MODEL OF CYBERSECURITY MEANS FINANCING WITH THE PROCEDURE OF ADDITIONAL DATA OBTAINING BY THE PROTECTION SIDE

[1] LAKHNO V., [2] MALYUKOV V., [3]YEREKESHEVA M., [4]KYDYRALINA L., [3] SARSIMBAYEVA S., [1]ZHUMADILOVA M., [5]BURIACHOK V., [1]SABYRBAYEVA G.

[1] Yessenov Caspian state university of technologies and engineering, Aktau, Kazakhstan,
[2] National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine,
[3] K. Zhubanov Aktobe Regional State University, Kazakhstan,
[4] Kazakh National Pedagogical University named after Abay, Almaty, Kazakhstan,
[5]Borys Grinchenko Kyiv University, Kiev, Ukraine

E-mail: [1]lva964@gmail.com

ABSTRACT

The article describes the model of cybersecurity means financing strategies of the information object with incomplete information about the financial resources of the attacking side. The proposed model is the core of the module of the developed decision support system in the problems of choosing rational investing variants for information protection and cybersecurity of various information objects. The model allows to find financial solutions using the tools of the theory of multistep games with several terminal surfaces. The authors proposed an approach that allows information security management to make a preliminary assessment of strategies for financing the effective cybersecurity systems. The model is distinguished by the assumption that the protection side does not have complete information, both about the financing strategies of the attacking side, and about its financial resources state aimed at overcoming cybersecurity lines of the information object. At the same time, the protection side has the opportunity to obtain additional information by the part of its financial resources. This makes it possible for the protection side to obtain a positive result for itself in the case when it can not be received without this procedure. The solution was found using a mathematical apparatus of a nonlinear multistep quality game with several terminal surfaces with alternate moves. In order to verify the adequacy of the model there was implemented a multivariate computational experiment. The results of this experiment are described in the article.

Key words: *Cybersecurity, Information Protection, Informatization Object, Theory Of Games, The Choice Of Financing Strategy, Procedure Of Additional Data Obtaining, Decision Support System.*

1. INTRODUCTION

Nowadays almost any informatization object (IO) has its commercial secrets. Such IOs, as a rule, have their own information security system (ISS) and cybersecurity (CS). Modern ISS and CS are many echeloned complexes that include antivirus software, firewalls, attack and anomalies detection systems in the network, cryptographic applications, etc. The listed methods and means of information protection and cybersecurity can sufficiently reliably protect information resources of various IO from external threats. However, not always at the implementation of ISS and CS an important leakage channel for secret data, such as personnel data, is taken into account. In works [1, 2] there was shown that data protection from insiders is a permanent and universal problem that does not depend on the scale of the IO. Various kinds of data, obtained from insiders, can serve as a basis for choosing different strategies (including financing strategy) for the attacking side. At the same time, we believe that the actions of hackers (the attacking side) are also associated with the costs of financial resources for hacking [3]. As a source of additional data obtaining about the attacking side, you can use closed data for obtaining of which we need a financial resource of the protection side. For example, additional information about new hacking technologies, used by hackers, or the search for an insider within the framework of the IO.

In works [4, 5] there is shown that one of the main problems at the construction of complex ISS and CS is the choice of a rational financing strategy for such IO protection systems. The established in recent years trend for the intellectualization of decision-making support [6, 7] in the field of the IO cybersecurity problems allowed to take a fresh look at the yet unsolved problems for such systems. In particular, the actual is the problem of the development new models for the selection of rational strategies for ISS and CS financing, in particular for situations when new hacking technologies cause a change in the level of cyber risks for IO, and, therefore, lead to the need to revise financing strategies for the information and cybersecurity protection.

2. THE AIM OF THE ARTICLE

The aim of the article is the development of a model for a decision support system for the selection of rational strategies for cybersecurity systems financing of the informatization object, taking into account the procedure of additional data obtaining about the attacking side by the protection side and about the corresponding financial resource costs for cybersecurity systems.

3. LITERATURE REVIEW

In works [8–10] there were described in details the methodologies for creating various modules for the decision support systems in the field of ISS and CS financing for information systems of various purposes. A common disadvantage suggested by various authors of approaches is the absence of the considered variants for choosing financing strategies in the ISS and CS, in situations where the protection side does not have complete information about the financial resources (FR) of the attacking side. In fact, this is important information [11], because it allows eventually to understand the potential capabilities of hackers. The financial resource, even of the powerful hacker group, and the cyber warfare resource of the potential enemy side can be differ at times [3].

Our new research develops ideas that were previously described by the authors in [12, 13]. In the framework of the previously proposed scheme for selecting financing strategies in the ISS and CS of IO, based on the theory of games. In accordance with similar works, based also on the theory [14, 15], there are considered two sides: player №1 - information protector (IP); player №2 - a hacker. Both players use financial resources in order to achieve their goals [13, 16]. We should note that in the framework of the analysis of the available approaches we were not able to find detailed calculations that consider the situation when the IP has full information about the FR of the attackers. According to the [13, 14, 16-18] the difference from the game with complete information is that the IP does not know exactly the initial financial state of the second player (hacker).

Taking into account the above mentioned, it seems relevant to improve the model for choosing rational financing strategies of ISS and CS of IO with the introduction of the procedure of additional data obtaining by the protection side by the cost of part of own resources for its obtaining.

4. MODELS AND METHODS

In works [13, 17] there are considered situations when were found the sets of preference for the first player and his optimal strategies. This meant that if the states of the players belong to the set of preferences of the first player, then he has a strategy, the implementation of which will allow him to achieve his goal. Thus, with a given probability, the first player (information protector - IP) brings the system to a state that reflects a positive result for him. However, situations are possible where the protector is required to obtain a positive result for him from the states from which he can not do it under the standard setting of the game rules. For example, he is limited in time of interaction. Then it seems appropriate to introduce a procedure of additional data obtaining by the cost of part of own resources for its obtaining.

4.1. Problem Statement

Below there is formulated the problem statement of financing of the information protector and its cracker (hacker) with the introduction of the procedure of additional data obtaining by the cost of part of IP's resources for its obtaining.

There are two players (two sides). One player is IP (for example, the information system protector - ISP). The second player is the cracker of the information system (hacker). The first player seeks to protect his IS. The second one - to crack the system in order to disrupt its normal functioning.

