Journal of Theoretical and Applied Information Technology
31st July 2021. Vol.99. No 14
© 2021 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF MEASURES AIMED AT ENSURING INFORMATION SECURITY OF THE OBJECT OF INFORMATIZATION

LAKHNO V.[1], AKHMETOV B.[2], MAZARAKI A.[3], KRYVORUCHKO O.[4], CHUBAIEVSKYI V.[5], DESIATKO A.[6]

[1] National University of Life and Environmental Sciences of Ukraine,
Department of Computer Systems and Networks, Kyiv, Ukraine
[2]Caspian University of Technology and Engineering named after Sh. Yessenov,
Aktau, Republic of Kazakhstan
[3,4,5,6] Kyiv National University of Trade and Economics, Department of Software Engineering and
Cybersecurity, Kyiv, Ukraine,

E-mail: [1]lva964@gmail.com, [2]lim4best@gmail.com, [3]rector@knute.edu.ua,
[4]kryvoruchko_ev@knute.edu.ua, [5]chubaievskyi_vi@knute.edu.ua, [6]desyatko@gmail.com

ABSTRACT

The article analyzes publications on the evaluation of investments in information security (IS) of objects of informatization (OBI). The possibility and necessity of obtaining the necessary data have been substantiated, contributing to a reliable assessment of the effectiveness of measures aimed at increasing the company's IS. In the study process, the modelling methods have been used. A methodology is proposed for calculating indicators from investment activities in the context of increasing IS metrics of OBI. A specific example of such simulation is described. The proposed methodology provides an assessment of the damage prevention from a cyber-attack. The amount of the damage prevention from a cyber-attack is taken as a basic indicator for calculating the economic effect of investing in information security tools (IST). The performed simulation modelling allowed taking into account the relative uncertainty of the real situation with IS of OBI. The conducted study will help practitioners in the field of IS to obtain informed decisions to increase the efficiency of investment projects in the field of IS for OBI, using the approach outlined in the study. Unlike the existing ones, the proposed methodology takes into account both direct and indirect factors of investment projects in the field of IS of OBI. The obtained research results make it possible to expand the tools of information security analysts in the synthesis and analysis of information security contours of objects of informatization of any scale.

Keywords: *Information Security, Information Protection, Uncertainty, Investment Process, Methodology, Damage Prevention*

1. INTRODUCTION

According to the generally accepted point of view, typical for most specialists in the information security (IS) field, the opinion was formed that investing in IS and its concept for a particular object of informatization (OBI) will be effective if the requirements of state regulations and standards are met. This point of view was formed on the basis of the absence of a unified generally accepted methodology for assessing the economic effect of investing in IS of OBI [1, 2]. It should be noted that in this context of the problem of assessing the effectiveness of investment in IS of OBI we understand the excess value of the final result of the corresponding measures over the total amount of investments, i.e. the total cost of financial resources for IS of OBI during a fixed period of time [3].

The complexity of assessing the real effect of investing in IS of OBI is explained by a fairly large list of factors specific to the information protection and cybersecurity sector. Without going into their detailed analysis, we note only a significant impact on the efficiency of investing in IS of OBI of such factors as 1) the constantly changing landscape of cyber threats; 2) different strategies and tactics of the attacking side (computer intruders); 3) the rapid development of technical tools of information security (IST) and cybersecurity (CS), etc. In turn, in accordance with the basic postulates of the theory of evaluating the effectiveness of systems, it is known that the quality of the information security tools (hereinafter IST) can only manifest itself in the course of their real targeted use for OBI. It is this circumstance that makes it possible to objectively assess the effectiveness of their application, and, consequently, the effectiveness of investments in the IST for OBI [4,5].

An additional difficulty of assessing the effectiveness of investing in IS of OBI is associated with the uncertainty of the results of the functioning of IS. Uncertainty factors are present already at the design stage of IST. For example, related to the fact that a situation may arise in which the side of OBI's defense will spend hundreds of thousands of dollars or even millions to defend against sophisticated targeted cyber-attacks, and the attacker often only needs to resort to low costs ("investment in a cyber-attack") and apply social engineering methods. Such tactics of applying social engineering methods in a number of cases helped to bypass the most modern IST [6]. Thus, the level of functionality of IST may decrease with the implementation of projects in IS field. Consequently, from the point of view of the methodology for modelling the effectiveness of investing in IS, a number of functional metrics of the IST cannot be identically expressed and described by deterministic indicators.

The procedures that provide testing and certification of the components of the IST do not fully eliminate the uncertainties of the properties of the protection system. These procedures cannot anticipate future attack scenarios and attacker tactics. Thus, the probabilistic parameters of the information security system can reasonably be considered as an objective qualitative characteristic of the IST, as well as its adaptability to the required level of IS in the face of an increase in the number and complexity of the destructive influences of computer intruders in the information and telecommunication infrastructure of OBI. The latter include parameters that characterize, for example, the degree of possibility to achieve the defined IS goals of a particular measure of protecting information under given conditions. It is this probabilistic parameter that should form the basis of a complex indicator (criterion) for assessing the effectiveness of the analyzed IS tool. In this case, as subcriteria, one can take the suitability of a certain IS tool and its optimality for a specific problem to be solved.

