ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

3

АЛМАТЫ
АЛМАТЫ
ALMATY

2018

МАУ
МАЙ
МАМЫР

NAS RK is pleased to announce that Bulletin of NAS RK scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Вестник НАН РК» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
www: nauka-nanrk.kz, bulletin-science.kz

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Вестник Национальной академии наук Республики Казахстан».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 3, Number 373 (2018), 6 – 14

UDC 004.056

B. B. Akhmetov[1], V. A. Lakhno[2], B. S. Akhmetov[3], V. P. Malyukov[2]

[1]Yessenov University, Aktau, Kazakhstan,
[2]Department of management of information systems and cybersecurity,
European University, Kiev, Ukraine,
[3]Kazakh National Pedagogical University named after Abay, Almaty, Kazakhstan.
E-mail: berik.Akhmetov@kguti.kz, Valss21@ukr.net, bakhytzhan.akhmetov.54@mail.ru,
volod.malyukov@gmail.com

THE CHOICE OF PROTECTION STRATEGIES DURING THE BILINEAR QUALITY GAME ON CYBER SECURITY FINANCING

Abstract. There is developed a model for the module of an intellectualized system for decision-making support on the cyber security means financing of the information object. The model is based on the toolkit use of the theory of multi-step games in which the steps are made alternately by the sides of cyber security and attacker. There was obtained a solution that enables interested parties to evaluate financial strategies for effective cyber security systems construction in the condition of not complete information about the financial state of the attacking party (hackers). The model differs from existing approaches by solving a bilinear multi-step quality game with several terminal surfaces.

In work, there is performed a computational experiment and is given the corresponding results. Confirmed during the simulation experiment solution takes into account the financial components of cyber security strategies at any ratio of parameters describing the process of cyber security financing in the condition of information lack about the financial condition of hackers.

Keywords: objects of informatization, cyber security, multi-step quality game, optimal financing strategies, decision-making support system.

Introduction. The researches of authors [1] have the information that managers of many organizations and companies do not have a deep understanding of the need to solve the permanent task of financing cyber security means (CSM) of their information systems and technologies (IST). As a result, in the condition of increasing amount of cyber threats [2] in combination with the lack of an appropriate funding strategy in CSM there are appeared situations in which there is a high degree of risk associated with the loss of important information or its discrediting. In the coming years, successful cyber attacks will unlikely be the result of one or two technological tools of hacking. Now there is formed a trend according to which hackers will use many different steps and elements to hack into IST.

Most small and medium-sized companies and organizations are limited to the standard procedure of IST protection, which in practice are focused on the deployment of antivirus systems and on the configuration of firewalls. However, we will note that such a strategy of cyber security (CS) (in some cases caused by limited financial resources from the protection side) may subsequently have a significant impact on the prospects of being attacked by computer intruders. And even in a situation where the

allocated budget for CSM is sufficiently large, the problem of evaluating the effectiveness of investment strategies in cyber security is a difficult task. This, in particular, is due to the ever-changing landscape of cyber threats and new IST vulnerabilities, and uncertainties in assessing the risks of CSM financing.

According to [3, 4] the main problems faced by companies and organizations at assessing and selecting rational strategies for investing in CSM of the informatization objects (IO) remain: the lack of a methodology for determining the exact values for risk assessment related to CSM financing; the complexity of the proposed models and methods, in particular their algorithmization and subsequent implementation, for example, in decision-making support systems (DMSS) for the selection of funding strategies for CSM; the lack of methodology, for evaluation the strategies of the attacking party, for example, when its financial resource is not limited, etc.

For example, massive DDoS attacks can last several days long [3, 4]. This is an atypical situation for a protected resource. As it was noted in [3] not each hacker can deal with such massive attacks. In works [1, 2] there was given the information that daily DDoS attacks of mixed type (UDP-amplification and SYN-flood) could cost the customer several tens of thousands of dollars.

