BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 1, Number 383 (2020), 128 – 139 **https://doi.org/10.32014/2020.2518-1467.16**

UDC 621.39:004.05

B. B. Akhmetov[1], V. A. Lakhno[2], A. B. Adranova[3], L. M. Kydyralina[3], L. D. Pliska[2]

[1]Yessenov University, Aktau, Kazakhstan;
[2]National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine;
[3]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan.
E-mail: berik.akhmetov@yu.edu.kz, Valss21@ukr.net, assel.adranova@gmail.com, lazat_75@mail.ru, luba.pliska@gmail.com

ANALYSIS OF MATHEMATICAL MODELS OF INVESTMENT STRATEGIES IN THE UNIVERSITY ON CYBER SECURITY SYSTEMS

Abstract. The article provides an overview and analysis of mathematical models for choosing investment strategies in cybersecurity systems of informatization objects (IO) as a particular example of educational information systems (IS). The purpose of the work is the analysis and comparison of known and new investment models for the IO protection. It is shown that previous researches have often purely economic nature and do not take into account the trends relating to the introduction of innovative information technologies in the control and decision-making procedures of the IO cybersecurity tasks. It is shown that the optimal value of resources allocated for the IO protection and cybersecurity depends not only on the vulnerabilities of IS, but also on the cost of information should be protected. All this makes it relevant to develop new models for the decision-making support on the IO protection and cybersecurity investment. The task, in particular, can be solved through the use of new information technologies and computer-based decision support systems (DSS). As a variant, it was proposed to use as a basic mathematical model for DSS the models based on game theory.

Key words: cybersecurity, information and educational environment of the university, investment, model, decision support system.

Introduction. Nowadays, information is the most valuable asset for any company or educational institution. Information and information technologies (IT) have become the basis of all educational and business processes in educational institutions. Modern universities today are at the forefront of innovative developments and projects in all areas of human activity[1]. Weak information security in the information and educational environment of the university (IEEU) can be a serious problem for the reputation and financial condition of universities.

Modern cyber attacks on important IS, in particular, on the IEEU have contributed to the development of researches that are associated with the intellectualization of calculations in the field of decision support for IP and cybersecurity (CS).

Investments in innovative projects, for example, in IT and CS, in many cases are determined by a high probability of inaccurate calculations. Created in recent years by various decision support systems (DSS) companies in IT and CS investment tasks have received good responses. Some of these DSSs provide an opportunity to optimize procedures related to the search for multivariate strategies for the financial investment of projects in the field of IEEU CS [1,2].

The purpose of the article. The purpose of the work is the analysis and comparison of known and new investment models for the protection of the information and educational environment of universities (IEEU).

Main part. The most common practical model was proposed by American researchers Lawrence Gordon and Martin Loeb of the Maryland University in 2002 [3]. The paper describes an economic model that determines the optimal amount of investments in order to protect a given set of information. The model takes into account the information vulnerability for security hacking and the potential loss in case of such hacking. It is shown that for a given potential loss, a company does not necessarily have to focus its investments on information sets with the highest vulnerability. Since extremely vulnerable sets of information may be prohibitively expensive in protection, the companies should better focus their power on information sets with medium-level vulnerabilities. The analysis also suggests that in order to maximize the expected benefits from investments in order to protect information, a company must spend only a small part of expected losses due to a security breach [3].

The model structure is static - decisions and results come at the same time, and dynamic effects, including the dependence of money on time, are not taken into account. An information set can take various forms, such as a customer list, a payables book:

λ – monetary loss caused by the security breach of the information set;

t – probability of attack, $t \in [0,1]$;

ν – the vulnerability of information, which means the probability that in condition of investment absence the attack will be successful for λ; $0 \le \nu \le 1$;

z – information security costs.

For the model $\lambda = const$, although in practice $\lambda = \lambda(t)$ λ the value t is a single attack (the simultaneous attacks are not considered).

Other values are also considered:

νt – probability of loss as a result of attacks;

$L = t\lambda$ – potential losses associated with an information asset;

$S(z,\nu)$ – probability of security breach.

The nature of information vulnerability and information security leads to consideration of the following assumptions (A1, A2, A3) regarding $S(z,\nu)$:

A1. $S(z,0) = 0$ for all z. That is, if the set of information is completely invulnerable, it will remain ideally protected for any amount of investments in security, including zero investment.

A2. For all ν, $S(0,\nu) = \nu$. That is, if there is no investment in information security, the probability of a security breach due to the realization of a threat will remain unchanged.

A3. For all $\nu \in (0,1)$ and all z, $S_z(z,\nu) < 0$ and $S_{zz}(z,\nu) > 0$, where S_z determines the partial derivative according to z and S_{zz} denotes the partial derivative from S_z with respect to z. Therefore, as investments in information security increases, information becomes more secure. In addition, there is an assumption that for all $\nu \in (0,1)$, $\lim S(z,\nu) \to 0$, as $z \to \infty$, therefore, due to the security investment the probability of a security breach is t times $S(z,\nu)$ that is, it can reach a zero [3].

The expected benefits from investments in information security, referred to as EBIS (Expected Benefits of an Investment in Information Security), are equal to the reduction of the expected losses of the company related to additional security:

$$EBIS(z) = [\nu - S(z,\nu]L. \tag{1}$$

The expected net income from an investment in information security (Expected Net Benefits from an Investment in Information Security, ENBIS) is equal to the difference of EBIS and the costs of investments:

$$ENBIS(z) = [\nu - S(z,\nu)]L - z. \tag{2}$$

The optimal size of investment is $z^*(\nu)$ at which $ENBIS(z)$ reaches the maximum value.