In the context of problem solving, by the suitability of IS tool we mean its ability, together with other tools (both hardware and software), to fulfill all the requirements set in IST. And in this case, optimality can be interpreted as a sign of the ability of IS tool to achieve extreme values in its work complying with a number of restrictions.

To solve a multicriteria task is a common practice in the process of synthesizing IS systems due to the need to compare different architectures of IST circuits. As an example, a centralized scheme for constructing the contours of IS or a decentralized one can be cited. When solving multicriteria optimization problems with regard to the choice of IST for distributed computing systems, there is inevitably need to analyze the efficiency indicator of a separate tool of IS as well as their sets. Actually, such sets of hardware and software tools of IS, organizational and other measures form complex information security systems. Such sets of IST can also be described using the probabilistic-temporal characteristics of the distribution functions. The latter, in particular, include the probabilistic indicators of the ability of attackers to overcome the contours of IST of OBI within a certain period of time.

The abovementioned arguments allow asserting that it is most expedient to use probabilistic methods in the process of assessing the effectiveness of the functioning of IST. In accordance with these methods, the guaranteed level of IS, acceptable for the defense side, will be transformed into the confidence probabilities of the corresponding information protection metrics and CS of OBI.

It should be noted that in the course of multi-criteria optimization of IST, the level of IS guarantees is also assessed depending on the features of OBI (for example, a bank, an industrial enterprise, commercial sector or educational, etc.). And this level depends to a fairly large extent on the size of the potentially damage prevention to the information arrays of OBI. In this case, a new problem arises related to obtaining a numerical risk assessment for OBI. That is, the defense side needs to have an idea of the distribution of random damage values in the event of an attack. In such a situation, the simulation methods are traditionally used. As an alternative approach, the results of an active IS audit are also applied (or IST) for the analyzed OBI.

2. THE AIM OF THE ARTICLE

The aim is to develop a methodology for calculating indicators from investments in information security systems of an informatization object.

To achieve the aim the following tasks are solved:

enhancement of the methodology for calculating indicators from investment measures as part of increasing the IS metrics of OBI based on the basic indicator – the amount of damage prevention from a cyber-attack;

execution of simulation modelling for a specific example of calculating the efficiency of investing in IS of OBI, taking into account both direct and indirect factors of investment projects in the field of IS of OBI.

3. LITERATURE REVIEW

In studies [7, 8] it was shown that cognitive models allow analyzing IST of OBI as a whole. The authors select a set of measures to improve IST in their models. Besides, it is possible to determine the direction of the necessary impacts on IS situation. The authors have also considered the procedure for choosing IS metrics that are able to characterize the evolving situation in the future. According to the authors [8, 9], the advantage of cognitive modeling is the ability to take into account not only qualitative, but also quantitative indicators of IST. Only scenario forecasts of the evolving situation can be noted as a disadvantage of this approach.

In [10] the authors in the course of modelling considered the time factor in the process of investing in IS of OBI. The defense tactics, which the authors call “wait-and-see”, are analyzed. Namely, the defense side should limit the excessive investment of funds in IST and IS (or in the author’s terminology of CS), based on the result already achieved. The undoubted advantage of this approach is the ability to take into account the uncertainty of the onset of the moment in time when, based on the available data on the attack, it is possible to flexibly increase (or decrease) the size of investment funds in IST to mitigate the consequences of the attack. In our opinion, this approach is not devoid of subjectivity. Indeed, according to the authors [10], the only way to obtain information about the attack is to record the fact of the attack. Only after that, the defense side should react and allocate a financial resource (hereinafter FR) for IS of OBI. The disadvantage of this approach is that it is based on a discrete attack time structure. And this leads to the need to re-carry out calculations in the event of a change of the situation and IS metrics of OBI.

In [11] reveal that traditional methods of evaluating investment projects, as a rule, underestimate their cost.

The authors [12] propose a model in which the required investment threshold is considered, taking into account the uncertainty of the situation in the course of investment. However, this approach has not received further development.

In [13] the authors proposed a model for consistent investment in new technologies. The difference of the model is that the authors take into account the possibility of consistent investment in new technologies. For example, a company may use existing technology with the expectation that the new technology will become more available in the market. The factor of technological uncertainty for the application of the new technology is not considered in detail by the authors. That, accordingly, in general, can affect the final profit from innovations, including in IS field.

In [14] the authors investigate the parameters of the optimal timing of the introduction of new technologies. An approach based on the Poisson process is taken as a basis. However, it should be noted that the authors do not take into account the price uncertainty, and this can play a crucial role in the information technology and technology of IST market.

A distinctive approach to modelling technological uncertainty in the implementation of innovations is described in [15]. The authors analyze a situation, where a company may face price and technological uncertainty when investing. The advantage of the described approach is the ability to take into account the compensation for the monopoly profit that the market leader will receive. The disadvantages of this approach include the lack of accounting for investment time parameters. And this situation is not typical for IS field.

In articles [10, 16] the problem of investing in cybersecurity is considered for the case when counterparties can exchange information, for example, regarding identified vulnerabilities in their information systems (IS). The authors have shown that such data exchange helps to reduce the level of uncertainty relating to potential risks. This, in turn, contributes to the optimization of investment terms. The authors themselves pointed out certain limitations imposed on the model. One of the main limitations is the assumption of risk reduction only due to the situation of extensive information exchange between counterparties. The model does not allow the investor to find the optimal investment strategy, since the model is only a formalized description of the investment process in CS of OBI.

