security of transport cloud infrastructures enterprises in Ukraine and Kazakhstan [6, 19, 21]. In [19] the acceptable operational accuracy of the ”SSDMI” programming module in the ratio with the simulation experiments results is confirmed.

VI. Discussion of Simulation Modeling Results

In fig. 1-3 the following cases are considered: a) in fig. 1 the case, in which the player the CIST defender has advantages in the amount of initial financial resources, is shown. That is these resources are in a set of the defenders preference. The defender, applying the optimum strategy, will achieve his purpose, as he has enough financial resources, despite their limitation at the initial timepoint. The defender's purpose is to bring the system status onto ”his” terminal surface. The set of the beams proceeding from the point (0,0) is considered in a positive orthant of the plane. These beams are set by the ratio: $h = (2.5 - 1/n) \cdot d$.These beams set the first player preference sets for n steps. For example, a set W_1^* is the set:

$$\left\{(d(0), h(0)) : (d(0), h(0)) \epsilon R_+^2, (2, 5 - 1/(n-1)) \leq d(0) \leq h(0) < (2.5 - 1/n) \cdot d(0)\right\}. \quad (16)$$

For example, if $n = 1$, then $W_1^* = \left\{(d(0), h(0)) : (d(0), h(0)) \epsilon R_+^2, 0 \leq h(0) < (1.5) \cdot d(0)\right\}$. The beam: $h(0) = (2.5) \cdot d(0)$ is a balance beam (it is shown by a solid line with round markers). Sets W_1^* are the sets of statuses of the players having the following property. Property: if a game begins from W_1^*,the defender in a single step will achieve the purpose in a single step with probability $(1/n)$, if the defender and the hacker apply the optimum mixed strategy. b) in fig. 2 the situation, in which the hacker using non-optimal behavior of the defender and the fact that starting states of the players are in the hackers preference area, is shown. The hacker has sufficient financial resources and, despite their limitation at the initial timepoint, he ”brings” a system status onto ”his” terminal surface. In a positive orthant of the plane the set of the beams proceeding from the point (0,0) is considered. The beams are set by a ratio: $h = (2.5 + 1/n) \cdot d$. The beams set the hackers preference sets for n steps. The beam $h = 2 \cdot d(0)$ is a balance beam. The sets W_1^* are the sets of statuses of the players having the following property. Property: if a game begins from W_1^*,the defender will achieve the purpose in a single step with probability $(1/n)$, if the defender and the hacker apply the optimum mixed strategy.c) in fig. 3 the situation, when the system starting state is on a balance beam, is shown. The defender and the hacker, applying the optimum strategy, ”move” along the beam. It ”satisfies” both the defender, and the hacker. While implementing the simulation experiment, we show that our model and also its program implementation in ”SSDMI”, are capable to provide the effective support of decision-making in the field of CSS financing. This work continues a number of our publications [4, 6, 7, 19] which state the theoretical and methodological bases of DMSS design, using a bilinear multistep quality game with several terminal surfaces. The approach offered in work, allows eliminating many components of uncertainty in the CSS financial investments modeling processes, in particular, for the CIST, influencing cyber security investments in different parameters. That feature distinguishes our research from the ones of other authors [15, 2225]. The drawback of the model, revealed during the simulation experiment, is the fact that the data retrieved at the choice of strategy of financing the

means of cyber security of transport cloud infrastructures, did not always match the actual data. The maximum deviation of the simulation experiment results from practical data made up 911Further development perspectives of this research is transferring of the accumulated experience to real projects on financing of cyber security means of cloud infrastructures, in particular, on transport in Ukraine and the Republic of Kazakhstan.

RESEARCH FINDINGS. In the article the following findings are received. The model is developed for the intellectualized decision-making support system in the course of financing in cyber security means of transport cloudy infrastructures. The offered model in its basis contains games theory tools. The model is integrated into the intellectualized support system of decision-making. The system allows the ultimate user to assess risks in the course of cyber security means financing. The scientific novelty of the model consists in the fact that unlike the existing approaches, the decision of a bilinear multistep quality game with several terminal surfaces is made. The decision of a bilinear multistep game in the class of strict strategy and also a one-step game in the class of the mixed strategy, found with the help of domination methods, developed for infinite antagonistic games, allowed to assess the risks for the players, who represent the parties of protection and attack respectively, for cloud-based computing infrastructures on transport. The results of the simulation experiment, during which different ratios of the parameters describing the process of financing in cyber security means of cloud-based computing infrastructures on transport, were considered. At the same time, for the party of protection, the financial strategy of the hacker for the cases of limited and unlimited financial resources, were analyzed. It is shown that the class of games, considered in the article, allows to adequately describe the process and to find the optimum financial strategy of the protection party. The decision, made theoretically and confirmed during the simulation experiment, assumes accounting financial components of protection strategy at any ratios of the parameters describing financing process. On the basis of the findings received due to the developed intellectualized decision-making support system, the conclusion about the risks of financial resources loss by the players for cyber protection and cracking of transport cloud-based computing infrastructures respectively, is drawn.