Both players need financial resources to realize their goals. We assume that for a given period of time $\{0,1,..., T\}$ (T is a natural number) IP has $x(0)$ financial resources (FR). The second player, respectively – $y^{\xi}(0)$. These resources determine the predicted, at the time t=0, value of FR that players have to achieve their goals. There is an interaction of players. This interaction will be described as a bilinear multistep game with sequential steps with incomplete information. Unlike the game with full information, IP does not known exactly the initial state of the second player. However, the IP knows the distribution function of the initial states $F_0(\cdot)$ of the second player. This function is a uniform distribution on the segment $[a-r, a+r]\subseteq R_+$. Also, the first player knows the initial state and the parameters that determine the interaction and, in addition, at each moment of time t he knows all his own states $x(\tau)$ for $\tau \leq$ t. It is assumed that the first player (IP) can receive additional data by the cost of a part of his FR. It can be possible with the introduction of a parameter $k(k\in[0,1])$ that determines the part of the resource of the first player. This part of the FR is equal to $(1-k)\cdot z$ (here z is the value of the IP's resource), which goes to obtain information that the random states y^{ξ} of the second player (hacker) are evenly distributed on the segment $[c-k^2d, c+k^2d]$ (here $[c-d, c+d]$ – the segment on which the random states y^{ξ} are distributed). Conclusions are conducted from the position of the first player (IP), therefore there are no assumptions about the awareness of the second player (hacker). Steps are made in turn. At even moments, the first player makes a step, at uneven - the second player takes the step.

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

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

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

here

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

Let's describe the game process.

4.2. Description Of Multistep Quality Game With Several Terminal Surfaces With Alternate Steps

At the moment of time $t\in\{0,2,4,...,2n\}$ the first player (IP) multiplies the value $x(t)$ by the coefficient (rate of change) of growth α . Next, IP selects the values $u(t)$ $(u(t)\in[0,1])$, $k(t)$ $(k(t)\in[0,1])$ that determine the share of the resource of the first player $\alpha\cdot x(t)$ allocated to the IP on the cybersecurity and on the receiption of additional data at the moment of time t. Then the states of the players at the moment of time $t+1$ are determined from the relations (1). That is, the second player (hacker) is forced to spent for the cracking the cybersecurity of IP the value $s_1\cdot u(t)\cdot k(t)\cdot\alpha\cdot x(t)$. In this expression, it is assumed that s_1- the coefficient determining the "effectiveness" of financing of the second player for the development or for purchase of tools for hacking the cybersecurity of IP.

If the condition $P(y^{\xi}(t+1)<0)\geq p_0, (0\leq p_0\leq 1)$ is fulfilled, we will say that the first player (IP) guaranteed himself protection with probability p_0 and the procedure of cybersecurity means financing is over. Otherwise, the procedure of cybersecurity means financing of the first player will continue.

Then there is a step of a cracker (hacker). He acts just like the first player (IP) without using the procedure of additional data obtaining. And then the states of players are determined from the relations (2). If it turns out that after the attacker (hacker) step the condition $P(x(t+2)>0)<p_1, (0\leq p_1\leq 1)$ will be fulfilled, we will say that the attacker inflicted damage to the IP with a probability more than $(1-p_1)$. Then the procedure of cybersecurity means financing for this configuration of the security barriers is over.

The first player seeks to find a lot of his initial states (InS), which have the following property. Property: if the game starts from the InS, then the first player can protect his IS by the selection his control actions $u(0), k(0),..., u(t), k(t)$ $(t=2n)$ with a probability more than p_0. In this case, IP is able to prevent damage from the hacker 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 introduce the following notation: Φ - the set of distribution functions of one-dimensional random values; 2n - the natural even number close to T; $T^* = \{0,2,\ldots,2n\}$ – the set of natural even numbers.

Definition. The pure strategy $[u(.,.,.),k(.,.,.)]$ of the first player (IP) is the set of functions $[u(.,.,.),k(.,.,.)]: T^* \times R_+ \times \Phi \to [0,1]$, such, as $u(t,x,F) \in [0,1], k(t,x,F) \in [0,1], (F \in \Phi)$.

Therefore, the strategy of the first player (IP) is a rule that allows him, based on available information, to determine the amount of FR, directed to the development of cybersecurity systems, and also to obtain additional data about the second player (hacker).

The second player chooses his strategy $v(.)$ based on any information. The aim of the first player is to find his set of preferences. IP's strategies are also defined, by applying of which he will receive the fulfillment of conditions that allow to complete the procedure of cybersecurity financing. 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 problem under risk conditions. In addition, such a model is a non-linear multistep quality game with several terminal surfaces with alternate steps. Finding sets of the first player's preferences (IP) and his optimal strategies depends on a variety of parameters.

4.3. Determining The Rational Financial Strategies Of The Player - Information Protector

The IP's set of preferences, taking into account the procedure of additional data obtaining, are differ from the sets of the first player's preferences without this procedure by the following circumstance. Due to the fact that the first player, receiving additional data during his step (and spending part of his FR), can ensure to himself the achievement of a positive result from the states in which he could not do this at the absence of this procedure. A large number of parameters, different cases in the considered problem are "forced" within the framework of the article to confine with the considering the procedure for obtaining additional information during the the steps of the first player. Consideration of cases of implementation of the procedure of additional data obtaining during the next steps is completely analogous. There should be noted that the consideration of the procedure of data obtaining at the first step affects the entire process of interaction at all steps.

Further we will consider that $p_1 = p_0$.

The set of preferences of the first player at the step T for the case using the additional data procedure will be denoted by $V^T_{1,k(1)}(p_0, p_0)$.

1. $T = 1$.

1.1. At $p_0 : 0 \le p_0 \le 0{,}5$ will be $V^1_{1,k(1)}(p_0, p_0) = \varnothing$.

1.2. At $p_0 : 0{,}5 < p_0 < 1$ will be:

1.2.1. If $a < 2 \cdot p_0 \cdot r - r$, то

$$V^1_{1,k(1)}(p_0, p_0) = \left\{ \begin{matrix} x(0) : 2\sqrt{a(2 \cdot p_0 \cdot r - r)} \le \\ \le s_1 \cdot \alpha \cdot x(0) < a + 2 \cdot p_0 \cdot r - r \end{matrix} \right\},$$

The optimal IP's strategy will be a couple of functions $[u(.,.,.),k(.,.,.)]$:

$$(\bar{k}(1))_2 < k^*(x(0), F(.)) < (k(1))_1,$$

$$(\bar{k}(1))_{1,2} = \frac{\phi \pm \sqrt{(\phi)^2 - 4 \cdot a(2 \cdot p_0 \cdot r - r)}}{2 \cdot (2 \cdot p_0 \cdot r - r)}; \tag{3}$$

where $\phi = s_1 \cdot \alpha \cdot x(0)$,

$u^*(x(0), F(.)) = 1$;

at

$$x(0) : 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} \le \phi. \tag{4}$$

$u^*(x(0), F(.)) = 0$; ;

at

$$x(0) : \phi < 2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}. \tag{5}$$

1.2.2. At $a \ge 2 \cdot p_0 \cdot r - r$ will be $V^1_{1,k(1)}(p_0, p_0) = \varnothing$.

2. $T = 2 \cdot k + 1 \ge 3$.