In [3] there were proposed two classes of vulnerability functions that meet the conditions of A1 – A3.

The first class of exponential functions:

$$S^I(z,\nu) = \frac{\nu}{(\alpha z + 1)^{\beta}}, \tag{3}$$

where the parameters $\alpha > 0$, $\beta \geq 1$ are the measures of information security performance (for the given ν and z the probability of a security breach decreases for both, α and β). From the condition $ENBIS'_z(z^*)=0$ it follows that the optimal amount of investments can be calculated as follows:

$$z^{I*}(\nu)=\frac{(\nu\beta\alpha L)\dfrac{1}{\beta+1}}{\alpha}. \tag{4}$$

That is, from (4) it follows that $z^{I*}(\nu)=0$ is for $0 \leq \nu \leq 1/\alpha\beta L$. Therefore, the optimal investments in security for the first class is zero until such the value ν does not increase up to $\nu=\dfrac{1}{\alpha\beta L}$. With a further increase of the ν threats probabilities, the value $z^{I*}(\nu)$, in accordance with (3), increases with decreasing speed.

The second class of exponential functions:

$$S^{II}(z,\nu)=\nu^{\alpha z+1}, \tag{5}$$

where the parameter $\alpha > 0$ - the measure of information security performance. From the condition $ENBIS'_z(z^*)=0$ we obtain:

$$z^{II*}(\nu)=\frac{\ln(\dfrac{1}{-\alpha\nu L(\ln\nu)})}{\alpha\ln\nu}. \tag{6}$$

From (6) it follows that for the second class of functions $S(z,\nu)$, the function z^{II*} firstly increases and then decreases with increasing of ν .

Despite the fact that the Gordon-Loeb model after publication was recognized in the scientific community and supplemented, both by other authors [4,5,6] and by Lawrence Gordon and Martin Loeb [7], many issues should still be resolved. The indisputable fact is that the authors of the model for the first time thoroughly examined the problem and identified the vulnerability function, which is a key indicator of information security.

We can distinguish the following disadvantages of the model:

1. It depends on the constant growth of cash receipts, the model is a single-phase, so it should not be used to evaluate companies whose cash receipts can vary considerably. For such companies it is better to use a multi-phase model. Based on the above mentioned, we can conclude that this model is more suitable for evaluating large companies that have already exhausted all the opportunities for the growth.

2. Too susceptible to input information, does not take into account changes in dividend policy, share repurchases, and others.

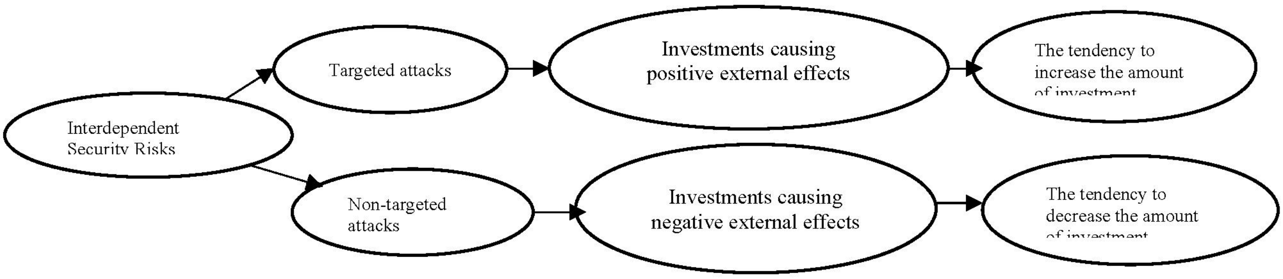
3. Focuses mainly on the study of the optimization aspects of risks control, which almost minimizes the possibility of taking into account the real risk object.

4. Discounted rate is greater than the growth of dividend payments.

Wuhenn Shim, on the basis of the work of Gordon-Loeb [3], developed his model of interrelated risks for two identical enterprises [8]. The author demonstrated that the optimal amount of investments in cybersecurity with negative external effects will be greater or equal to the optimal amount of investments with independent risks, and the area of zero investments will be less. If the cooperation of enterprises creates positive external effects, then the optimal amount of investments in cybersecurity will be greater or equal to the optimal amount of investments with independent risks, and the area of zero investments will be identical to the model with independent risks.

In addition, Shim [9] theoretically and empirically proved that financial investments for resisting untargeted attacks and aimed at damaging the maximum possible amount of susceptible systems will cause positive external effects, because an increase of financial investments of an organization will reduce the risks of other companies connected to the system of this company. As a result, a relationship was depicted among external effects problems and types of attacks, as shown on figure.

Both of the models discussed above have disadvantages. None of them takes into account the calculation of the optimal solution in a dynamic mode, in particular the effect of financial investments. For example, they do not analyze how the intruder changes the strategies of his attacks after the appearance of additional financial investments in cybersecurity. For each of these models, there is the difficulty of obtaining data, such as quantitative losses evaluation, threats probability evaluation and evaluation of the system susceptibility to the intruders attacks. The model of interrelated risks is only suitable for the same enterprises, therefore it is not suitable for all organizations. Both models are based on two classes of information system vulnerability functions.