All this in combination makes the task of continuing the researches in the direction of developing new methods and models for the selection of rational strategies for CSM financing, particularly for situations where new cyber threats cause a change in the level of risks for organizations and companies, and, therefore, lead to the necessity revision of its own financing strategies in the CSM.

The purpose of the article is to develop a model for financing the cyber security system in the condition of not complete information about the financial state of the attacking party (hackers). It is also necessary to find sets of preference and optimal financial strategies for protection the information object in a risk environment.

Literature review. In works [5, 6] it was shown that the current stage of the development of information systems and technologies is accompanied by a trend of funding increase for hacker attacks. In particular, the US secret services [7] for several months sought for hackers funding sources who manipulated the election campaign in the United States. In work [8] it is noted that investing in hacker groups is one of the priority projects of the DPRK government. At the same time, there are developed the works in the segment of developing new methods and models for decision-making support on the choice of strategies for investing in cyber security of various information objects. In work [9] there was shown that the decision-making on cyber security financing is a constant task. However, the lack of many works and, in particular of [10, 11], is the lack of realistic recommendations for the development of financing strategies for the cyber security of IO. In particular, there are no researches suggesting models that take into account strategies of active financial counteraction to hackers who can attack various IO. A new direction are the researches devoted to the application of various expert [12] and decision-making support systems [13, 14] for the selection of financing strategies for cyber security of the IST. The disadvantage of these researches [15, 16] is the lack of unambiguous modeling results. Most of the models considered in [13-16] do not allow to find effective recommendations and financing strategies for CSM of complex information objects. The models proposed in [17, 18] also do not allow to assess the risk of losing financial resources by the cyber protection side. In work [19] there are proposed the models based on the theory of games for evaluating the effectiveness of financing in CSM. The authors, however, did not take into account many factors, for example, the change in the financial components of the attacking party. The elimination of this disadvantage in previous researches of various authors is possible due to the application of methods of the theory of differential and multi-step quality games with several terminal surfaces [20-22]. This will improve the effectiveness of the forecast calculations from the IO protection side on the risk assessment of financial losses in the CSM.

Therefore, as the analysis of the performed researches has shown the problem of the further development of models for DMSS in the tasks of cyber security means financing remains relevant. In particular, it is necessary to consider situations with incomplete information about the financial state of the attacking party in the process of finding sets of preference and optimal financial strategies for protection the information object.

Models and methods. The article continues the research of authors [14, 20, 21], in which the apparatus of the game theory is used, there are considered two sides: player #1 – an information system defender (ISD); player #2 is a hacker. Both players use financial resources to achieve their goals [21]. We

assume that for a given period of time $\{0,1,...,T\}$ (T is a natural number) the players 1 and 2 have, respectively, $x(0)$ and $y(0)$ financial resources. There is an interaction of players. This interaction will be described as a bilinear multi-step game with alternately steps with incomplete information. Unlike the game with complete information, the first player does not know exactly the initial state of the second player, but the distribution function of its initial states $F_0(\cdot)$ is known. The steps in such a game are made alternately. At even moments of time, the first player makes the step, at uneven moments of time the second player makes the step.

Let $t = 2n, x(t)$, $x(t+1)$ – the state of the first player at time t, $t+1$. $x_2^{\xi}(t), x_2^{\xi}(t+1)$ – random states of the second player at time t, $t+1$. Then the states of the players at time $t+1, t+2$ are determined from the relations:

$$x(t+1) = \alpha(t) \cdot x(t) - u(t) \cdot \alpha(t) \cdot x(t); \quad (1)$$

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

$$y^{\xi}(t+2) = \beta(t) \cdot y^{\xi}(t+1) - \nu(t) \cdot \beta(t) \cdot y^{\xi}(t+1); \quad (3)$$

$$x(t+2) = x(t+1) - s_2(t) \cdot \nu(t) \cdot \beta(t) \cdot y^{\xi}(t+1); \quad (4)$$

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

Let describe the game process.