In [17] the author summarizes the approaches of the implementation of the investment process in CS. The paper considers a five-stage methodology for decision support for CS of OBI. Since the methodology is quite voluminous, its implementation in practice will become quite laborious without appropriate computer decision making support, which reduces the practical value of the described approach.

In [18] the authors presented an original empirical model for choosing the optimal strategy for investing in IS. The model is based on Bayesian statistics, and takes into account specific CS mechanisms. In the study, an example of taking into account the rapidly developing technologies of intrusion detection systems (IDS) in the investment process is considered. The approach proposed in [18] was developed in papers [19, 20]. So the authors in new studies took into account the optimal investment terms. And besides, the improved model allows taking into account the capabilities of improving the characteristics of IDS based on their Bayesian training. According to the authors, the most acceptable strategy for investing in IS should be a phased strategy for investing funds in IS of OBI, if new threats and vulnerabilities are identified. The study [18] also considers the option, when investment is carried out in interrelated investment projects.

In [21] a model is proposed that considers the inflexibility of a number of investment projects. In some situations, this may be inherent to the selection of strategies for investing in IS of OBI. The model is focused on studying the profitability of using current technologies and is able to predict the situation, when it is advisable for a company to switch to a more advanced technology. The authors applied traditional dynamic programming methods to calculate the cost of an investment. It should be noted that the use of dynamic programming imposes restrictions due to the impossibility of solving the multidimensional problem of investing in IS of OBI.

In [22] the author proposes a model that takes into account the increase in the efficiency of investments in CS. The model considers a decrease in uncertainty from the expected loss as a result of an attack and a general decrease in the security level of OBI. However, as the author admits, the model has a limitation. This is due to the fact that the availability of measures to reduce potential damage as a result of an attack directly depends on technological innovations in CS field. And these innovations can happen at random moments. Accordingly, this stochastic influence on CS of OBI can ultimately reduce the investment effect and increase the risks for the investor.

In [23, 24] there have been examined models of the investment process in IS based on the solution of a system of bilinear differential equations. The models are focused only on the economic aspects of investing in IS and do not take into account technological approaches to ensuring the information protection and CS of OBI.

Thus, the performed analysis of publications on the study topic shows that at the moment there are no unified approaches to the issue of assessing the effectiveness of measures aimed at ensuring IS of OBI in conditions of uncertainty. At the moment, there is no unified generally accepted model that allows assessing the dynamic characteristics of investment projects in the field of IS of OBI. Such a model should consider both traditional financial and technological, temporary, organizational and other parameters of the investment project.

Summarizing the abovementioned, we can state that:

1) the effectiveness of measures aimed at increasing the degree of protection and IS of OBI cannot be given only on the basis of deterministic assessments;

2) the effectiveness of measures aimed at increasing the protection of OBI and improving its IS requires the use of probabilistic characteristics. These include, in particular, the distribution function of indicators of the damage prevention as a result of destructive actions of malefactors for OBI.

4. MODELS AND METHODS

In the process of calculating the economic efficiency from investments in IS of OBI, generally, the following two variables are used. Accordingly, the result obtained during the implementation of IS tools and measures, reduced to a monetary indicator. And the corresponding costs of the implemented tools and measures of IS.

The actual end result of the introduction of IS measures can be considered the amount (in monetary terms) of the prevented losses (damage prevention from cyber-attacks). This parameter can be formalized like this:

$$D_i = D_i^{'} - D_i^{''}, \tag{1}$$

where $D_i^{'}, D_i^{''}$ – attacks damage, respectively, before and after the implementation of IS tools and measures.

In fact, the amount of the damage prevention from cyber-attacks reflects the share of the profit that was not received if the IS tools and measures corresponding to the threats are not implemented.

Then the total amount of the damage prevention from cyber-attacks is defined as follows:

$$P = \sum_{i=1}^{n} P_i + R_i, \tag{2}$$

where R_i – the amount of directly returned financial resources. Such resources can include, for example, funds that are used as penalties against employees who have violated the company's IS policy, etc.

As practice shows [14, 16], it is rather difficult to determine the real amount of damage prevention from cyber-attacks. To do this, it is necessary to have real statistics on cyber-incidents, and in addition, in several situations, it is necessary to involve information security experts. It should be noted that the involvement of experts inevitably introduces subjectivity into the assessment of the amount of the damage prevention. And while expert methods are increasingly being replaced by the widespread use of intelligent DSS in the tasks of assessing damage and risks from attacks, the combination of the above two approaches in the decision-making process can be considered the most expedient.