Interdependent Security Risks
Targeted attacks
Investments causing positive external effects
The tendency to increase the amount of investment
Non-targeted attacks
Investments causing negative external effects
The tendency to decrease the amount of investment

Communication between external effects and types of attacks

In the work of **V.K. Zadiraky and co-authors** [10] there was considered a version of the model for determining the amount of information protection costs that could be useful for organizations in order to create or to improve their own information security system.

The total expected amount of information security losses V can be expressed as the sum of expenses S and potential losses $b(S)$:

$$V = S + b(S). \tag{7}$$

Function (7) can be represented as a targeted one, which should be minimized:

$$V(S) = S + b(S) \to \min. \tag{8}$$

Investment of the information protection costs S should reduce the amount of expected losses $b(S)$ from a security breach, larger values of S corresponds to smaller values of $b(S)$:

$$0 < S_1 < S_2 \Rightarrow b(S_2) < b(S_1) < b(0) = B. \tag{9}$$

The formula (9) means that the function $b(S)$ is monotonically decreasing, and therefore the rate of change $b(S)$ of expected losses of costs is negative:

$$b^{'}(S) < 0. \tag{10}$$

Maximum value of S – costs we obtain in the following way:

$$S_{\max} = \frac{\nu B^{1-\nu} - B^{1-\nu}}{(\nu-1)(\nu B^{1-\nu})\frac{\nu}{\nu-1}} = \frac{(B^{1-\nu})^{\frac{1}{\nu-1}}}{\nu\frac{\nu}{\nu-1}} = \frac{B}{\nu^{\frac{\nu}{\nu-1}}}. \tag{11}$$

In the work of **Glushak-Novikov** [11, 12] there was proposed an approach in order to solve the problem of creating an information protection system with the condition of the complex nature of the attacks and with the limited resources of the protector in order to create a protection system. According to the developed model, there was formed an optimization task to decrease the costs for the creation of a protection system at the presence of information about the attacker and vulnerabilities in the system.

The object of the study is a distributed information and communication system (ICS) with an open architecture, which consists of C interacting components involved in information processing. Each component is described by a set of characteristics, including information processing technology, operating environment, and others. The specified parameters of the components determine their value for the system, which will be denoted by q_c.

Taking into account the nature of the computing environment, each of the components is vulnerable to certain threats with A acceptable threats. It is assumed that the information about the architecture of the ICS is opened and is known to the sides of the conflict. In addition, there is given the probability of successful realization of a threat α against a component of the system c, as well as the probability of neutralizing the threat by establishing protection mechanisms p. Therefore, random factors that need to be considered at modeling are influencing the effectiveness of decisions made by an attacker or protector.

Relationships between the protector and the attacker can be formalized using the risk function. The attacker, by damaging the system, tries to maximize the risk. At the same time, the protector, opposing the attacker, establishes protection mechanisms, seeking to reduce the risk to a zero. In conditions of limited financial and technical resources, according to a predetermined model of an attacker, the protector needs to distribute the means and protection measures so that the risk in ICS was minimal. In terms of game theory, the risk function is a payment function. The quantitative value for risk assessment is the caused damage Q_c, which is expressed in the form of costs and lost benefits. Therefore, the damage value Q_c is caused by a certain component c equivalent to the value of this component q_c for the functioning of the system as a whole. In general, the ratio for the information security risk function $R_{\alpha c}$ can be written as the composition of the probability $P^{\sim}_{\alpha c}$ of the threat realization α and the caused damage during the realization of this threat Q_c. The variable $V_{\alpha c}$ describes the probability of neutralizing the threat using the established additional protection mechanisms [11]:

$$R_{\alpha c} = P^{\sim}_{\alpha c} * Q_c * (1 - V_{\alpha c}). \tag{12}$$

One of the features of the confrontation between the protector and the attacker is dynamic character, since the attack is usually preceded by monitoring the system and intelligence, which must be taken into account in the model. Therefore, the state of conflict can change over time.

The creation of an information protection system (IPS) according to the developed approach [12] can be divided into the following stages:

1. Collection and analysis of initial information using expert assessment methods - structure analysis, vulnerability analysis, threat analysis.

2. Synthesis of the information security system structure. We substitute the initial data obtained at the first stage into the model. As a result the solution of the obtained problem using the method simplex was obtained by the relative value of risk R, as well as a set of protection mechanisms that will be optimal during the confrontation.

The model of confrontation between the two sides, developed within the framework of the RAND company, is the **model of Gross** [13], designed to simulate tactical military operations. According to this model, the conflicting sides have the resources X and Y, and the result of their opposition is determined by the objective function, which linearly depends on the difference of the invested resources and leads to the linear programming problem:

$$i(x,y) = \sum\nolimits_{k=1}^{l} i_k(x_k y_k) = \sum\nolimits_{k=1}^{l} g_k \max(x_k - y_k, 0), \tag{13}$$

where k – object number, x_k and y_k– attack and protection resources at k object, g_k – a weight coefficient which expresses the importance of objects or their vulnerability.