2.1. At $\alpha \le \beta$ the first player's set of preferences (IP) can not be constructed.

2.2. $a < 2 \cdot p_0 \cdot r - r$;

Let define the natural k_0 from the condition:

$$k_0 \geq 1, s_1 \cdot \alpha \cdot s_2 < \left(\frac{\beta}{\alpha}\right)^{k_0 - 1}, \quad \text{at} \quad \alpha > \beta.$$

$$s_1 \cdot \alpha \cdot s_2 \geq \left(\frac{\beta}{\alpha}\right)^{k_0},$$

The first player's set of preferences, taking into account the additional data procedure, will be written as follows for $T = 2 \cdot k + 1 \leq 2 \cdot k_0 + 1$, at $\bar{k} \leq k \leq k_0$, where $\bar{k} : \bar{k} \geq 1$, and

2.2.1.

$$(s_1 \cdot \alpha \cdot s_2) \cdot \left(\frac{\alpha}{\beta}\right)^{\bar{k}-2} < \frac{2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}}{a + 2 \cdot p_0 \cdot r - r};$$

$$(s_1 \cdot \alpha \cdot s_2) \cdot \left(\frac{\alpha}{\beta}\right)^{\bar{k}-1} \geq \frac{2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}}{a + 2 \cdot p_0 \cdot r - r};$$

$$s_1 \cdot \beta \cdot s_2 < \frac{2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}}{a + 2 \cdot p_0 \cdot r - r};$$

$$V_{1,k(1)}^{1}(p_0, p_0) = \left\{ \begin{array}{l} x(0) : 2\sqrt{\alpha(2 \cdot p_0 \cdot r - r)} \leq \\ \leq s_1 \cdot \alpha \cdot x(0) < a + \\ + 2 \cdot p_0 \cdot r - r \end{array} \right\}, \qquad (6)$$

$$V_{1,k(1)}^{2k+1}(p_0, p_0) = \varnothing, \quad \text{for} \quad 1 \leq k < \bar{k};$$
(7)

$$V_{1,k(1)}^{2\bar{k}+1}(p_0, p_0) = \left\{ \begin{array}{l} x(0) : 2 \cdot \left(\frac{\beta}{\alpha}\right)^{\bar{k}} \sqrt{a(2 \cdot p_0 \cdot r - r)} \leq \\ \leq s_1 \cdot \alpha \cdot x(0) < s_1 \cdot \beta \cdot s_2 \cdot \\ \cdot (a + 2 \cdot p_0 \cdot r - r) \end{array} \right\}, \qquad (8)$$

$$V_{1,k(1)}^{2k+1}(p_0, p_0) = \left\{ \begin{array}{l} x(0) : 2 \cdot \left(\frac{\beta}{\alpha}\right)^{k} \sqrt{a(2 \cdot p_0 \cdot r - r)} \leq \\ \leq \phi < 2 \cdot \left(\frac{\beta}{\alpha}\right)^{k-1} \cdot \sqrt{a(2 \cdot p_0 \cdot r - r)} \end{array} \right\}, \qquad (9)$$

For $\bar{k} \leq k \leq k_0$.

The optimal strategy of the first player will be a couple of functions $[u^*(.,.,.), k^*(.,.,.)]$:

$$(\bar{k}(1))_2 < k^*(x(0), F_0(.)) < \min(1, (\bar{k}(1))_1),$$

$$(\bar{k}(1))_{1,2} = \frac{s_1 \cdot \alpha \cdot x(0) \cdot \left(\frac{\alpha}{\beta}\right)^k \pm \sqrt{(\phi) \cdot \left(\left(\frac{\alpha}{\beta}\right)^k\right)^2 - 4 \cdot a(2 \cdot p_0 \cdot r - r)}}{2 \cdot (2 \cdot p_0 \cdot r - r)}; \qquad (10)$$

at

$$2 \cdot \left(\frac{\beta}{\alpha}\right)^k \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} \leq s_1 \cdot \alpha \cdot x(0);$$

$$k^*(x(0), F_0(.)) = 1$$

at

$$2 \cdot \left(\frac{\beta}{\alpha}\right)^k \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} > s_1 \cdot \alpha \cdot x(0);$$
(11)

$$u^*(x(0), F_0(.)) = 1$$

at

$$x(0) : 2 \cdot \left(\frac{\beta}{\alpha}\right)^k \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} \leq \phi; \qquad (12)$$

$$u^*(x(0), F_0(.)) = 0$$

at

$$x(0) : 2 \cdot \left(\frac{\beta}{\alpha}\right)^k \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)} > \phi. \qquad (13)$$

The first player's set of preferences, taking into account the additional data procedure, will be written as follows for $T = 2 \cdot k + 1 \leq 2 \cdot k_0 + 1$,

at

2.2.2.

$$k_0 \geq 1, s_1 \cdot \alpha \cdot s_2 < \left(\frac{\beta}{\alpha}\right)^{k_0 - 1}, \quad s_1 \cdot \alpha \cdot s_2 \geq \left(\frac{\beta}{\alpha}\right)^{k_0},$$

at $\alpha > \beta$,

$$s_1 \cdot \beta \cdot s_2 \geq \frac{2 \cdot \sqrt{a \cdot (2 \cdot p_0 \cdot r - r)}}{a + 2 \cdot p_0 \cdot r - r};$$

$$V_{1,k(1)}^{2\bar{k}+1}(p_0,p_0)=\left\{\begin{array}{l} x(0):2\cdot\left(\frac{\beta}{\alpha}\right)^{k}\sqrt{a(2\cdot p_0\cdot r-r)}\le \\ \le s_1\cdot\alpha\cdot x(0)<2\cdot\left(\frac{\beta}{\alpha}\right)^{k-1}\cdot \\ \cdot\sqrt{a(2\cdot p_0\cdot r-r)} \end{array}\right\}, \tag{14}$$

$(k=1,\dots,k_0)$.