Using such a combined approach assumes the following sequence of actions to simulate (for example, simulate) the size of the damage prevention of cyber-attacks:

Step 1. Divide potential damage (losses) into groups. As a criterion for such a division, it is possible to apply the categorical division of IS incidents according to the degree of danger to OBI, using typical IS metrics;

Step 2. Based on the available statistics of cyber-incidents regarding OBI and using DSS or experts, we estimate the value of the amount of losses (damage prevention) for each incident. This value can vary from: minimum (min) to and maximum (max) values. A similar step is performed both before and after the implementation of measures to strengthen IS of OBI;

Step 3. Using the preselected distribution law, model the values of losses (before and after the implementation of IS tools and measures);

Step 4. Calculate the total value of the damage prevention of cyber-attacks based on the previous steps 1-3;

Step 5. Calculate the statistical characteristics for the simulated values, as well as the resulting indicators of the economic efficiency of the implemented tools and measures taken to strengthen IS of OBI.

To visualize the result of the calculation, it is advisable to construct a histogram of the distribution of the resulting value of the damage prevention from cyber-attacks. Or a histogram of the cumulative percentage of the distribution of the damage prevention of cyber-attacks.

Accurate selection of the distribution law of the total resulting value of the damage prevention from cyber-attacks will permit fairly accurately assessment of the probabilistic characteristics at any place in the histogram or in relation to the analyzed interval.

Thus, the probabilistic characteristic of the damage prevention from cyber-attacks can be taken as a reasonable criterion for the effectiveness of measures aimed at increasing IS of OBI.

A more time-consuming task is to determine the specific size of the cost of providing IS of OBI. Such costs include the following items:

maintenance of IS department of OBI;

purchase, operation, repair costs, etc. hardware and software IST;

and etc.

In addition, when calculating the effectiveness of investing in IS OBI, it is crucial to take into account the importance of information assets in the company's business processes. You can calculate this parameter by applying the following dependence [25]:

$$S_j = {}^{C}\!/_{Y}, \quad (3)$$

где S_j – the importance of the j - th information asset in the company's business processes;

C – value of the j - th information asset;

Y – the amount of capital invested in the operation of j -th information asset

When it comes to assessing the effectiveness or other information security information, one should take into account such a category of parameters as the risks of violation of information security OBI. The risk can be single, subjective, cumulative [25].

Accordingly, each of these types of risk can be calculated as follows:

Single risk (R_i):

$$R_i = p_i \cdot d_i, \quad (4)$$

где p_i – the probability that an attacker realizes a threat against IS of OBI;

d_i – damage of i -th threat against IS of OBI;

Subjective risk (R_{sub}):

$$R_{sub} = {}^{N_R}\!/_{Y}, \quad (5)$$

где N_R – the total number of all risks;

Y – number of actual risks;

Aggregate risk (Q):

$$Q = \sum_{i=1}^{n} R_i + R_{sub}, \quad (6)$$

где n – total number of cyber threats against IS of OBI.

As the analysis of a number of publications [26-28] shows, most of the researchers are focused on assessing the risks of IS violation by local features. If we summarize the publication data (see Table 1), then we can notice that such models are mainly used: Cost Benefit Analysis - CBA, Net Present Value - NPV, Profitability Index - PI, Internal Rate of Return - IRR and others [28].

Currently, the following models are most popular for estimating the IS cost: NPV (Net Present Value) и DCF (Discounted Cash Flow). Without going into a detailed analysis of the advantages and disadvantages of each of these and other methods and models (a lot of publications are devoted to this issue, for example, [28, 29]), we note that many models themselves are focused only on the economic aspect of evaluating efficiency. However, in the context of the tasks solved in this article, we note that the following issues remain controversial:

1) what expenses should be specifically attributed to IS? Currently, there are no generally accepted criteria:

2) today IS has become an integral part of almost all business processes of companies. Consequently, many components of information security and cybersecurity (for example, the cost of network technologies and distributed computing systems of OBI) have become an integral part of the business processes of companies. This raises a new question. What part of investments in the development of IT companies is directed specifically at IS? And, for example, not to network or other IT companies? As a result, an erroneous opinion on these issues can give an incorrect picture of the share of investments in IS. They are only a fraction of a company's total IT investment;

3) focusing only on the amount of investment in IS of OBI is not correct. Indeed, closer attention to this issue will immediately show that it is impossible to discard many components of the complex of measures aimed at increasing the level of IS of OBI. For example, this expense item may include training for IS specialists, as well as advanced training on IS for all employees of the company.

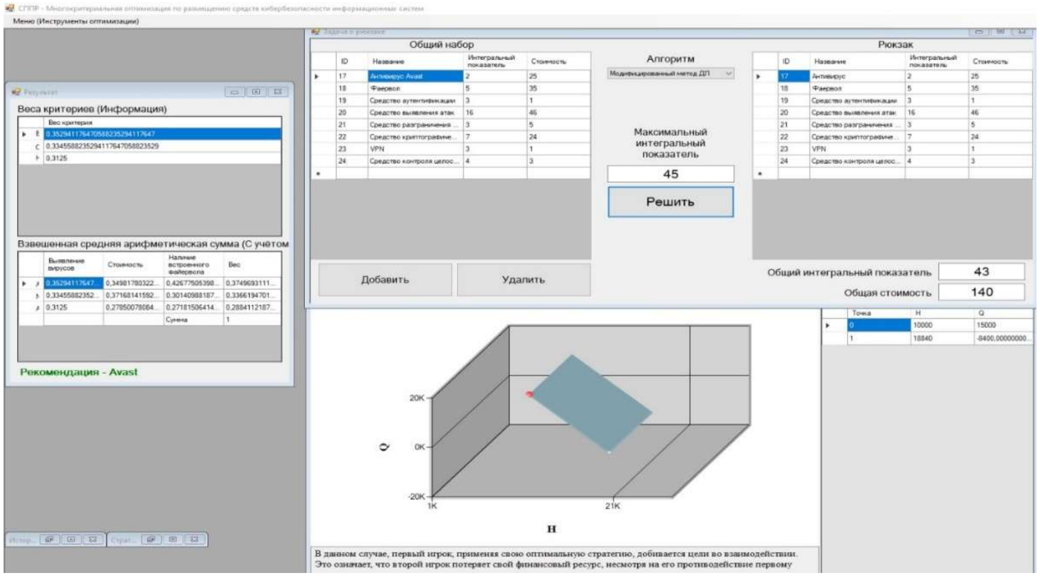
In our opinion, the methodology, outlined above, for assessing the damage prevention from cyber-attacks based on the basic indicator of calculating the economic effect of investing in IST will eliminate the inconsistency in assessing the effectiveness of measures aimed at ensuring IS of OBI.