The value $\max(x_k - y_k, 0)$, the value of which is the larger of the two numbers $x_k - y_k$ and 0, is the part of the unit x_k that is able to penetrate the protection to the object. Therefore, the value $g_k \max(x_k - y_k, 0)$ characterises the success of the attack on the k object. For the applying to information security tasks, g_k expresses the relative value of information at the k object, and $g_k \max(x_k - y_k, 0)$ - the damage caused by information leakage. Since the damage cannot be greater than its cost, it should be $i(x,y) = 1$ at $x - y \geq 1$. Consequently, the function $i(x,y)$ has a piecewise linear character. The entire interval of a variable x, with a constant value of y, can be divided into three zones, bounded by two limiting values x_1 and x_2, at $x < x_1$ we have $i(x,y) = 0$, at $x > x_1 - i(x,y) = 1$, at $x_1 < x < x_2$ - the function $i(x,y)$ grows linearly with an angular coefficient g. Taking into account the above considerations, the objective function, which expresses the damage caused by the information leakage, takes the form [13]:

$$i(x,y) = \sum\nolimits_{k=1}^{l} g_k (x_k - y_k), \tag{14}$$

where $x_k - y_k = \begin{cases} 0 \; at \; x_k - y_k \leq 0; \\ \mathrm{x_k} - y_k \; at \; 0 < x_k - y_k \leq 1; \\ 1 \; at \; x_k - y_k > 1. \end{cases}$.

The task of Gross, which arose during the planning of military operations, has a number of differences from the considered tasks. Firstly, the objective function has a discrete nature, since it determines the amount of units that broke through the protection or that destroyed the attack or protection. Secondly, these units in each episode of confrontation are the same for attack and, accordingly, for protection. The uniformity of objects greatly simplifies the solution of the problem, but limits the conditions of the confrontation. However, the main disadvantage of the Gross model is the piecewise linear character of its objective function, which, of course, cannot correspond to real conditions. For this reason, the Gross model, at its simplicity, is used only to approximate the objective function and to obtain results at the first approximation [13].

The research [14] describes the study of cyber attack on the information sphere by **Grischuk R. V.** An assessment of the cyber attacker's capabilities during cyber attacks is carried out using game methods for cyber attacks analysis.

The author reviewed the non-cooperative cyber attack A of n cyber attack players on information systems:

$$A = \left\langle N, \{x_i\}_{i \in N,} \{f_i(x)_{i \in N}\} \right\rangle, \tag{15}$$

where n – the amount of cyber attack players that is defined on the set N, $n \in \{N\}, N = \{1,2,...,n\}$; i – the number of cyber attack player, $i \in \{N\}$; x_i – i cyber attack player strategy, $x_i \in \{X_i\}$; $f_i(x)$ – a fee of i player of the cyber attack A at choosing by n players their own strategies x of the cyber attack $x \in \{X\}$.

The fee for a successful cyber attack of the i player has the form of a quadratic function:

$$f_i(x) = xM^{(i)}x^T, \tag{16}$$

where $M^{(i)}$ – symmetric scalar quadratic matrix, x^T – column vector.

The aim of a cyber attack for i player in a cyber attack is to choose such a strategy $x_i \in X_i$ when the success of the implementation will be greatest:

$$f_i(x) \to \max. \tag{17}$$

This model does not take into account the impact of investments on the choice of the optimal solution, however, the researchers demonstrate how the developed game analysis methods allow to evaluate both single and group cyber attacks. This allows to receive guaranteed and reliable estimates of the information security level from cyber attacks on the information sphere.

Works **O. E. Arkhipov** [15, 16] study the use of "attack-protection" economic value models for risk assessment and research of the effectiveness of investments in information security.

There was considered the situation that arises when an attacker A implements a threat T with respect to a certain information resource I that belongs to the side B. It is assumed that D - the total cost of expenses of the attacking side A for the implementation of the threat T , g - the resulting "benefit", the value of which is determined by the value of the resource I for the attacker. The damage incurred in this situation by the side B (the owner of the resource I), that is, the cost of the resource from the point of view of its owner, is estimated by him as q , and the total cost of the implemented complex of protective measures is equal to c.

On the basis of this information, it is possible to create a logical-heuristic scheme for expert estimation of probabilistic characteristics used to calculate information risks. The net income of the attacker in case of a successful threat T is $Q = g - D$. If the value g of the resource I for the attacking side A is significant, in particular, if $g >> D$ it can be assumed that the attacker will try to use any chances to realize this threat. On the contrary, for small values of g the economic motives for the occurrence of a threat T are practically absent: at $Q = 0$ (or $g = D$) an attack of a resource becomes impractical, in this case $P_t = 0$. For $g < D$ an attempt to realize the threat T loses all economic sense. Based on these considerations, in [15] there is proposed a relationship:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}, \tag{18}$$

which can be used to estimate the approximate values of the activation probability (occurrence) of the threat T . In the general case, the probability of a threat T realization is a composition of:

$$P_T = P_t P_v, \tag{19}$$

where P_v - the probability of use by an attacker successfully the information system vulnerabilities (IS or IO) containing an information resource I. The probability value P_v depends on the degree of IP protection, which, in turn, is determined by the volume of investments in IPS, which with a certain approximation is taken into account by the relation [16]:

$$P_v = \frac{q}{q + sc}, \tag{20}$$

where s – the coefficient by which the level of investments efficiency c in the information protection system is determined, namely: the larger the value s is, the lower, under the condition of the same investment volume of c, the probability value P_v. From the formula (20) it is obvious that at the absence of critical information in IS (that is $q = 0$) the probability is $P_v = 0$. When the cost q of a resource I is high or very high, however, the costs on the creation and operation of IPS are low, that is $q >> sc$, the probability is $P_v \to 1$. If the owner of the resource I pays enough attention to its protection, the values q and sc are proportionate, $P_v < 1$. In general, the probability value P_V at $q = const$ grow with a decrease in the level of IPS investment c and vice versa, increase with the growth of their volume. Formulas (18), (20) allow to create an optimization scheme, according to which it will be possible to draw conclusions about the effectiveness and feasibility of investing in IPS. For this, it is assumed in [16] that with a zero investment in IPS $P_v = 1$ the output information risk is $R_1 = P_t q$. Investing in IPS the costs c (under the condition of rational costs of these funds for the needs of protection) leads to the fact that the probability of successful execution of vulnerability becomes less than 1, that is $P_v < 1$. The residual risk in this case will be equal to $R_t = P_t P_v q$, the amount of losses that could be prevented – $R_1 - R_t = P_t q - P_t P_v q = (1 - P_v) P_t q$ and the corresponding "income" – $\Delta_R = R_1 - R_t - c = (1 - P_v) P_t q - c$.