The optimal strategy of the first player will be a couple of functions $\left[u^{*}(.,.,.),k^{*}(.,.,.)\right]$:

$$\left(\bar{k}(1)\right)_2<k^{*}(x(0),F_0(.))<\min\left(1,\left(\bar{k}(1)\right)_1\right),$$

$$\left(\bar{k}(1)\right)_{1,2}=\frac{s_1\cdot\alpha\cdot x(0)\cdot\left(\frac{\alpha}{\beta}\right)^{k}\pm\sqrt{(s_1\cdot\alpha\cdot x(0))\cdot\left(\left(\frac{\alpha}{\beta}\right)^{k}\right)^{2}-4\cdot a(2\cdot p_0\cdot r-r)}}{2(2\cdot p_0\cdot r-r)}; \tag{15}$$

Two cases $2\cdot\left(\frac{\beta}{\alpha}\right)^{k}\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}\le\phi$ we have:

$$k^{*}(x(0),F_0(.))=1$$

at

$$2\cdot\left(\frac{\beta}{\alpha}\right)^{k}\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}>\phi; \tag{16}$$

$$u^{*}(x(0),F_0(.))=1$$

at

$$x(0):2\cdot\left(\frac{\beta}{\alpha}\right)^{k}\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}\le\phi; \tag{17}$$

$$u^{*}(x(0),F_0(.))=0$$

at

$$x(0):2\cdot\left(\frac{\beta}{\alpha}\right)^{k}\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}>\phi. \tag{18}$$

The set of preferences for $T=2\cdot k_0+3$, in case:

$$(s_1\cdot\alpha\cdot s_2)\cdot\left(\frac{\alpha}{\beta}\right)^{k_0-1}< \\ <\frac{2\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}}{a+2\cdot p_0\cdot r-r},$$

will be written as:

$$V_{1,k(1)}^{2k_0+3}(p_0,p_0)=\left\{\begin{array}{l} x(0):2\cdot s_1\cdot\beta\cdot s_2\cdot \\ \cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}\le\phi< \\ <s_1\cdot\beta\cdot s_{2.}(a+2\cdot p_0\cdot r-r) \end{array}\right\}. \tag{19}$$

The optimal strategy of the first player will be a couple of functions $\left[u^{*}(.,.,.),k^{*}(.,.,.)\right]$:

$$\left(\bar{k}(1)\right)_2<k^{*}(x(0),F_0(.))<\min\left(1,\left(\bar{k}(1)\right)_1\right),$$

$$\left(\bar{k}(1)\right)_{1,2}=\frac{\phi\cdot\left(\frac{1}{s_1\cdot\beta\cdot s_2}\right)\pm\sqrt{(\phi)\cdot\left(\frac{1}{s_1\cdot\beta\cdot s_2}\right)^{2}-4\cdot a(2\cdot p_0\cdot r-r)}}{2\cdot(2\cdot p_0\cdot r-r)}; \tag{20}$$

At $2\cdot(s_1\cdot\beta\cdot s_2)\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}\le\phi$ we have:

$$u^{*}(x(0),F_0(.))=1$$

at

$$x(0):\phi\ge 2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}; \tag{21}$$

$$k^{*}(x(0),F_0(.))=0$$

at $2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}>\phi$. (22)

In case:

$$(s_1\cdot\alpha\cdot s_2)\cdot\left(\frac{\alpha}{\beta}\right)^{k_0-1}\ge\frac{2\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}}{a+2\cdot p_0\cdot r-r};$$

$$V_{1,k(1)}^{2k_0+3}(p_0,p_0)=\left\{\begin{array}{l} x(0):2\cdot s_1\cdot\beta\cdot s_2\cdot \\ \cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)}\le\phi< \\ <2\cdot\left(\frac{\beta}{\alpha}\right)^{k_0}\cdot\sqrt{a\cdot(2\cdot p_0\cdot r-r)} \end{array}\right\}. \tag{23}$$

The optimal strategy of the first player will be a couple of functions $\left[u^{*}(.,.,.),k^{*}(.,.,.)\right]$:

$$\left(\bar{k}(1)\right)_2 < k^{*}\left(x(0),F_0(.)\right) < \min\left(1,\left(\bar{k}(1)\right)_1\right),$$

$$\left(\bar{k}(1)\right)_{1,2} = \frac{\phi\cdot\left(\frac{1}{s_1\cdot\beta\cdot s_2}\right)\pm\sqrt{(\phi)\cdot\left(\frac{1}{s_1\cdot\beta\cdot s_2}\right)^2 - -\left(4\cdot a\left(2\cdot p_0\cdot r-r\right)\right)}}{2\cdot\left(2\cdot p_0\cdot r-r\right)}; \qquad (24)$$

at
$2\cdot\left(s_1\cdot\beta\cdot s_2\right)\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}\leq\phi$

we will receive:

$$k^{*}\left(x(0),F_0(.)\right)=1$$

at

$$2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}>\phi; \qquad (25)$$

$$u^{*}\left(x(0),F_0(.)\right)=1$$

at

$$x(0):\phi\geq 2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}; \qquad (26)$$

$$u^{*}\left(x(0),F_0(.)\right)=0$$

at

$$x(0):\phi< 2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}. \qquad (27)$$

At $T=2\cdot k+1>2\cdot k_0+3$ the set of preferences of the first player can not be constructed, i.e.

$$V_{1,k(1)}^{2k+1}\left(p_0,p_0\right)=\varnothing \text{ at } k>k_0+1.$$

Let note that the inequality

$$\phi=s_1\cdot\alpha\cdot x(0)\geq$$
$$\geq 2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}$$

determines the area in which the first player (IP) can get a positive result for himself at the moment of time $t=2\cdot k+1\leq 2\cdot k_0+3$. it means that the value $g=\frac{s_2\cdot\beta}{\alpha\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}}$ is analogous to the barrier [18]. If we consider the relation $\phi=2\cdot s_1\cdot\beta\cdot s_2\cdot\sqrt{a\cdot\left(2\cdot p_0\cdot r-r\right)}$ in surface $\left(x(0),a\right)$, where a – the mathematical expectation of a random variable $y^{\xi}(0)$, then it determines the line of stochastic balance in the problem, taking into account the procedure of additional data obtaining.

2.3. $a\geq 2\cdot p_0\cdot r-r;$

The set of preferences of the first player $V_{1,k(1)}^{2k+1}\left(p_0,p_0\right)=\varnothing$ at any $k=0,1,...$

5. COMPUTATIONAL EXPERIMENT

In order to test the efficiency and adequacy of the proposed model there were performed simulation experiments. The objectives of the simulation were: 1) the definition of a set of strategies of the players (IP) and the attacking side; 2) an assessment of the adequacy of the mathematical model.

The results of three computational experiments are shown on Fig. 1–3.

Solutions are obtained for all cases of the relation of the parameters of the game considered in the work. Using the results of the game there were found the optimal variants of the financial strategies of the protector of the informatization object.

The maximum deviation of the results of the computational simulation experiment from practical data was 9–12%.