The results obtained on the basis of the implementation of steps 1-5 can be used in conjunction with any of the methods (CBA, NPV, PI, IRR, etc.). Such a combined approach will allow owners of the company's information resources (OBI) with a guaranteed probability to receive various scenarios (from pessimistic to optimistic) of the results of investing in IS of OBI. In this case, the main computational work can be transferred to intelligent information systems, for example, DSS, see Fig. 1.

The block diagram of the functioning algorithm of the subsystem "Assessment of the effectiveness of measures aimed at ensuring IS of OBI" is shown in Fig. 2.

Table 1 – Models for Estimating the Cost of IS of OBI

№	Model	Advantages	Disadvantages
1	DCF	1. An integrated approach to assessing the cost of IS. 2. Considering all stages of the life cycle of the components of IST, as well as the business processes of the company.	The model is static. Possible changes in the information security situation were not taken into account, for example, during a long-term attack.
2	PI	1.Good correlation of the model with typical accounting methods. 2.Ease and speed of obtaining the results of evaluating investment in IS.	1.Inflation is not taken into account. 2.Non-additivity
3	NPV	1.Ability to consider different costs of resources to increase the degree of IS of OBI. 2.The position and interests of the investor were taken into account.	1.Part of the resources cannot be estimated in monetary terms. 2.Linking the model to the company's value indicators.



СППР - Многокритериальная оптимизация по размещению средств кибербезопасности информационных систем

Меню (Инструменты оптимизации)

Результат

Веса критериев (Информация)

	Вес критерия
E	0,352941176470588235294117647
C	0,3345588235294117647058823529
F	0,3125

Взвешенная средняя арифметическая сумма (С учетом

Выявление вирусов	Стоимость	Наличие встроенного файервола	Вес
0,35294117647...	0,34981780322...	0,42677505398...	0,3749693111...
0,33455882352...	0,37168141592...	0,30140988187...	0,3366194701...
0,3125	0,27850078084...	0,27181506414...	0,2884112187...
		Сумма	1

Рекомендация - Avast

Задача о рюкзаке

Общий набор

ID	Название	Интегральный показатель	Стоимость
17	Антивирус Avast	2	25
18	Фаервол	5	35
19	Средство аутентификации	3	1
20	Средство выявления атак	16	46
21	Средство разграничения ...	3	5
22	Средство криптографиче...	7	24
23	VPN	3	1
24	Средство контроля целос...	4	3

Алгоритм: Модифицированный метод ДП

Максимальный интегральный показатель: 45

Рюкзак

ID	Название	Интегральный показатель	Стоимость
17	Антивирус	2	25
18	Фаервол	5	35
19	Средство аутентификации	3	1
20	Средство выявления атак	16	46
21	Средство разграничения ...	3	5
22	Средство криптографиче...	7	24
23	VPN	3	1
24	Средство контроля целос...	4	3