At time $t \in \{0,2,4,...,2 \cdot n\}$ the first player multiplies the value $x(t)$ on the coefficient (rate of change, growth rate) $\alpha(t)$ and choose the value $u(t)$ $(u(t) \in [0,1])$, which determines the amount of the resource of the first player $\alpha(t) \cdot x(t)$, allocated to the cyber security of IST at time t. Then the states of the players at the moment of time $t+1$ are determined by the relations (1) and (2). Consequently, the hacker is forced to allocate for IST hacking the value $s_1 \cdot u(t) \cdot \alpha(t) \cdot x(t)$ of financial resources. Coefficient s_1 determines the "effectiveness" of second player investment for the development or purchase of IST hacking tools of the first player's.

If the condition $P(y^{\xi}(t+1) < 0) \geq p_o, (0 \leq p_o \leq 1)$ is satisfied, then the first player, using his financial resources, guarantees the protection of IST with a probability p_0. We assume that from the side of the first player the procedure of CSM financing is completed. Otherwise, the first player continues to finance CSM.

The hacker makes his step. He acts just like the first player. And then the states of the players are determined by the relations (3) and (4). If it turns that after hacker's step the condition $P(x(t+2) > 0) < p_1, (0 \leq p_1 \leq 1)$, will be satisfied, then the attacker damaged the IS with a probability more than $(1 - p_1)$ and the procedure of CSM financing is completed.

The first player tries to find a lot of his initial states, which have the following property. *Property*: if the game starts from the initial states, then the first player can ensure the cyber security of his IST by the selection the control actions $u(0),...,u(t)(t = 2n)$ with a probability more than p_0. In this case, the strategy chosen by player 1 prevents the hacker's damage to the IST with a probability more than $(1 - p_1)$. The set of such states will be called **the set of preferences** of the first player.

Let denote by Φ - the set of distribution functions of one-dimensional random variables, by $2n$ - the closest natural even number to T, $T^* = \{0,2,...,2n\}$ - the set of natural numbers.

Definition. A pure strategy $u(.,.,.)$ of the first player is a function: $u(.,.,.): T^* \times R_+ \times \Phi \to [0,1]$, such that $u(t,x,F) \in [0,1], (F \in \Phi)$.

That is, the strategy of the first player is a rule that allows the first player on the basis of available information to determine the value of the financial resource that player 1 allocates for the development or modernization of CSM. Player 2 chooses his strategy $\nu(.)$ on the basis of any information.

The aim of the first player is to find a set of preferences, as well as finding his strategies, by applying of which he will meet the conditions that allow the protection side to finish the financing procedure in CSM. The strategies of the first player with these properties will be called his optimal strategies. The formulated game model corresponds according to the classification of the decision-making theory to the decision-making task under risk conditions. In addition, such a model is a bilinear multi-step quality game with several terminal surfaces with alternate steps. Finding the sets of preference of the first player and his optimal strategies depend on a set of parameters.

In order to describe the sets of preference of the first player, you must use two values:

$$c(0) = \inf\{c'\},\ d(0) = \inf\{d'\},$$

$$F_0(c') \geq p_0,\ F_0(d') \geq p_1.$$

The first player's sets of preference and his optimal strategies are found for $T = 1,3,...$ We will use the notation for sets of preference:

$V_1^T(p_0, p_1)$ – the set of preferences of the first player from which he successfully completes the CSM financing procedure by the T steps.

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

Optimal strategy:

$$u_*(1, x, c) = \begin{cases} 1, \textit{ for } s_1 \cdot \alpha \cdot x \geq c; \\ 0, \textit{ otherwise.} \end{cases} \tag{5}$$

Let consider various cases of the game parameters ratio.

Case 1. $p_0 = p_1$.

1.1. $\alpha > \beta$.