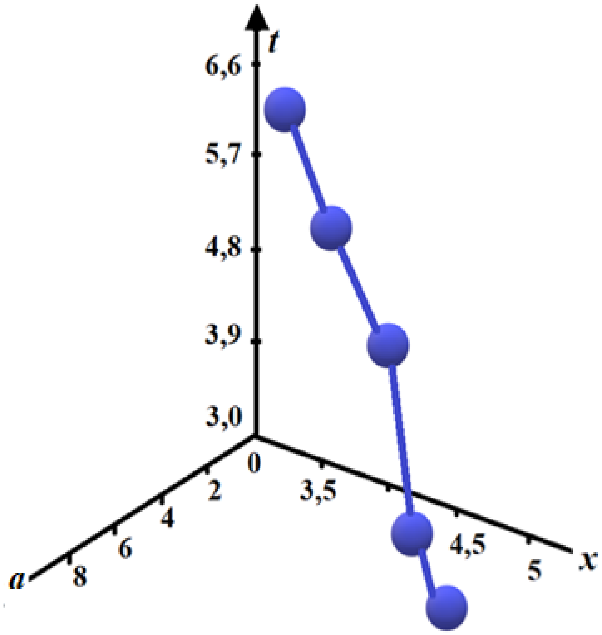


Figure 1 : The results the computational experiment №1

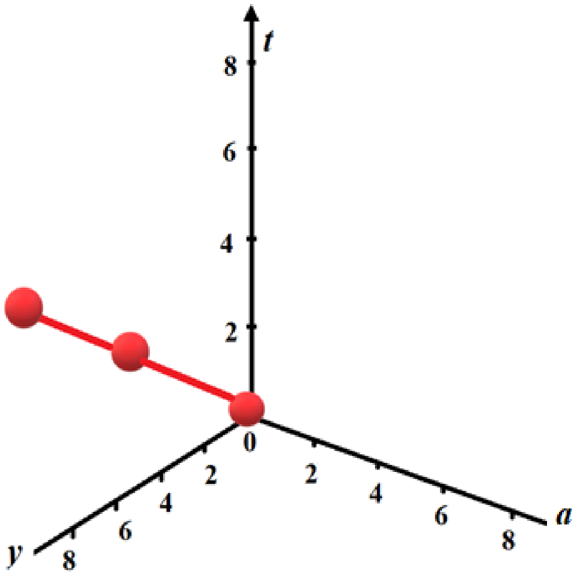


Figure 2 : The Results The Computational Experiment № 2

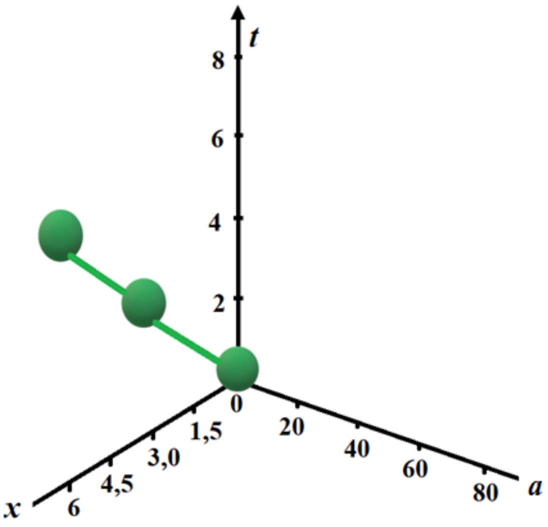
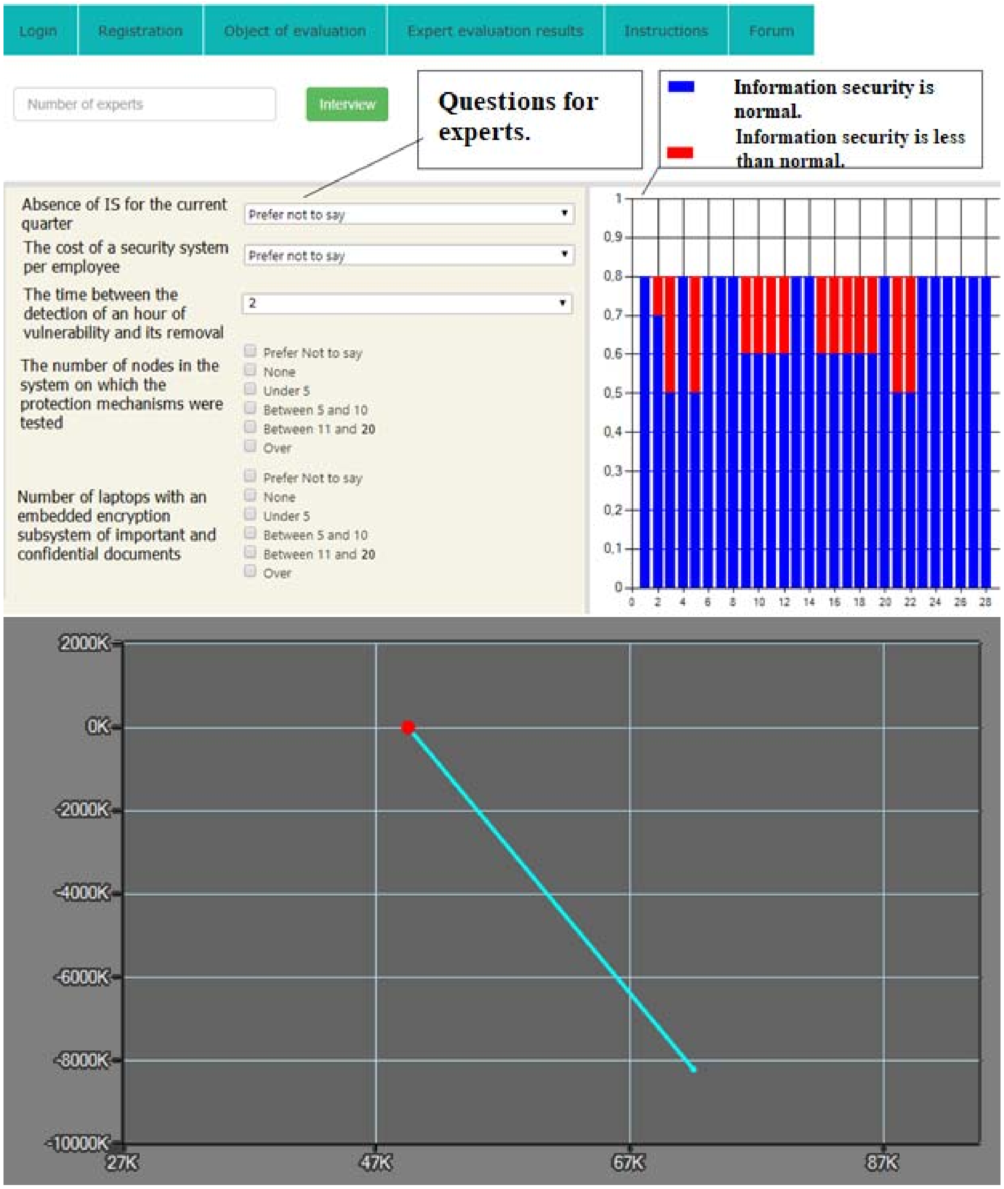


Figure 3 : The results the computational experiment № 3

The developed model was implemented as a software product Decision Support System (DSS) - “The choice of a rational financial strategy for ensuring cybersecurity of an informatization object (IDSS)”. A general view of the results of the work of the DSS is shown on Figures 4.