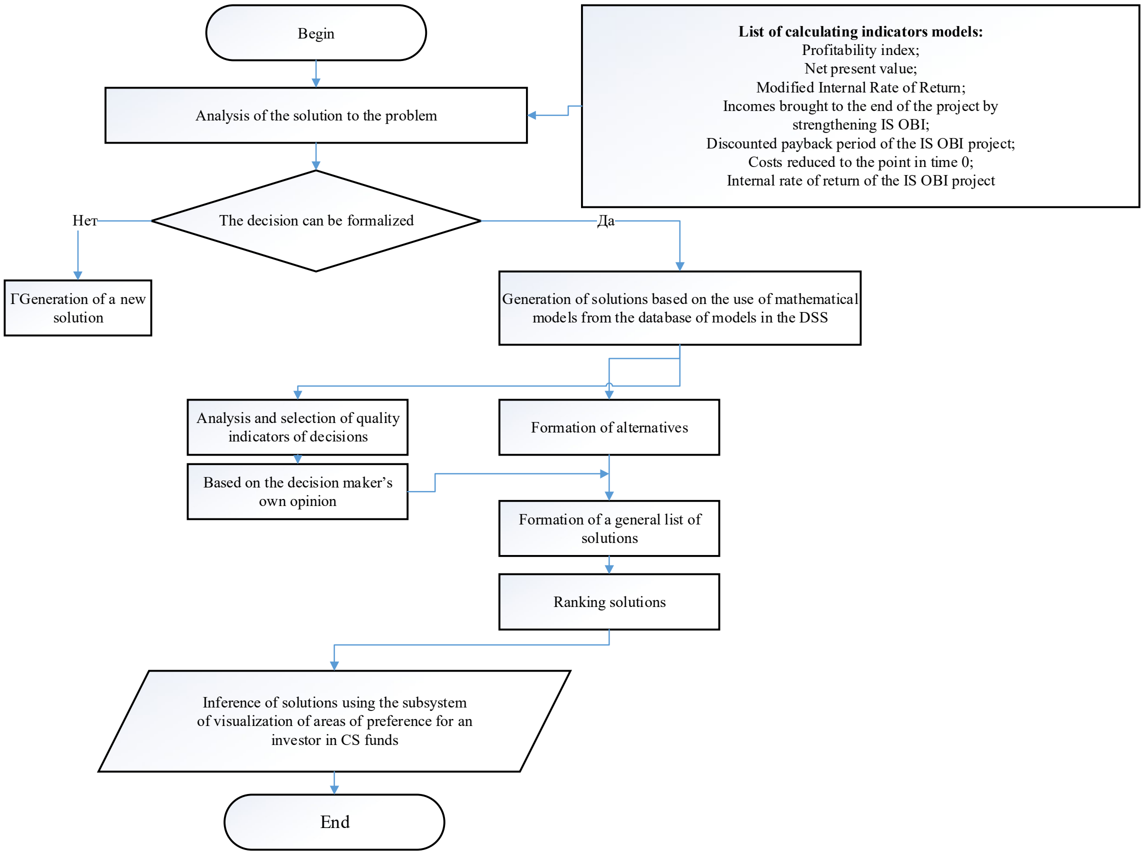
Общий интегральный показатель: 43

Общая стоимость: 140

Точка	H	Q
0	10000	15000
1	18840	-8400,00000000...

В данном случае, первый игрок, применяя свою оптимальную стратегию, добивается цели во взаимодействии. Это означает, что второй игрок потеряет свой финансовый ресурс, несмотря на его противодействие первому

Figure 1 – General View of the Interface of an Intelligent System for Assessing the Effectiveness of Measures Aimed at Ensuring IS of OBI



Begin
Analysis of the solution to the problem
List of calculating indicators models:
Profitability index;
Net present value;
Modified Internal Rate of Return;
Incomes brought to the end of the project by strengthening IS OBI;
Discounted payback period of the IS OBI project;
Costs reduced to the point in time 0;
Internal rate of return of the IS OBI project
The decision can be formalized
Нет
Да
ГGeneration of a new solution
Generation of solutions based on the use of mathematical models from the database of models in the DSS
Analysis and selection of quality indicators of decisions
Formation of alternatives
Based on the decision maker's own opinion
Formation of a general list of solutions
Ranking solutions
Inference of solutions using the subsystem of visualization of areas of preference for an investor in CS funds
End

Figure 2 – Block Diagram of the Operation Algorithm of the DSS Subsystem "Assessment of the Effectiveness of Measures Aimed at Ensuring IS of OBI"

Consider an example of a variant of assessing the effectiveness of measures aimed at ensuring IS of OBI.

Suppose there is a project to increase the degree of IS of OBI. In a test case, the project may include the following activities, see Table 2.

To calculate the indicators of net present value (NPV), profitability index (PI), internal rate of return (IRR), modified internal rate of return (MIRR), discounted payback period of the project (DPB), we will use the formulas given in [4], as well as formulas (1) - (6) in the article. It is necessary to obtain results for three scenario outcomes of the calculation in order to make a justified decision about the feasibility of investing in IS projects.

Table 2 – Expenditures and Possible Revenues of Funds as a Result of Implementation of Measures Taken to Increase IS of OBI

Measures to increase the level of IS of OBI	Expenditures, thousand USD	Revenues, thousand USD			
		Designation	Min (minimal)	Mid (Most likely)	Max (Maximum)
M1 (technical, such as purchasing a new firewall)	65	P1	160	270	420
M2 (organizational, for example, trainings for employees of the information security department)	35	P2	90	170	300
M3 (others)	20	P3	50	100	190
Amount	**120**		**300**	**540**	**910**

Initially, it is necessary to model the volumes of potential revenues as a result of the implementation of the IST and the corresponding measures. In fact, these indicators will correspond to the amount of the damage prevention from cyber-attacks.

The results of potential revenues are visualized in the DSS in the form of a histogram characterizing the final distribution of funds from activities M1 – M3, see Fig. 3.