Let $k_0 \in N$ (the set of natural numbers):

$s_1 \cdot \alpha \cdot s_2 \leq \left(\frac{\alpha}{\beta}\right)^{k_0}$, $s_1 \cdot \alpha \cdot s_2 > \left(\frac{\alpha}{\beta}\right)^{k_0+1}$ then

$$V_1^T(p_0, p_0) = \left\{x(0): c(0) \leq s_1 \cdot \alpha \cdot \left(\frac{\alpha}{\beta}\right)^k x(0); c(0) > s_1 \cdot \alpha \cdot \left(\frac{\alpha}{\beta}\right)^{k-1} x(0)\right\},$$

where $T = 2k + 1 \leq 2k_0 + 3$.

The set

$$V_1^{2k_0+s}(p_0, p_0) = \left\{x(0): c(0) > s_1 \cdot \alpha \cdot \left(\frac{\alpha}{\beta}\right)^{k_0+1} x(0); c(0) \leq \left(\alpha / (s_2 \beta)\right) x(0)\right\},\ V_1^T(p_0, p_0) = \varnothing.$$

For $T = 2k + 1 \geq 2k_0 + 7$.

Optimal strategy

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

The beam $\left\{x(0): x(0) \in R_+, c(0) \in R_+\ c(0) = \left(\alpha / (s_2 \cdot \beta)\right) x(0)\right\}$ will be a barrier [22]. It means that from the states $x(0): c(0) > \left(\alpha / (s_2 \cdot \beta)\right) x(0)$ it is impossible for the first player to reach the goal with probability $p \geq p_0$. This beam can be called a stochastic beam of balance for the procedure of CSM IS financing.

1.2. $\alpha \le \beta$.

1.2.1. $s_1 \cdot \alpha \cdot s_2 \le 1$.

In this case, we will receive $V_1^T(p_0, p_0) = \varnothing$ for $T = 2k+1 \ge 3$.

1.2.2. $s_1 \cdot \alpha \cdot s_2 > 1$.

1.2.2.1. $s_1 \cdot \beta \cdot s_2 > 1$.

In this case, we will receive $V_1^T(p_0, p_0) = \varnothing$ for $T = 2k+1 \ge 3$.

1.2.2.2. $s_1 \cdot \beta \cdot s_2 \le 1$.

In this case, we will receive $V_1^3(p_0, p_0) = \left\{x(0) : c(0) \le \left(\alpha / (s_2 \cdot \beta)\right) x(0), c(0) > s_1 \cdot \alpha \cdot x(0)\right\}$.

Optimal strategy

$$u_*(n, x, c) = \begin{cases} 1, \textit{ for } s_1 \cdot \alpha \cdot x \ge c; \\ 0, \textit{ otherwise.} \end{cases} \tag{7}$$

$V_1^T(p_0, p_0) = \varnothing$ for $T = 2k+1 \ge 5$.

Case 2. $p_0 > p_1$.

In this case, we will receive $V_1^T(p_0, p_1) = V_1^T(p_0, p_0)$.