During the testing of the DSS there were considered situations when two players (the protector - Player 1 and the hacker - Player 2) control the dynamic system. The purpose of the experiment was to determine the set of strategies of the players. There were considered cases when the players' strategies put them to the corresponding terminal surfaces. During the experiment, there were found the sets of initial states of objects and their strategies that allow objects to lead the system to that or to another terminal surface. On the plane, the x-axis is the financial resources of the 1st player (protector). Y-axis - financial resources of the 2nd player (hacker or attacking side as a whole).



Questions for experts.

🟦 Information security is normal.
🟥 Information security is less than normal.

Absence of IS for the current quarter: Prefer not to say ▾

The cost of a security system per employee: Prefer not to say ▾

The time between the detection of an hour of vulnerability and its removal: 2 ▾

The number of nodes in the system on which the protection mechanisms were tested:
□ Prefer Not to say
□ None
□ Under 5
□ Between 5 and 10
□ Between 11 and 20
□ Over

Number of laptops with an embedded encryption subsystem of important and confidential documents:
□ Prefer Not to say
□ None
□ Under 5
□ Between 5 and 10
□ Between 11 and 20
□ Over

Figure 4 : Graph displaying in DSS based on game results

Caption*: Solution* – there was obtained a solution in which the allocated financial resources for cybersecurity and information protection for an informatization object are not sufficient if the time of interaction between the sides is limited. In order to solve the problem with a greater probability, there should be increased the amount of financial resources allocated by the decision-maker for information protection measures. It is accepted that the financial resources of the attacking side are not limited.

The obtained results demonstrate the effectiveness of the approach proposed in the article. During testing of the model and software product, the correctness of the obtained results was established.

6. DISCUSSION OF SIMULATION RESULTS

There is taken a three-dimensional positive orthant in a three-dimensional space – $(t, x(0), a)$. The time axis t "goes from bottom to top, from zero". It is assumed that the parameter t will designate the amount of steps of the players.

In this three-dimensional orthant we consider the set of surfaces issuing from the point (0,0,0).

Surfaces are perpendicular to the plane $(0,x(0),a)$. These surfaces are defined by the relation: $a=\left(3-\frac{1}{n}\right)\cdot(x(0))^2$ for any positive *n*. The surfaces allow to define the set of preferences of the first player for *n* (*n* – uneven natural number) steps with probability p_0 using the additional information procedure, i.e. it is believed that $p_0 = p_1$. For example, a set $V^n_{1,k(1)}(p_0,p_0)$.

Then $V^n_{1,k(1)}(p_0,p_0)$ is a set

$$\left\{\begin{array}{l}(n,x(0),a)\in R_+^2,(3-1/(n-1))(x(0))^2\le\\ \le a<(3-1/(n-1))(x(0))^2,\\ t=n\end{array}\right\}.$$

Then at $n = 1$ will be

$$V^1_{1,k(1)}(p_0,p_0)=\left\{\begin{array}{l}(1,x(0),a):(x(0),a)\in R_+^2,0\le\\ \le a<2\cdot(x(0))^2,t=1\end{array}\right\}.$$

The line: $a=3\cdot(x(0))^2$ in the surface $(x(0),a)$ will be a line of stochastic balance.

Test calculations № 1 (Fig. 1). There is received: (0, x(0), a(0))) = (0, 3, 6.5), (1, x(1), a(1)) = (1, 3.5, 5.5), (3, x(3), a(3)) = (3, 4.0, 5.0), (5, x(5), a(5)) = (5, 4.5, 4.0), (7, x(7), a(7)) = (7, 5.0, 3.0). There should be noted that points are considered in three-dimensional space $(t,x(0),a)$. Trajectory of motion is shown by a red curve.

Test calculations 2 (Fig. 2). The set of preferences of the second player (attacking side, i.e. there is consider a symmetric task for the second player) will look like this. There is taken a three-dimensional positive orthant in a three-dimensional space $(t,x(0),a)$. In this orthant we consider the set of surfaces issuing from the point (0,0,0) perpendicular to the plane $(t,a,y(0))$.

These surfaces are given by the relation: $a=\left(0{,}9+\frac{1}{n}\right)\cdot(y(0))^2$ for any positive *n*. These surfaces allow to define the set of the preferences of the second player for *n* (*n* – uneven natural number) steps with probability p_0, i.e. it is believed that $p_0 = p_1$.

For example, the set $V^n_{2,k(1)}(p_0,p_0)$ – is the set

$$\left\{\begin{array}{l}(n,a,y(0))\in R_+^2,\left(0{,}9+\frac{1}{n}\right)(y(0))^2\le\\ \le a<(0{,}9+1/(n-1))(y(0))^2,t=n\end{array}\right\}.$$

Then at $n = 1$ will be

$$V^1_{2,k(1)}(p_0,p_0)=\left\{\begin{array}{l}(1,a,y(0))\in R_+^2,a\le\\ \le 1.9\cdot(y(0))^2,t=1\end{array}\right\}.$$

The line: $a=(0{,}9)\cdot(y(0))^2$ in the surface $(a,y(0))$ will be a line of stochastic balance.

There is received: (0, a(0), y(0)) = (0, 5.0, 3.0), (1, a(1), y(1))=(1, 4.0, 4.0), (3, a(3), y(3))=(3, 3.0, 5.0), (5, a(5), y(5))=(5, 2.0, 6.0), (7, a(7), y(7))= (7, 1, 8.0). The points are considered in three-dimensional space $(t,a,y(0))$. Trajectory of motion is shown by a blue curve.

Test calculations № 3 (Fig. 3). Corresponds to the "movement" along the line of balance: $a=3\cdot(x(0))^2$.

Here the original task for the first player is considered. The following values are obtained: (0, x(0), a(0)) = (0, 5, 75.0), (1, x(1), a(1))=(1, 4, 48.0), (3, x(3), a(3))=(3, 3, 27.0), (5, x(5), a(5)) = (5, 2, 12.0), (7, x(7), c(7)) = (7, 1, 3.0). The points are considered in three-dimensional space $(t,x(0),a)$. Trajectory of motion is shown by a green curve.

