UDC 004.56.53
DOI: 10.15587/2706-5448.2025.340229

Yurii Kopytin,
Maryna Kopytina,
Volodymyr Korchynskyi

DEVELOPMENT OF AN OPTIMAL OPTIONS-FORMING METHOD FOR INFORMATION SECURITY RISK TREATMENT BASED ON QUANTITATIVE ASSESSMENT MODELS

The object of the research is the processes of forming optimal options for information security risk treatment of the organization. One of the most problematic areas is the choice of means and measures of protection from the set of available options for information security risk treatment that will allow reducing information security risks in a way that is not detrimental to the organization. The available models and methods are cumbersome, which makes their practical use impossible, and also do not take into account the economic features of implementing means and measures of protection.

The research used methods of investment theory, which allowed it to assess the effectiveness of reducing information security risks due to the implementation of a set of means and/or measures of information protection, and the ABC analysis method, which allowed it to identify the most effective ones among them by dividing them into groups. This approach simplified the process of assessing information security risks and choosing the optimal set of means and measures of protection. The proposed method involves calculating the indicators of net present value and payback period of the project, which allows the owner of the organization to assess the economic efficiency of implementing a set of means and measures of protection, as well as to understand when the costs of the information protection system will pay off.

The obtained method, that significantly simplified the process of reducing information security risks at a break-even price. This is due to the fact that the proposed method has a number of features in the formation of options for information security risk treatment, particularly. It involves assessing the effectiveness of the implementation of each of the means and/or measures of protection and ranking them by effectiveness by dividing them into groups. This enables the creation of a risk-oriented information security system. Compared to similar known models and methods, this enables a simplified procedure for information security risk treatment in practice.

Keywords: *risk analysis, risk treatment, risk management, information security, economic efficiency, ABC analysis.*

Received: 12.07.2025
Received in revised form: 03.09.2025
Accepted: 27.09.2025
Published: 30.10.2025

How to cite
Kopytin, Y., Kopytina, M., Korchynskyi, V. (2025). Development of an optimal options-forming method for information security risk treatment based on quantitative assessment models. Technology Audit and Production Reserves, 5 (2 (85)), 47–55. https://doi.org/10.15587/2706-5448.2025.340229

1. Introduction

Information security risk management is an integral component that ensures the proper function of any organization. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 [1] states that EU countries should ensure that important entities take necessary and reasonable technical, organizational and operational measures. These measures are necessary to manage the risks to the security of the networks and information systems they use in their operations or to provide services.

Modern information protection systems are dynamic and are characterized by the emergence of information security risks from the implementation of new threats to the organization's assets. These force the building of an information security system based on a risk-oriented approach, which allows the use of economically justified means and measures of protection to counteract threats.

One of the key processes of information security risk management is risk treatment, which involves the implementation of sets of means and measures of protection against the impact of the threats set to the organization's assets.

Information security risk treatment can occur by avoidance, reduction, transfer or acceptance of the risk. For choosing the optimal option of information security risks treatment, it is necessary to conduct their assessment, which includes identification, analysis and evaluation.

Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 [2] issued by ENISA and the international standard ISO/IEC 27002:2023 [3] offer more than 100 recommendations for the implementation of measures and means of protection aimed at reducing information security risks. The means and measures of protection proposed in them are only a starting point for the formation of a risk-oriented information security system. Using these or other documents with recommendations, information security specialists have to implement a set of means and measures of protection and choose from hundreds of possible options the most relevant for the protection of the organization's information. Because of this, models and methods for assessing and evaluating information security risks, including the formation of options for their treatment, are essential in the daily work of information security specialists.

ISSN-L 2664-9969; E-ISSN 2706-5448

The number of international standards and the work of many authors are devoted to the issue of assessing and evaluating information security risks. Particularly, in [4] it is proposed to use scenario analysis, fault tree analysis, event tree analysis, Monte Carlo method, Delphi method, models based on probability theory, fuzzy set theory, graph theory, etc. for risk assessment and evaluation. These models are aimed at assessing and evaluating the acceptability of information security risks and when calculating information security risks, allow assessing the impact of threats on the organization's assets. These approaches are understandable for information security specialists, but they are not aimed at finding options for information security risk treatment by choosing the optimal set of means and measures of protection.