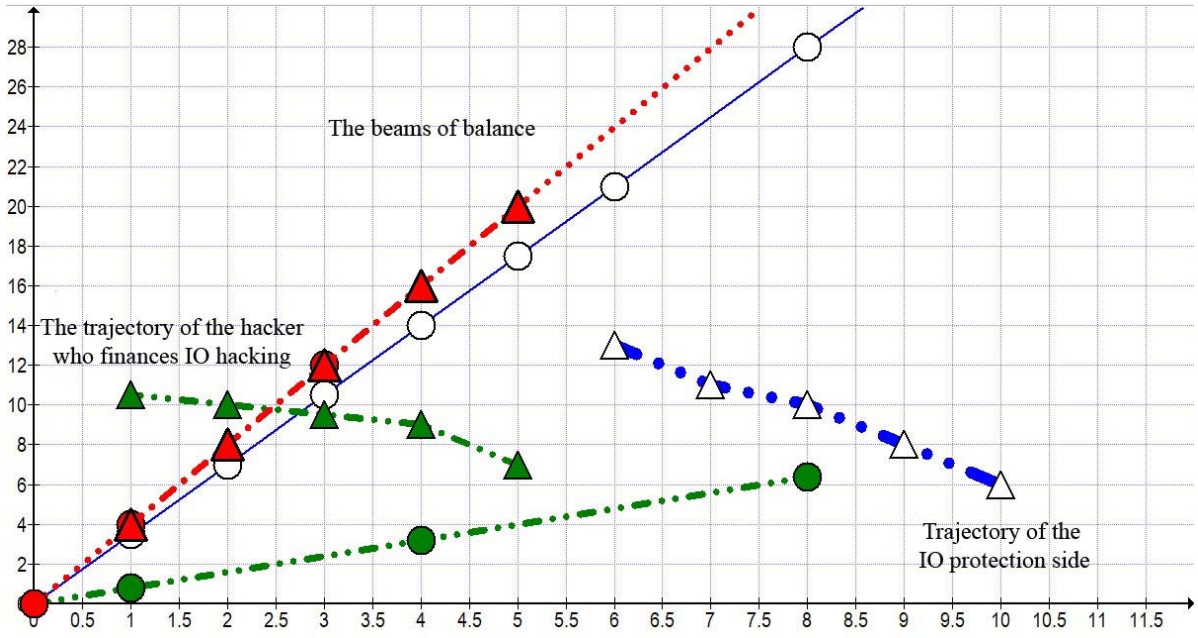
Case 3. $p_0 < p_1$.

In this case we will receive $V_1^T(p_0, p_1) = V_1^T(p_0, p_0) \cap \left\{x(0) : d(0) \le \left(\alpha / (s_2 \cdot \beta)\right) x(0)\right\}$.

The model proposed in the article was applied in the MathCad environment.

Computational experiment. The aims of the computational experiment: to determine the sets of strategies of players 1 and 2; to assess the risks that are associated with the loss by the players their financial resources for IO protection and hacking the cyber security perimeter; to check the adequacy of the proposed model.

The results of three computational experiments are shown on figure.



The results of computational experiments on the choice of rational financial strategies of the informatization object defender

The designations adopted on the figure:

1) the beams of balance are shown in the figure by the lines with round markers;

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

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

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

The solution of the game is given for all cases of the game parameters ratio. Using the game results we find the optimal behavior of the IO defender in the case when he does not know exactly the state of the financial resource of the hacker, but only the distribution function of his states is known. Note that such a situation could arise if the hacker uses his mixed strategy in order to complicate the IO cyber protection.

The discussion of the modeling results.

Computational experiment for the protection side. The game results are shown in blue lines (trajectory and balance beam). A positive orthant on the plane $(x(0), c(0))$. is considered. Next, in this orthant, we consider the set of beams from the point (0,0). These beams are given by the ratio: $c = \left(3.5 - \frac{1}{n}\right) \cdot x$. These beams specify the set of preferences of the first player (IO defender) for *n* steps with the probability p_0, i.e. it is assumed that $p_0 = p_1$.

For example, the set $V_1^T(p_0, p_0)$ is the set

$$\left\{(x(0), c(0) : x(0), c(0)) \in R_+^2, \left(3.5 - 1/(n-1)\right)x(0) \le c(0) < \left(3.5 - 1/(n)\right)x(0)\right\}.$$

At $n = 1$ there will be $V_1^1(p_0) = \left\{(x(0), y(0) : x(0), c(0)) \in R_+^2, 0 \le c(0) < (2.5)x(0)\right\}$.

The beam: $c(0) = (3.5) \cdot x(0)$ will be a beam of the stochastic balance.

Computational experiment for the hacker's side. The game results are shown in green lines (trajectory and balance beam). Test calculation 2, for the second player's (hacker's) sets of preference there is considered the symmetric task for the second player. At the positive orthant, we consider the set of beams from the point (0,0). These beams are given by the ratio: $y = \left(0.8 + \frac{1}{n}\right) \cdot c$. These beams specify the set of preferences of the second player for *n* steps. For example, the set $V_2^n(p_0, p_0)$ is the set

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

At $n = 1$ there will be $V_2^1(p_0) = \left\{(c(0), y(0) : c(0), y(0)) \in R_+^2, 0 \le y(0) < (1.8)c(0)\right\}$.