The economic value model is based on the results of the analysis of the real indicators of the organization's information system security level, information security requirements, requiring the use of real information risk control mechanisms, taking into account economic trends, and then allows to hope to achieve more objective results at assessing the optimal investment volume in the information protection system.

The cost-based "attack-protection" models also provide an opportunity, on the basis of specific information about a real organization, to check whether the funds invested in the information security of this organization are sufficient in volume.

Levchenko and co-authors in works [17,18,19,20] proposed a mathematical model that provides for the use of the objective function $i(x;y)$, where i is assigned to the total amount of the lost information cost, x and y is the i attack and protection resources, respectively. This function in general terms has the form:

$$i(x,y)=\sum\nolimits_{k=1}^{l} i_k(x,y)=\sum\nolimits_{k=1}^{l} g_k p_k q_k(x,y) f_k(x,y), \tag{21}$$

where $k=\overline{1,l}$ – the object number; g_k – amount of information on the object; p_k – probability of attack on an object; $q_k(x;y)$ – the probability density of allocation of attacks resources x on k object; $f_k(x;y)$ – dependence of the share of lost information on the ratio of x and y, which can be considered as the probability of information loss at given values x and y.

Two classes of functions are proposed as dependencies. $f_k(x,y)$:

$$\text{range } f(x,y)=\frac{\alpha(x/y)^n}{b(x/y)^n+c}, \tag{22}$$

$$\text{exponential } f(x,y)=d(1-e^{-m(x/y)^n}), \tag{23}$$

where the parameters α, b, c, d, n, m take positive values and determine the position and slope of the curves.

The work [17] proposed two possible types of dependencies $q(x)$ in the form $q(x)=Nx^n e^{-h^2x^2}$: the Maxwell distribution $q_M(x)=Nx^2e^{-h^2x^2}$ and the Rayleigh distribution $q_p(x)=Nxe^{-h^2x^2}$, where N is the normalization coefficient and the constants n, h determine the position of the dependence maximum and the degree of its asymmetry. Comparing these distributions, their essential difference lies in the fact that for the $q_M(x)$ in the initial area $x \overset{\sim}{>} 0$ the convexity is directed downwards and for $q_p(x)$ - upwards.

The given values allow the managers of a company or an educational institution to conclude that the allocated funds are sufficient or expedient to increase them. This depends, of course, on the permissible values $i(x,y)$, which, in turn, are determined from the subjective assessment of the top manager and his risk tendency.

Also, in order to invest cybersecurity, there are created new models based on game theory. One of these models is the Akhmetov-Malyukov model.

The **Akhmetov-Malyukov model** [21] describes a model for cybersecurity systems investment. The pure strategy of the first ally-player is the function $u:T\cdot[0,1]\cdot[0,1]\to[0,1]$, setting to the state of the information (position) $(t,(z_1(0),z_2(0)))$ the value $u(t,(z_1(0),z_2(0)))$: $0\le u(t,(z_1(0),z_2(0)))\le 1$, where u is the control parameter of the first investor; t - time parameter; z_1 - the value of the financial resource of the first investor; z_2 - the value of the financial resource of the second investor. With regard to the awareness of the opponent player (within the framework of the positional game scheme), no assumptions are made, which is equivalent to the fact that the opponent player chooses his control action $u(t)$ based on any information.

For any moment of time t, following conditions are met: $\alpha_1(t)=\alpha_1$; $\alpha_2(t)=\alpha_2$; $\beta_1(t)=\beta_1$; $\beta_2(t)=\beta_2$; $r_1(t)=r_1$; $r_2(t)=r_2$. We denote: $q_1=(1-\beta_1)\cdot(a_1+r_1)-1$; $q_2=(1-\beta_2)\cdot(a_2+r_2)-1$, where α_1 – the coefficient determining the interest fee for the financial resource of the second investor to the first investor; α_2 - the coefficient determining the interest fee for the financial resource of the first investor to the second investor; β_1 - the coefficient determining the share of repayment of the debt of the first investor to the second investor; β_2 - the coefficient determining the share of repayment of the debt of the second investor to the first investor; r_1 - the coefficient determining the share of return of the financial resource of the second investor to the first investor; r_2 - the coefficient determining the share of return of the financial resource of the first investor to the second investor; q^* - the coefficient that determines the equilibrium beam.

In [21], there was proposed a model for a decision support system module for mutual investment in the cybersecurity systems of a situational transport center. The model allows to predict the results of investment and to find strategies for investment process managing. Unlike the existing solutions, the proposed model gives specific recommendations at choosing strategies in the investment process of a protected situational center creation. With an unsatisfactory forecast, a flexible adjustment of the parameters of the investment process is possible in order to achieve an acceptable financial result by the sides [21].