Therefore, the adequacy of the refined model was confirmed by computational experiments. Also there was confirmed the ability of the model to provide effective support for decision-making in the field of cybersecurity means financing of various IOs. The work continued a number of publications by the authors [8, 12, 13], in which there were presented the theoretical and methodological foundations of DSS creation. This work develops these researches within the framework of complementing of the existing DSS [13, 15] with mathematical models that are based on a bilinear multistep quality game with several terminal surfaces [15, 18]. The refinements in the model eliminate the disadvantages of the solutions presented in [8, 13, 19, 20]. Since in [8, 13, 21–34] there were not taken into account all the initial conditions for choosing financial strategies for investing in cybersecurity of IO.

The prospect of further research is the possibility of applying the results obtained for the subsequent algorithmization of the processes associated with the analysis cybersecurity of IO. In this context, our work continues previous publications of the authors [35–46].

7. GRATITUDES

The research and the article were carried out within the framework of promising scientific and technical programs of the Department of Computer Systems and Networks of National University of Bioresources and Natural Resources Use of Ukraine as well as a grant of the Republic of Kazakhstan registration number AP05132723 "Development of adaptive expert systems in the field of cybersecurity of very important information objects".

8. CONCLUSIONS

Among scientists, quite a lot of authors were involved in the description of dynamic controlled objects using differential equations [5-10]. They propose certain methods of game theory that allow solving real practical problems. In [27, 28], there were developed methods for finding optimal strategies for players in such an interaction. Our research has overcome these limitations. In the works it was proposed to consider discrete analogues of differential equations, but without making a final transition from differential equations to discrete systems. This circumstance has led to the fact that the opposition class of the opposing player must be at least functions, have dimensions. Therefore, the project idea is to develop an intelligent decision support system at investing in various cyber security projects of various information systems. Models, algorithms, and the DSS itself, which is being developed as a part of a study based on bilinear differential equations with dependent movements, allows constructively finding optimal strategies and giving concrete recommendations to investors in cybersecurity projects or other large investment projects, for example, in the field of Smart City.

The working hypothesis of the study is following. It is assumed that if we develop an intelligent decision support system at investing in high-tech and at the same time risky projects for the development of cybersecurity systems, then due to the fact that the basic DSS models are based on bilinear differential equations with dependent movements, it will be possible to increase the efficiency of choosing rational strategies for attracting financial resources for the task of investing in cybersecurity of various informatization objects.

There is proposed a refined model of cybersecurity system financing for various information objects. The proposed variant of the refined model differs from the assumption that the protection side does not have complete information, both about the financial strategies of the attacking party, and about the states of its financial resources aimed at overcoming the protection boundaries of the object of cyberattacks. At the same time, the protection side has the opportunity to obtain additional data by the cost of a part of his financial resources. The last makes it possible for the protection side to receive a positive result for himself in case when he can not receive it without this procedure.

The solution is based on the method of dynamic programming. This allows, in contrast to existing approaches, to find more effectively solutions. In order to find the solution we also used the mathematical apparatus of a nonlinear multistep quality game with several terminal surfaces with alternate moves.

The article considers the variants of situations in which the information content requires the resources of players from the protection of the informatization object.

The results of the simulation experiment are also shown in the article. There are considered the variants of the optimal behavior of the cybersecurity side of the informatization object. Simulation experiments confirmed the adequacy of the model. The deviation of the results of the simulation experiment from practical data does not exceed 9–12%.

REFERENCES:

[1] T. Sawik. “Selection of optimal countermeasure portfo lio in it security planning”, *Decision Support Systems,* Vol. 55, Iss. 1, 2013, pp. 156–164.

[2] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi. “Decision support approaches for cyber security investment”, *Decision Support Systems,* Vol. 86, 2016, pp. 13–23.

[3] L. Atymtayeva, K. Kozhakhmet, G. Bortsova. “Building a Knowledge Base for Expert System in Information Security, *Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing,* Vol. 270, 2014, pp. 57–76.

[4] M. M. Gamal, B. Hasan, A. F. Hegazy. “A Security Analysis Framework Powered by an Expert System”, *International Journal of Computer Science and Security (IJCSS) 2011,* vol. 4, no. 6, pp. 505–527.

[5] Chang Li-Yun, Lee Zne-Jung. "Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system", *International Conference on Fuzzy Theory and Its Applications (iFUZZY) 2013*, pp. 346 – 351.

[6] M. Kanatov, L. Atymtayeva, B. Yagaliyeva. "Expert systems for information security management and audit, Implementation phase issues", *Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS) 2014*, pp. 896 – 900.

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

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

[9] P. Louvieris, N. Clewley, X. Liu. "Effects-based feature identification for network intrusion detection", *Neurocomputing 2013*, Vol. 121, Iss. 9, pp. 265–273.

[10] M. Carlton & Y. Levy. "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals", *In SoutheastCon 2015,* pp. 1–6. IEEE.

[11] R. K. Abercrombie, F.T. Sheldon, A. Mili. Managing complex IT security processes with value based measures, *Computational Intelligence in Cyber Security 2009.*

[12] A.T. Sherman, L. Oliva, D. DeLatte, E. Golaszewski, M. Neary, K. Patsourakos, D. Phatak, T. Scheponik, G. L. Herman, J. Thompson. Creating a Cybersecurity Concept Inventory: A Status Report on the CATS Project, Appears in the proceedings of the 2017 National Cyber Summit, Huntsville, AL.

[13] Y. Nugraha, I. Brown, A. S. Sastrosubroto. "An Adaptive Wi deband Delphi Method to Study State CyberDefence Requirements", *IEEE Transactions on Emerging Topics in Computing 2016*, Vol. 4, Iss. 1, pp. 47 – 59.

[14] J Bedford, L. Van Der Laan. "Organizational Vulnera bility to Insider Threat", *In: C. Stephanidis. (eds) HCI International 2016 – Posters' Extended Abstracts. HCI 2016. Communications in Computer and Information Science 2016*, vol. 617. Springer, pp. 465–470.

[16] A.M. Johnson. "Business and security executives views of information security investment drivers: Results from a delphi study", *Journal of Information Privacy and Security 2009*, 5(1), pp. 3–27.

[17] D. Pruitt-Mentle. "A Delphi Study of Research Priorties in Cyberawareness", *Educational Technology Policy, Research and Outreach–CyberWatch, 2011.*

[18] M. Chaturvedi, A. N. Singh, M. P. Gupta, J. Bhattacharya. "Analyses of issues of information security in Indian context", *Transforming Government: People, Process and Policy 2014*, Vol. 8 Iss. 3, pp.374–397.

[19] V. Lakhno, Y. Boiko, A. Mishchenko, V. Kozlovskii & O Pupchenko. "Development of the intelligent decision-making support system to manage cyber protection at the object of informatization", *Eastern-European Journal of Enterprise Technologies 2017*, 2 (9(86)), pp. 53–61.