The beam: $y(0) = (0.8) \cdot c(0)$ will be a beam of the stochastic balance.

Computational experiment for equal financial strategies of players. The third test calculation will correspond to the "movement" along the beam of balance: $y(0) = (3.5) \cdot c(0)$. Here the original task for the first player is considered.

In the course of the computational experiment, it is shown that our model is capable to provide effective decision-making support in the sphere of CSM financing. This work continues a number of our publications [14, 21], in which the theoretical and methodological foundations of DSS design were

described using a bilinear multi-step quality game with several terminal surfaces. The approach proposed in the work allowed to eliminate the disadvantages of the earlier versions of the model, since the complete information on the financial state of the attacking party (hackers) is not taken into account. This distinguishes our research from the works of other authors [9-12].

The disadvantage of the model revealed during the computational experiment is the fact that the obtained data of the predictive estimation at choosing financing strategies in the CSM IO did not always coincide with the actual data. The maximum deviation of the results of the simulation experiment from practical data was 8-12%.

Prospects for the development of this research are the further development of the computer model for the DSS "SSDMI" [14, 21].

Thanks. The work was carried out within the framework of grant financing of the project AP05132723 "Development of adaptive expert systems in the field of cyber security of critical information objects" (Republic of Kazakhstan).

Conclusions. The following results were obtained in the article:

– developed a model for financing the informatization object of cyber security system in the absence of complete information on the financial state of the attacking party. The model differs from the known ones by the dynamic programming method that was used to solve the problem with incomplete information, which allows to effectively solve problems in which the information content requires the players' resources, both financial and material;

– conducted a computational experiment. In the course of which it is shown that the proposed model is capable to provide effective decision-making support in the field of cyber security systems financing of various informatization objects. The adequacy of the model was confirmed, the maximum deviation of the results of the computational experiment from practical data was 8-12%.

REFERENCES

[1] Van der Meulen, N. Investing in Cybersecurity. 2015. RAND Europe. https://english.wodc.nl/binaries/2551-full-text_tcm29-73946.pdf

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

[3] Gordon L.A., Loeb M.P., Zhou L. Investing in cybersecurity: Insights from the Gordon-Loeb model // Journal of Information Security. 2016. 7(02). 49. doi: 10.4236/jis.2016.72004

[4] Kelly B.B. Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform // BUL Rev. 2012. 92, 1663. http://search.proquest.com/docview/132833278?accountid=32521

[5] Taylor R.W., Fritsch. E.J., Liederbach J. Digital crime and digital terrorism // Prentice Hall Press. 2014. ISBN: 0-13-114137-6

[6] Rose R. IA3–Hacker culture and mitigation: Al-Qassam cyber fighters and pnc bank. 2014. https://kuldoc.com/queue/csec-620-ia3-hacker-culture-and-mitigation-al-qassam-cyber-fighters-and-pnc-bank-_59d5255c1723dd52a382c703_pdf?queue_id=5aaf4fbbd64ab2867215bf3a

[7] FBI, 5 other agencies probe possible covert Kremlin aid to Trump. http://www.mcclatchydc.com/news/politics-government/article127231799.html

[8] North Korean Hacker Group Seen Behind Crypto Attack in South. https://www.bloomberg.com/news/articles/2018-01-16/north-korean-hacker-group-seen-behind-crypto-attack-in-south

[9] Gordon L.A., Loeb M.P., Lucyshyn W., Zhou L. The impact of information sharing on cybersecurity underinvestment: a real options perspective // Journal of Accounting and Public Policy. 2015. 34(5). P. 509-519. DOI: 10.1016/j.jaccpubpol.2015.05.001