REFERENCES

[1] K. Sagar, A. Kumar, G. Ankush, T. Harika, M. Saranya,and D. Hemanth. "Implementation of IoT based railway calamity avoidance system using cloud computing technology", *Indian Journal of Science and Technology* 9 (17), 1–5 (2016).

[2] S. Ramgovind, M. Eloff,and E. Smith, "The management of security in cloud computing",*In Information Security for South Africa (ISSA)*, 1–7 (2010).

[3] A. Sajid, H. Abbas,and K. Saleem,"Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges", *IEEE Access* 4, 1375-1384 (2016).

[4] O. Petrov, B. Borowik, M. Karpinskyy, O. Korchenko,and V. Lakhno, "Immune and defensive corporate systems with intellectual identification of threats, Pszczyna : lska Oficyna Drukarska", 222 p. ISBN: 978–83–62674–68–8 (2016).

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

[6] V. Malyukov, "A differential game of quality for two groups of objects",*Journal of Applied Mathematics and Mechanics*,Vol. 5 (55), 596–606 (1991).

[7] I. Krass, V. Malyukov, "O sushhestvovanii optimal'nyh smeshannyh strategij dlja nekotoryh antagonisticheskih igr, Optimizacija" 20 (37),135–146 (1978).

[8] M. Manshaei, Q. Zhu, T. Alpcan, "Game theory meets network security and privacy",*ACM Computing Surveys*, 3 (45), 1-39, (2013).

[9] N. BenAsher, C. Gonzalez, "Effects of cyber security knowledge on attack detection",*Computers in Human Behavior*, (48), 51-61, (2015).

[10] J. Grossklags, N. Christin, J. Chuang, "Secure or insure?: a game-theoretic analysis of information security games",(Conferense) 17th international conference on World Wide Web, Beijing, China, 21-25 April 2008 : proceedings. New York, ACM, 2008. 209-218.

[11] H. Cavusoglu, B. Mishra, S. Raghunathan, "A model for evaluating IT security investments",*Communications of the ACM*,7 (47), 87-92 (2004).

[12] A. Fielder, E. Panaousis, P. Malacaria, Decision support approaches for cyber security investment, Decision Support Systems, Vol. 86, 13-23 (2016).

[13] P. Meland, I. Tondel, B. Solhaug, "Mitigating risk with cyberinsurance", *IEEE Security and Privacy*, 13 (6), 38-43 (2015).

[14] A. Fielder, S. Konig, E. Panaousis, S. Schauer, and S. Rass, Uncertainty in Cyber Security Investments. arXiv preprint arXiv:1712.05893 (2017).

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

[16] 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*, 11 (65), 1682-1691 (2014).

[17] V. Malyukov, "Discrete-approximation method for solving a bilinear differential game", *Cybernetics and Systems Analysis*, Vol. 6 (29), 879 888 (1993).

[18] V. Lakhno, V. Malyukov, N. Gerasymchuk, "Development of the decision making support system to control a procedure of financial investment", *Eastern-European Journal of Enterprise Technologies*, 3 (6), 24-41 (2017).

[19] F. Smeraldi, P. Malacaria, "How to spend it: optimal investment for cyber security", 1st International Workshop on Agents and CyberSecurity, Paris, France, 0608 May 2014 : proceedings, New York, ACM, 2014, 8.

[20] B. Akhmetov, B, V. Lakhno, Y. Boiko, A. Mishchenko, "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *Eastern-European Journal of Enterprise Technologies*, 1(2(85)), 4-15 (2017).

[21] M. Chronopoulos, E. Panaousis, and J. Grossklags, "An options approach to cybersecurity investment", IEEE Access (2017).

[22] S. Rass, S. Knig, and S. Schauer, "Uncertainty in games: Using probability-distributions as payoffs", In International Conference on Decision and Game Theory for Security (pp. 346-357). Springer, Cham.

[23] Y. Lee, R. Kauffman, and R. Sougstad, "Profit-maximizing firm investments in customer information security", *Decision support systems*, 51 (4), 904-920 (2011).

[24] T. Moore, S. Dynes, and F. Chang, Identifying how firms manage cybersecurity investment. Available: Southern Methodist University. Available at: http://blog.smu.edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14), 32 (2015).