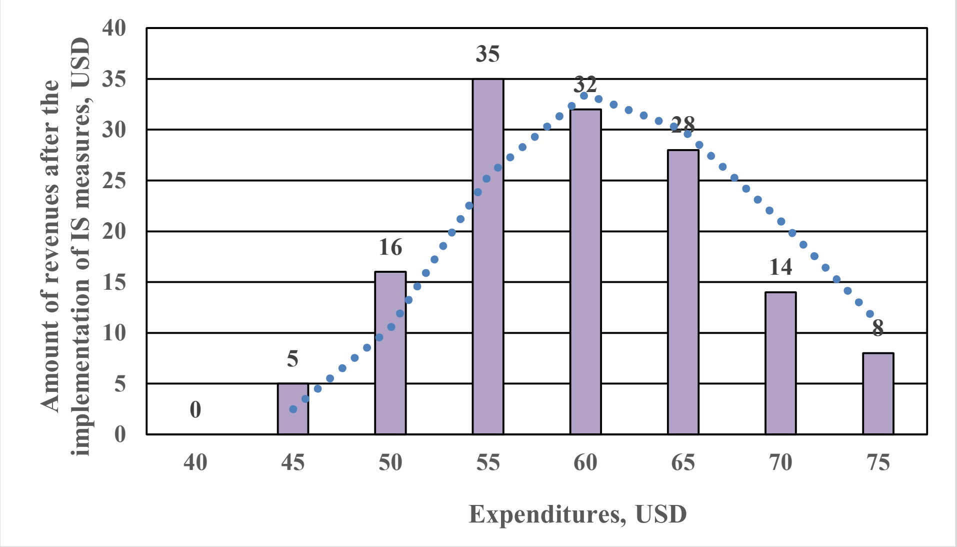


Figure 3 – The Total and Average Distribution of Possible Revenues from the Implementation of Measures (M1-M3) Taken to Increase IS of OBI

Descriptive statistics of the final distribution of the amount of damage prevention from cyber-attacks will be presented in tabular form. For example, as it is shown in Table 3.

The simulation results for various scenarios of the investment process in IS of OBI for the test case are set in Table 4.

At the final stage of testing, for each of the scenarios, we determine the performance indicators of the project of IS improvement. The results are summarized in Table 5.

Analysis of the calculation results allowed us to make such a conclusion (for the given initial data). All scenarios, except for the pessimistic one, satisfy the conditions for approval by the company's management of the project for investing in IST and measures aimed at increasing the level of it's IS.

Table 3 – The Results of Calculating Descriptive Statistics for the Revenues as a Result of the Measures Taken to Increase IS of OBI

Indicator	**Designation**	**Signification**
Mean	μ	33,9
Standard error	δ	0,74
Standard deviation	σ	7,4
Sample variance	Ω	470,2
Min signification	*Min*	5
Max signification	*Max*	35,1

Table 4 – Assessment of the Effectiveness of Projects to Improve IS of OBI for Different Scenarios

Scenarios	**Symbol**	**Revenues for the period, thousand USD**
Pessimistic	S_{pes}	31
More probable	S_{mp}	45
Optimistic	S_{op}	62

Table 5 – Indicators of the effectiveness of an IT project by scenarios

The indicator of the effectiveness of the investment project in IS of OBI	**Parameter identification**	**Scenario variant**		
		S_{pes}	S_{mp}	S_{op}
Profitability index	*PI*	0,85	1,2	1,11
Net present value	*NPV*	9,2	27,0	13,3
Modified Internal Rate of Return	*MIIR*	0,12	0,18	0,17
Revenues reduced by the end of the project to strengthen IS of OBI	*FPI*	189,0	196,0	161,3
Discounted payback period of the IS of OBI project	*DPB*	3,7	2,4	1,79
Expenditures adjusted to point in time $t = 0$	*PVO*	120	120	120
Internal rate of return of the IS of OBI project	*IIR* *IIR*	0,14	0,22	0,18

In order for the company's management to make a final decision on the feasibility of investing in IS, it is necessary to determine the proximity of each of the considered scenarios to a hypothetical perfect project. This can be done using, for example, metrics such as Euclidean distance or Pearson correlation. In this case, it is necessary to normalize the indicator of net present value (NPV) for the corresponding scenario. The standardization must be carried out in relation to the maximum value. An investment project in IS can be considered perfect if the scenario corresponds to such indicators: $NPV = 2; PI = 2; MIRR = 1$.

It should be noted that today, in the face of complicating scenarios for carrying out cyber-attacks against companies, their management (decision-makers – DM) are aware of the need to search for adequate answers to the growth of cyber threats. However, in practice, it is not uncommon for a company and its management to be constrained by the size of the investment funds that they are willing to invest in increasing the level of IS. This is partly due to the fact that the increase in the company's profits as a result of an increase in IS level is not as obvious as, for example, investing in new production assets or marketing. Therefore, all the advantages of investing in IS of OBI can be shown only by supporting verbal and logical arguments with the results of calculations and modeling. The emphasis on the return on investment in IS of the company should be done after having obtained data from model studies and having convincing statistics on CS incidents that could be (or have already) resulted in financial, reputational and other losses for the company.

5. ACKNOWLEDGEMENTS

The study was carried out as part of a grant research AP08855887-OT-20 "Development of an intelligent decision support system in the process of investing in cyber security systems".