[10] Fielder A., Konig S., Panaousis E., Schauer S., Rass S. Uncertainty in Cyber Security Investments. arXiv preprint arXiv:1712.05893. 2017. https://arxiv.org/pdf/1712.05893.pdf

[11] Gordon L.A., Loeb M.P., Lucyshyn W., Zhou, L. Increasing cybersecurity investments in private sector firms // Journal of Cybersecurity. 2015. 1(1). P. 3-17. https://doi.org/10.1093/cybsec/tyv011

[12] Goztepe K. Designing Fuzzy Rule Based Expert System for Cyber Security // International Journal of Information Security Science. 2012. Vol. 1, N 1. P. 13-19. https://www.academia.edu/1513768/Designing_Fuzzy_Rule_Based_Expert_System_for_Cyber_Security

[13] Fielder A., Panaousis E., Malacaria P. et al. Decision support approaches for cyber security investment // Decision Support Systems. 2016. Vol. 86. P. 13-23. https://doi.org/10.1016/j.dss.2016.02.012

[14] Lakhno V.A. Development of a support system for managing the cyber security // Radio Electronics, Computer Science, Control. 2017. N 2. P. 109-116. https://doi.org/10.15588/1607-3274-2017-2-12

[15] Cavusoglu H., Mishra B., Raghunathan S. A model for evaluating IT security investments // Communications of the ACM. 2004. Vol. 47, N 7. P. 87-92. doi>10.1145/1005817.1005828

[16] Manshaei M. H., Zhu Q., Alpcan T. et al. Game theory meets network security and privacy // ACM Computing Surveys. 2013. Vol. 45, N 3. P. 1-39. DOI: 10.1145/2480741.2480742

[17] Fielder A., Panaousis E., Malacaria P. et al. Game theory meets information security management // IFIP International Information Security Conference, Marrakech, Morroco, 2–4 June 2014 : proceedings, Berlin, Springer, 2014, 15–29. DOI 10.1007/978-3-642-55415-5

[18] Smeraldi F., Malacaria P. How to spend it: optimal investment for cyber security // 1st International Workshop on Agents and Cyber Security. Paris, France, 06–08 May 2014: proceedings, New York, ACM, 2014, 8. doi>10.1145/2602945.2602952

[19] Gao X., Zhong W., Mei S. A game-theoretic analysis of information sharing and security investment for complementary firms // Journal of the Operational Research Society. 2014. Vol. 65, N 11. P. 1682-1691. https://doi.org/10.1057/jors.2013.133

[20] Malyukov V.P. Discrete-approximation method for solving a bilinear differential game // Cybernetics and Systems Analysis. 1993.Vol. 29, N 6. P. 879-888.

[21] 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, N 3. P. 35–41. DOI: 10.15587/1729-4061.2017.119259

[22] Isaacs, R. Differential games: a mathematical theory with applications to warfare and pursuit, control and optimization // Courier Corporation. 1999. https://books.google.es/books?hl=es&lr=&id=XIxmMyIQgm0C&oi=fnd&pg=PA1&dq=differential+games+Isaacs&ots=WhR34ML8_v&sig=hVOwUrKJ8YnHQo7Q7u3YeGLofQ0#v=onepage&q=differential%20games%20Isaacs&f=false

Б. Б. Ахметов[1], В. А. Лахно[2],
Б. С. Ахметов[3], В. П. Малюков[4]

[1]Есенов университеті, Ақтау, Қазақстан,
[2]Европалық университет, Киев, Украина,
[3]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан

КИБЕРҚАУІПСІЗДІКТІ ҚАРЖЫЛАНДЫРУ БОЙЫНША САПАНЫҢ БИСЫЗЫҚТЫ ОЙЫНЫ БАРЫСЫНДА ҚОРҒАУ СТРАТЕГИЯЛАРЫН ТАҢДАУ

Аннотация. Ақпараттандыру объект үшін киберқауіпсіздік құралдарын қаржыландыру бойынша интеллектуалды шешімдерді қолдау жүйесінің модулі үшін модель әзірленді. Модель киберқауіпсіздік және шабуылшылар тараптарының кезек-кезек қабылданатын көп сатылы ойындар теориясының құралдарын пайдалануына негізделген. Шабуыл жасайтын тараптың (хакерлердің) қаржылық жай-күйі туралы толық ақпарат болмаған жағдайда тиімді киберқауіпсіздік жүйесін құру үшін мүдделі тараптарға қаржылық стратегияларды бағалауға мүмкіндік беретін шешім қабылданды. Модель бірнеше терминал беттерімен сапалы бисызықты көпжүрісті ойындарды шешу арқылы қолданыстағы тәсілдерден ерекшеленеді.

Есептеу эксперименті орындалды және тиісті нәтижелер жұмыста көрсетілген., Имитациялау эксперименті барысында расталған, хакерлердің қаржылық жағдайы туралы ақпарат болмаған жағдайда, киберқауіпсіздік құралдарын қаржыландыру үдерісін сипаттайтын, параметрлердің кез-келген қатынасында киберқауіпсіздік стратегиясының қаржылық компоненттерінің шешімін есепке алуды қамтиды.

Түйін сөздер: ақпараттандыру объектілері, киберқауіпсіздік, сапалы көпжүрісті ойын, оңтайлы қаржыландыру стратегиясы, шешімдерді қолдау жүйесі.

Б. Б. Ахметов[1], В. А. Лахно[2], Б. С. Ахметов[3], В. П. Малюков[2]

[1]Университет Есенов, Актау, Казахстан,
[2]Кибербезопасность и управления защиты информационных систем,
Европейский университет, Киев, Украина,
[3]Казахский национальный педагогический университет имени Абая, Алматы, Казахстан

ВЫБОР СТРАТЕГИЙ ЗАЩИТЫ В ХОДЕ БИЛИНЕЙНОЙ ИГРЫ КАЧЕСТВА ПО ФИНАНСИРОВАНИЮ КИБЕРБЕЗОПАСНОСТИ

Аннотация. Статья содержит результаты сравнительного анализа предшествующих исследований в области кибербезопасности информационно-коммуникационных систем транспорта. Анализ выполнен в контексте решаемой проблемы дальнейшего развития методов и моделей распознавания киберугроз, аномалий и атак, направленных против информационно-коммуникационных систем транспорта, а также оценивания рисков для информационной безопасности транспортной отрасли как одной из составляющих критически важной инфраструктуры Республики Казахстан. Актуальность задачи также вызвана формированием единой информационно-коммуникационной среды транспортной отрасли Казахстана, внедрением новых и модернизацией существующих информационных систем на транспорте в условиях увеличения количества дестабилизирующих воздействий на доступность, конфиденциальность и целостность информации.

Ключевые слова: информационно-коммуникационные системы, информационная безопасность, критически важные компьютерные системы, система защиты информации, системы обнаружения кибератак.

Сведения об авторах:

Ахметов Берик Бахытжанович – кандидат технических наук, ректор Каспийского государственного университета технологий и инжиниринга имени Ш. Есенова, e-mail: berik.Akhmetov@kguti.kz,

Лахно Валерий Александрович – доктор технических наук, профессор, заведующий кафедрой кибербезопасности и управления защитой информационных систем, Европейский университет. e-mail: Valss21@ukr.net,

Ахметов Бахытжан Сражатдинович – доктор технических наук, профессор, директор Центра повышения квалификации и дистанционного образования, Казахский национальный педагогический университет имени Абая, e-mail: bakhytzhan.akhmetov.54@mail.ru,

Малюков Владимир Павлович – доктор технических наук, профессор кафедрой информационные системы и математические дисциплины, Европейский университет, e-mail: volod.malyukov@gmail.com

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)

http://www.bulletin-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Т. М. Апендиев, Д. С. Аленов*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 08.06.2018.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
20,4 п.л. Тираж 500. Заказ 3.