Analysis of mathematical models of investment strategies for cybersecurity systems showed that fixed assets and forces are applied to the issues of determining the amount of investment in order to protect information systems (table). In addition, existing models rarely take into account how the intruder changes his cyber attack tactics in response to additional investments in information security. There are difficulties in obtaining data for models, such as a numerical assessment of the caused damage, the probability of threats and vulnerabilities.

Mathematical models of investment strategies for information security

Comparison criteria	Gordon-Loeb model	Wuhenn Shim model	Arkhipov model	Levchenko-Prus model	Zadiraky model	Akhmetov-Malyukov model
Calculation of the optimal solution in a dynamic mode	–	–	+	+	–	+
Object Vulnerability Accounting	–	–	+	+	–	–
Resource allocation optimization	+	+	–	+	–	+
Security means accounting	+	+	+	+	+	–
Attacking means accounting	–	–	+	+	–	–
The difference between positive and negative effects	–	+	–	–	–	–
Accounting of the cost of each protection	–	–	+	–	–	–

Conclusions. It is shown that the disadvantage of most of the considered models is the lack of specific recommendations on the formation of strategies for financial investments in protection and cyber security systems.

There is justified the need to develop new models of DSS, which will allow finding optimal strategies for financial investments in information protection and cybersecurity of the information and educational environment of universities.

It is shown that the DSS in the investment problems of IEEU CS can be created on the basis of the application of mathematical models of game theory, which make it possible to find rational investment strategies.

Б. Б. Ахметов[1], В. А. Лахно[2], А. Б. Адранова[3], Л. М. Кыдыралина[3], Л. Д. Плиска[2]

[1]Есенов университеті, Ақтау, Қазақстан;
[2]Украинаның биоресурстар және табиғатты пайдалану ұлттық университеті, Киев, Украина;
[3]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Казақстан

УНИВЕРСИТЕТТЕРДІҢ КИБЕРҚАУІПСІЗДІК ЖҮЙЕСІНЕ ИНВЕСТИЦИЯЛАУ СТРАТЕГИЯЛАРЫНЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІН ТАЛДАУ

Аннотация. Мақалада оқу орындарының ақпараттық жүйелерінің (АЖ) жеке мысалы ретінде ақпараттандыру объектілерінің (АОб) киберқауіпсіздік жүйесіне инвестициялау стратегиясын таңдау үшін математикалық модельдерге шолу және талдау жасалған. Білім беруде алдыңғы қатарлы цифрлық технологияларды жылдам игеретін оқу орындарының ақпараттық жүйелерінің жұмысына деструктивті араласу санының өсуі жағдайында бәсекеге қабілеттілік және табысты дамудың негізгі шарты ақпаратты сауатты құрылған қорғау ақпараттары болуы мүмкін.

Жұмыстың мақсаты - АОб-ін қорғауға инвестициялаудың белгілі және жаңа үлгілерін талдау және салыстыру. Алдыңғы зерттеулер жиі таза экономикалық сипатқа ие және АОб-нің киберқорғау міндеттерін бақылау және шешімдер қабылдау рәсімдеріне инновациялық ақпараттық технологияларды енгізуге қатысты үрдістерді ескермейді.

Ақпараттандыру объектілерінің және университеттердің киберқауіпсіздігіне қаржы салымдарын бағалау есебінде пайдаланылатын негізгі модельдерге жан-жақты талдау жасалды. Гордон-Лоеба моделі талданды, ол қауіпсіздікті бұзу үшін ақпараттың осалдығын және осындай бұзу жағдайында жоғалту ықтималдығын ескереді. Сонымен қатар өзара байланысты тәуекелдер үшін В. Шим модельдері, В.К. Задирак, Глушак-Новикова модельдері зиянкестің шабуылдарының кешенді сипаты және қорғау жүйесін құруға қорғаушы ресурстарының шектеулілігі шартымен ақпаратты қорғау жүйесін құру бойынша міндеттерді шешу әдісі ұсынылған. Әр түрлі авторлардың басқа да модельдері қарастырылған.

Университеттің ақпараттық-білім беру ортасындағы (ББАЖ) мәліметтердің әлсіз қорғалуы университеттердің беделі мен қаржылық жағдайы үшін маңызды проблемалардың пайда болуына себеп болуы мүмкін екені анықталды.

АОб-ін қорғау мен киберқауіпсіздігіне бөлінетін ресурстардың оңтайлы мәні ақпараттық жүйенің осалдықтарына ғана емес, қорғауға жататын ақпараттың құнына да байланысты екендігі көрсетілді. Осының барлығы ақпараттандыру объектілерін қорғау мен киберқауіпсіздігіне инвестициялау бойынша шешімдер қабылдауды қолдау үшін жаңа модельдерді әзірлеуді өзекті етеді. Міндет, атап айтқанда, жаңа ақпараттық технологиялар мен шешімдерді қабылдауды қолдаудың компьютерлік жүйелерін (ШҚҚЖ) қолдану негізінде шешілуі мүмкін. Нұсқа ретінде ұсынылған, шешім қабылдауды қолдау жүйесі үшін базалық математикалық модель ретінде, ойын теориясының негізінде модельді пайдалану.

Ақпаратты қорғау жүйесіне және ақпараттандырудың әртүрлі объектілерінің киберқауіпсіздігіне, оның ішінде оқу орындарының ақпараттық жүйелеріне инвестициялау тиімділігін бағалау үшін қолда бар модельдерге талдау жасалды.