6. CONCLUSIONS

The following main results were obtained in the study:

the analysis of publications on the problems of assessing investments in information security (IS) of objects of t (OBI) has been carried out. The possibility and necessity of obtaining the necessary data has been substantiated, contributing to a reliable assessment of the effectiveness of measures aimed at increasing the information security (IS) of the company;

proposed a methodology for calculating indicators from investment activities in the framework of increasing the metrics of IS of OBI. A specific example of simulation is described. The proposed methodology provides an assessment of the damage prevention from a cyber-attack. The amount of the damage prevention from a cyber-attack is taken as a basic indicator for calculating the economic effect of investing in IST;

simulation modelling was carried out for a specific example of calculating the effectiveness of investment in IS of OBI. It allowed considering the relative uncertainty of the real situation with IS of OBI. It was shown that the conducted studies would help practitioners in IS field to obtain, using the approach outlined in the paper, justified decisions to increase the efficiency of investment projects in the IS field of OBI. Unlike the existing ones, the proposed methodology took into account both direct and indirect factors of investment projects in the field of IS of OBI.

REFERENCES:

[1] Pieters, W., Probst, C. W., Lukszo, Z., & Montoya, L. (2014). Cost-effectiveness of security measures: A model-based framework. In Approaches and processes for managing the economics of information systems (pp. 139-156). IGI global.

[2] Brangetto, P., & Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex, 1(9-16), 86.

[3] Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. Procedia computer science, 149, 65-70.

[4] Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. IEEE Access, 6, 12175-12186.

[5] Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., Slayback, S. M., & San Miguel, J. M. (2021). Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. International Journal of Organizational and Collective Intelligence (IJOCI), 11(2), 91-112.

[6] Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. European Journal of Operational Research, 260(2), 588-600.

[7] Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. Frontiers in psychology, 9, 691.

[8] Gonzalez, C., Ben-Asher, N., & Morrison, D. (2017). Dynamics of decision making in cyber defense: Using multi-agent cognitive modeling to understand cyberwar. In Theory and Models for Cyber Situation Awareness (pp. 113-127). Springer, Cham.

[9] Maqbool, Z., Pammi, V. C., & Dutt, V. (2019). Behavioral Cybersecurity: Investigating the influence of Patching Vulnerabilities in Markov Security Games via Cognitive Modeling. IJCSA, 4(1), 185-209.

[10] Gordon, L., Loeb, M., Lucyshyn, W. Information security expenditures and real options: A wait-and-see approach, Computer Security Journal, vol. 19, no. 2, pp. 1-7, 2003.

[11] Majd, S, Pindyck, R. Time to build, option value, and investment decisions, Journal of Financial Economics, vol. 18, no. 1, pp. 7-27, 1987.

[12] Malchow-Muller, N., Thorsen, B. Repeated real options: Optimal investment behaviour and a good rule of thumb, Journal of Economic Dynamics and Control, vol. 29, no. 6, pp. 1025-1041, 2005.

[13] Grenadier, S., Weiss, A. Investment in technological innovations: An option pricing approach, Journal of Financial Economics, vol. 44, no. 3, pp. 397-416, 1997.

[14] Farzin, H., Huisman, K., Kort, P. Optimal timing of technology adoption, Journal of Economic Dynamics and Control, vol. 22, no. 5, pp. 779-799, 1998.

[15] Huisman, K., Kort, P., Strategic technology adoption taking into account future technological improvements: A real options approach", European Journal of Operational Research, vol. 159, no. 3, pp. 705-728, 2004.

[16] Gordon, L., Loeb, M., Lucyshyn, W., Zhou, L. The impact of information sharing on cybersecurity underinvestment: A real options perspective", Journal of Accounting and Public Policy, vol. 34, no. 5, pp. 509-519, 2015.

[17] Daneva, M. Applying real options thinking to information security in networked organizations, Centre for Telematics and Information Technology, University of Twente, Tech. Rep., 2006. pp. 1-12.

[18] Herath, H., Herath, T. Investments in information security: A real options perspective with Bayesian postaudit," Journal of Management Information Systems, vol. 25, no. 3, pp. 337-375, 2008.

[19] Benaroch, M., Shah, S., Jeffery, M. On the valuation of multistage information technology investments embedding nested real options", Journal of Management Information Systems, vol. 23, no. 1, pp. 239- 261, 2006.

[20] Herath, H., Park, C. Multi-stage capital investment opportunities as compound real options, The Engineering Economist, vol. 47, no. 1, pp. 1-27, 2002.

[21] Khansa, L., Liginlal, D. Valuing the flexibility of investing in security process innovations", European Journal of Operational Research, vol. 192, no. 1, pp. 216-235, 2009.

[22] Benaroch, M. (2018). Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. Information Systems Research, 29(2), pp. 315-340.

[23] Lakhno, V., Malyukov, V., Gerasymchuk, N., & Shtuler, I. (2017). Development of the decision making support system to control a procedure of financial investment. Eastern-European Journal of Enterprise Technologies, (6 (3)), 35-41. (2017) DOI: 10.15587/1729-4061.2017.119259

[24] 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, (3), pp. 6-14.

[25] Chudin, A.V. (2018). Methods for evaluating the effectiveness of IT at the operational stage. IT consulting and innovative software development, (3), 12-15.

[26] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & security, 57, 14-30.

[27] Behnia, A., Abd Rashid, R., & Chaudhry, J. A. (2012). A survey of information security risk analysis methods. SmartCR, 2(1), 79-94.

[28] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & security, 56, 1-27.

[29] Wangen, G. (2017). Information security risk assessment: a method comparison. Computer, 50(4), 52-61.