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

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

[22] Akhmetov, Bakhytzhan, etc. "The choice of protection strategies during the bilinear quality game on cyber security financing", *Bulletin of the national academy of sciences of the republic of Kazakhstan*, (3), 2018, pp. 6–14.

[23] Beketova, G., Akhmetov, G. B., Korchenko, etc. "Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition", *Computer modelling and new technologies*, 21(2), 2017, pp. 7–16.

[24] Akhmetov, Berik, etc. "Model of cyber security financing within the framework of the bilinear differential quality game scheme", *Radio Electronics, Computer Science, Control*, (3). 2018, pp. 17–26.

[25] Beketova, G. S., Akhmetov, Bakhytzhan S., Korchenko, A. G., etc. "Optimization backup model for critical important information systems", *Bulletin of the National Academy of Sciences of the Republic of Kazakhstan*, (5), 2017, pp. 37–44.

[26] Beketova, G., Akhmetov, Bakhytzhan, Korchenko, A., & etc. "Simulation modeling of

cyber security systems in matlab and Simulink”, *Bulletin of the National Academy of Sciences of the Republic of Kazakhstan,* (3), 2017, pp. 54–64.

[27] Berik Akhmetov, etc. "Automation of decision making support on the distribution of financial resources on the elimination of accidents on railway transport”, *International Journal of Civil Engineering and Technology (IJCIET),* Volume 10, Issue 3, 2019, pp. 2716–2724.

[28] Bakhytzhan Akhmetov, Lazat Kydyralina, etc. “Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions”, *International Journal of Mechanical Engineering and Technology (IJMET)*, Volume 9, Issue 10, 2018, pp. 1114–1122.

[29] A.G. Korchenko, B.S. Akhmetov, S.V. Kazmirchuk, M.N. Zhekambaeva "Method of n-fold incrementation the number of terms the linguistic variables in the tasks of analysis and risk assessment", *Bezpeka Informácie*, 21(2), 2015. pp. 191–200.

[30] Korchenko, A., Akhmetov, B., Kazmirchuk, S., & Chasnovskiy, Ye. “Sistema otsenivaniya riskov informatsionnoy bezopasnosti–RISK-KALKULYATOR”, Bezpeka informatsiï, 23(2), 2017, pp. 145–152.

[31] Akhmetov, B. S., & Kydyralina, L. M. “Modyel na osnovye syeti pyetri dlya razgranichyeniya polnomochiy polzovatyelyey v syeti informatsionno-obrazovatyelnoy sryedy univyersityeta”, *In Problemy informatiki v obrazovanii, upravlenii, ekonomike i tekhnike, 2018,* pp. 81–84.

[32] Akhmetov, B. S., Korchenko, A. G., Kazmirchuk, S. V., & Zhekambayeva, M. N. “Methods of estimation of risks for control systems of information security”, *Bulletin of the national academy of sciences of the republic of Kazakhstan*, (6), 2015, pp. 23–38.

[33] Shaikhanova, A., Shangytbayeva, G., Ahmetov, B., & Beisembekova, R. “Comparison of Methods of Treatment of Fuzzy Information for Distribution of Access in Computer Systems”, *Research Journal of Applied Sciences, Engineering and Technology*, 10(9), 2015, pp. 1082–1088.

[34] Akhmetov, B. S., Ivanov, A. I., Malygina, E. A., & Nadeev, D. N. “Modifications of bernoulli trials for a statistical description of networks of artificial neural with multilevel quantizers”, *Bulletin of the national academy of sciences of the republic of Kazakhstan*, (6), 2014, pp. 7–15.

[35] V. Lakhno, V. Malyukov, V. Domrachev, O. Stepanenko & O. Kramarov. “Development of a system for the detection of cyber attacks based on the clustering and formation of reference deviations of attributes”, *Eastern-European Journal of Enterprise Technologies 2017*, 3 (9(87)), pp. 43–52.

[36] Al Hadidi, M. M., Ibrahim, Y. K., etc. "Intelligent Systems for Monitoring and Recognition of Cyber Attacks on Information and Communication Systems of Transport", *International Review on Computers and Software (IRECOS)*, 2016, 11(12), pp. 1167–1177.

[37] Lakhno, V. A., Petrov, O. S., Hrabariev, A. V., Ivanchenko, Y. V., & Beketova, G. S. "Improving of information transport security under the conditions of destructive influence on the information-communication system", *Journal of theoretical and applied information technology*, 89(2), 2016, pp. 352–362.

[38] Lakhno, V. A., Kravchuk, P. U., Pleskach, V. L., Stepanenko, O. P., Tishchenko, R. V., & Chernyshov, V. A. “Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems”, *Journal of Theoretical and Applied Information Technology*, 95(8), 2017, pp. 1705–1714.

[39] B. Akhmetov, etc., “Decision support system about investments in smart city in conditions of incomplete information”, *International Journal of Civil Engineering and Technology*, 10 (2), 2019, pp. 661–670.

[40] Bidiuk, P.I., Prosiankina-Zharova, T.I., Terentieev, O.M., etc. “Intellectual technologies and decision support systems for the control of the economic and financial processes”, *Journal of Theoretical and Applied Information Technology*, 2019, 97 (1), pp. 71–87.

[41] B. Akhmetov, etc. “Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity”, *Advances in Intelligent Systems and Computing*, 860, 2019, pp. 162–171. DOI: 10.1007/978-3-030-00184-1_15

[42] Akhmetov, B., Balgabayeva, L., etc. “Mobile platform for decision support system during mutual continuous investment in technology for smart city”, *Studies in Systems, Decision and Control*, 199, 2019, pp. 731–742. DOI: 10.1007/978-3-030-12072-6_59

[43] Akhmetov, B. etc. "Models and algorithms of vector optimization in selecting security measures for higher education institution's information learning environment", *Advances in Intelligent Systems and Computing*, 860, 2019, pp. 135–142. DOI: 10.1007/978-3-030-00184-1_13

[44] Akhmetov, Bakhytzhan, Kydyralina, L. etc. "Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions", *International Journal of Mechanical Engineering and Technology*, 9 (10), 2018, pp. 1114–1122.

[45] Akhmetov, Berik, etc. "System of decision support in weaklyformalized problems of transport cybersecurity ensuring", *Journal of Theoretical and Applied Information Technology*, 96 (8), 2018, pp. 2184–2196.

[46] Akhmetov, B.S., Akhmetov, B.B., et al. (2019). "Adaptive model of mutual financial investment procedure control in cybersecurity systems of situational transport centers", *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*, Vol.3, Iss. 435, pp. 159–172.