Осы саладағы зерттеулердің көпшілігі қорғау жүйесіне қаржы қаражатын салудың оңтайлы стратегияларын іздестіру міндетін экономикалық тұрғыдан қоюға ғана назар аударылғандығы және инвестициялық жобалар үшін бақылау және шешімдер қабылдау рәсімдеріне ақпараттық технологияларды енгізуге қатысты үрдістерді ескермегені көрсетілген.

Түйін сөздер: киберқауіпсіздік, университеттің ақпараттық-білім беру ортасы, инвестициялау, модель, шешім қабылдауды қолдау жүйесі.

Б.Б.Ахметов[1], В.А.Лахно[2], А.Б.Адранова[3], Л.М.Кыдыралина[3], Л.Д.Плиска[2]

[1]Университет Есенова, Актау, Казахстан;
[2]Национальный университет биоресурсов и природопользования Украины, Киев, Украина;
[3]Казахский национальный педагогический университет имени Абая, Алматы, Казахстан

АНАЛИЗ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ СТРАТЕГИЙ ИНВЕСТИРОВАНИЯ В СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ УНИВЕРСИТЕТОВ

Аннотация. В статье выполнен обзор и анализ математических моделей для выбора стратегий инвестирования в системы кибербезопасности объектов информатизации (ОбИ), как частного примера информационных систем (ИС) учебных заведений. Показано, что в условиях роста количества деструктивных вмешательств в работу ИС учебных заведений, которые стремительно осваивают передовые цифровые технологии в образовании, основополагающим условием конкурентоспособности и успешного развития может послужить грамотно выстроенная защита информации.

Цель работы – анализ и сравнение известных и новых математических моделей инвестирования в защиту объектов информатизации. Показано, что предшествующие исследования часто носят чисто экономический характер и не учитывают тенденции, касающиеся внедрения инновационных информационных технологий в процедуры контроля и принятия решений в задачах киберзащиты ОбИ.

Выполнен всесторонний анализ основных моделей, используемых в задаче оценки финансовых вложений в кибербезопасность ОбИ, и университетов, в частности. Проанализированы модель Гордона-Лоеба, которая учитывает уязвимость информации для взлома безопасности и потенциальную потерю в случае такого взлома. Также рассмотрены модели В. Шима для взаимосвязанных рисков, модель В.К. Задираки, модель Глушака-Новикова, в которой предложен подход к решению задачи по созданию системы защиты информации с условием комплексного характера атак злоумышленника и ограниченности ресурсов защитника на построение системы защиты. Рассмотрены и другие модели различных авторов.

Установлено, что слабая защищенность данных в информационно-образовательной среде университета (ИОСУ) может послужить появлением серьезных проблем для репутации и финансового состояния университетов.

Показано, что оптимальное значение ресурсов, выделяемых на защиту и кибербезопасность ОбИ, зависит не только от уязвимостей ИС, но и от стоимости информации, которая подлежит защите. Все это делает актуальным разработку новых моделей для поддержки принятия решений по инвестированию в защиту и кибербезопасности ОбИ. Задача, в частности, может быть решена на основе применения новых информационных технологий и компьютерных систем поддержки принятия решений (СППР). Как вариант предложено, использовать в качестве базовой математической модели для СППР, модели на основе теории игр.

Выполнен анализ имеющихся моделей для оценивания эффективности инвестирования в системы защиты информации и кибербезопасности различных объектов информатизации, в том числе, информационных систем учебных заведений.

Показано, что большинство исследований в данной области акцентировано лишь на экономической постановке задачи поиска оптимальных стратегий вложения финансовых средств в системы защиты и не учитывают тенденции, касающиеся внедрения информационных технологий в процедуры контроля и принятия решений для инвестиционных проектов.

Ключевые слова: кибербезопасность, информационно-образовательная среда университета, инвестирование, модель, система поддержки принятия решений.

Information about authors:

Akhmetov Berik Bakhytzhanovich, candidate of technical sciences, academician of the international academy of informatization, rector of the caspian state university of technology and engineering named after Sh. Yessenov; berik.akhmetov@yu.edu.kz; https://orcid.org/0000-0003-2860-2188

Valeriy Lakhno, doctor of technical sciences, professor, computer systems and networks department, national university of life and environmental sciences of Ukraine; Valss21@ukr.net; https://orcid.org/0000-0001-9695-4543

Adranova Asselkhan, PhD student, Abai Kazakh National Pedagogical University; assel.adranova@gmail.com; https://orcid.org/0000-0001-7233-4104

Kydyralina Lazat, PhD student, Abai Kazakh National Pedagogical University; lazat_75@mail.ru; https://orcid.org/0000-0002-2836-0919

Pliska Luba, Post graduate student, national university of life and environmental sciences of Ukraine; luba.pliska@gmail.com; https://orcid.org/0000-0002-6383-7233

REFERENCES

[1] Lakhno V. (2017) Development of the decision making support system to control a procedure of financial investment / V.A. Lakhno,V. Malyukov, N. Gerasymchuk // Eastern-European Journal of Enterprise Technologies. 6(3):24-41. DOI: https://doi.org/10.15587/1729-4061.2017.119259 (In Eng.).

[2] Lakhno VA. (2017) Developmentof a support system for managing the cybersecurity [Text]// Radio Electronics, Computer Science, Control. 2:109–116. DOI: https://doi.org/10.15588/1607-3274-2017-2-12 (In Eng.).

[3] Gordon L. (2002) The Economics of Information Security Investment // Gordon L., Loeb M.// ACM Transactions on Information and System Security.5(4):438-457. DOI:10.1145/581271.581274 (In Eng.).

[4] Tleuberdiyeva G, Naizabayeva L (2016). Monte carlo method for simulation of the application process with the use of service-desk technical support // Bulletin of the National Academy of Sciences of the Republic of Kazakhstan. ISSN 1991-3494, Vol. 1, N 359: 32 – 39. DOI:10.1007/s10796-006-9011-6 (In Eng.).

[5] Willemson J. (2006) On the Gordon & Loeb Model for Information Security Investment // Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006). P. 101-112. DOI:https://www.econinfosec.org/archive/weis2006/docs/12.pdf (In Eng.).

[6] Sanalieva L.K., Kengzhegalieva G.B., Idelbayeva A.S., Niyazbekova Sh.U. (2018). Investigation of modern economic mechanisms for construction of the intellectual potential of the country as a moving factor of innovative economic development // Bulletin of the National Academy of Sciences of the Republic of Kazakhstan. Vol. 5, N 375, 144–148. ISSN 1991-3494. DOI:10.32014/2018.2518-1467.19 (In Eng.).

[7] Gordon LA, Loeb MP, Lucyshyn W. And Zhou L. (2015) Externalities and the Magnitude of Cyber Security Under investment by Private Sector Firms: A Modification of the Gordon-Loeb Model // Journal of Information Security. 6:24-30. DOI: 10.4236/jis.2015.61003 (In Eng.).

[8] Shim Woohyun (2011) Vulnerability and Information Security Investment under Interdependent Risks: A Theoretical Approach / Woohyun Shim // Asia Pacific Journal of Information Systems. 21(4): http://dx.doi.org/10.2139/ssrn.1830804 (In Eng.).

[9] Shim W. (2010) Interdependent risk and cybersecurity: Analysis of security investment and cyberinsurance //Michigan State University, EastLansing. (In Eng.).

[10] Murtazin Y.Z., Miroshnichenko O.L., Trushel L.Y. (2018). Methods of making of geoinformational and analytical system of groundwater resources in Kazakhstan// News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical sciences, 5: 21-31 DOI: 10.32014/2018.2518-170X.6 (In Eng.).

[11] Hlushak V.V. (2013) Syntez struktury systemy zahystu informacii z vykorystannjam pozycijnoi gry zahysnyka ta zlovmysnyka/ V.V. Hlushak, O.M. Novikov // Systemni doslidzhennja ta informacijni tehnologii. 2:89-100. (In Ukr.).

[12] Hlushak V.V., Novikov O.M. (2011) Metod proektuvannja systemy zahystu informacii z vykorystannjam determinovanoi gry “zahysnyk-zlovmysnyk” //Naukovi visti NTUU "KPI". 2: 46-53. (In Ukr.).

[13] Akhmetov B.S., Gnatyuk S., Zhmurko T., Kinzeryavyy V., Yubuzova Kh. (2018) Experimental research of the simulation model for deterministic secure communication protocol in quantum channel with noise // Reports of the National Academy of Sciences of the Republic of Kazakhstan, ISSN 2224-5227, Vol. 5, N 321 (2018), 5–11. DOI: https://doi.org/10.32014/2018.2518-1483.1 (In Eng.).

[14] Gryschuk R.V. (2011) Hierarchical differential-gaming model for evaluation efficiency of information systems protection/ R.V. Gryschuk// Informatics & Mathematical Methods in Simulation. N 2. (In Eng.).

[15] Arkhypov O. (2014) Methods and Approaches to Investigating Information Risks by Means of Economic Cost Models / O. Arkhypov, A. Skyba // The Advanced Science Journal. 2(12):75-82. DOI: 10.15550/ASJ.2014.12.075 (In Eng.).

[16] Arhypov O.Y. (2014) Informacijni ryzyky: metody ta sposoby doslidzhennja, modeli ryzykiv I metody ih identyfikacii / A.Y. Arhypov, A.V. Skyba // Zahyst informacii. 4:366-375. (In Ukr.) .

[17] Prus RB. (2010) Formation of the objective function in the tasks of information security management / R.B. Prus, V.A. Shvets // The Fourth World Congress – Aviation in the XXI-st Century‖ Safety in Aviation and Space Technologies. P. 17.14–17.17. (In Eng.).

[18] Levchenko Ye.G. (2011) Matematychni modeli ekonomichnogo menedzhmentu informacijnoi bezpeky / Ye.G. Levchenko, M.V. Demchyshyn, A.O. Rabchun // Systemni doslidzhennja ta informacijni tehnologii. 4:88-96. (In Eng.).

[19] Levchenko Ye.G. (2015) The correlation of expenses in multi-barrier information security systems / Ye.G. Levchenko, D.I. Rabchun// System research and information technologies. 2:131–140. (In Eng.).

[20] Levchenko Ye.G. (2010) Optymizacijni zadachi menedzhmentu informacijnoi bezpeky / Ye. G. Levchenko, A.O. Rabchun // Suchasnyj zahyst informacii. 1:16-23. (In Ukr.).

[21] Akhmetov B.B., Lakhno V.A., Akhmetov B.S., Malyukov V.P. (2018) 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. ISSN 1991-3494 Vol. 3, N 373 (2018), 6–14. DOI: https://doi.org/10.15588/1607-3274-2018-2-9 (In Eng.).