Various models and methods are used for optimization (e. g., multi-criteria optimization, heuristic methods, mathematical programming methods, etc.). In [5, 6], the ABC analysis method is used for the selection of optimal solutions in information security systems. The ABC analysis method involves classifying objects by degree of importance based on a certain indicator. In particular, in [5, 6], the frequency of threat occurrence is used as an indicator for ranking. This allows implementing means and measures of protection against threats that most often occur in organizations and thereby reduce the organization's information security risks. These publications do not take into account the cost of means and measures of protection and the amount of information security risk reduction from their implementation. In other words, the effectiveness of reducing information security risks by a set of means and measures of protection, which costs a certain price, is not taken into account. In addition, the works do not take into account investment indicators, particularly, it does not check whether the implementation of means and measures of protection is carried out at a cost that is not loss-making for the organization.

Certain scientific publications are devoted to the assessment of investments in information security systems. In particular, for assessing the economic effect of the implementation of information security systems in [7, 8], use such indicators and methods as: cost-benefit analysis, return of investments, net profit value, discount playback period, etc. These indicators allow assessing the economic effect of implementation of means and measures of protection from different angles, namely: they assess the percentage return on investment, the time it takes for the investment to pay off, the cost-benefit ratio, etc. Indicated indicators are calculated on the assumption that information security risks are static over a certain period of time. This does not take into account the fact that the information security system is a dynamic system that involves a constant change in the level of information security risks due to the emergence of new threats and methods of implementation. Accordingly, the ability to reduce the effectiveness of the implemented means and measures of protection, since measures and means of protection against the impact of new threats are implemented with a delay [9]. In other words, new threats appear for which means and measures of protection have not been implemented, and the level of the information security risks change accordingly after the implementation of these means and measures over time. This should be taken into account when assessing the effectiveness of investments in the information security system. In addition, existing models focus on the profits and costs received, rather than information security risks.

The scientific publications mentioned above separately address the issue of finding optimal means and measures of protection and the issue of assessing economic efficiency. However, there is still no method that takes these things into account in the complex and will be based on information security risks.

Thus, *the aim of research* is to develop a method for forming optimal options of information security risk treatment based on quantitative assessment models. These models should rely on economic methods and take into account the impact of threats on the organization's assets. This method should provide information security specialists with an understanding of the priority of implementing means and measures of protection.

To achieve this aim, the following objectives were accomplished:
– select models of economic theory that can be used in assessing the effectiveness of investments in the information security system;
– adapt the selected models of economic theory to the issue of forming an optimal set of means and measures of protection, taking into account that the information security system is a system with a delay;
– adapt the ABC-analysis method to the issue of forming an optimal set of means and measures of protection, taking into account the cost of means and measures of protection and the amount of information security risk reduction from their implementation;
– propose a sequence of actions for forming the optimal option for information security risk treatment, which is based on adapted selected models of economic theory and an adapted ABC analysis method;
– demonstrate using an example of the use of the proposed method for forming optimal options for information security risk treatment.

2. Materials and Methods

The object of research is the processes of forming optimal options for information security risk treatment of the organization.

The developed method of forming optimal options of information security risk treatment is based on the methods of economic theory, which allowed to assess the effectiveness of reducing information security risks as a result of the implementation of a set of means and/or measures of information protection, and the ABC analysis method, which allowed to identify the most effective ones among them by dividing them into groups. The proposed method involves calculating the indicators of net present value and the payback period of the project, which allows the owner of the organization to assess the economic efficiency of implementing a set of means and measures of protection, as well as to understand when the costs of the information protection system will pay off.

The following scientific methods were used in the research:
– a synthetic method for forming a holistic view of the features of implementing means and measures of protection, and the impact of their implementation on information security risks;
– an analogy method for demonstrating the economic effect of investments in implementing means and measures of protection;
– abstraction method to simplify the calculation of the net present value in terms of the implementation of means and measures of protection, the discount rate coefficient was excluded from the calculations;
– deduction method to highlight additional properties in the process of calculating the net present value of investments in the information security system;
– modeling method to identify and assess information security risks.

During the development of the model, made the following assumptions:
– the implementation of one means or measure of protection can provide protection against one or more threats to the organization's assets;
– the implementation of means and measures of protection should ensure the reduction of information security risks at a cost that is not detrimental to the organization;
– the implementation of means and measures of protection can occur both once and on a regular basis;
– the assessment of information security risk occurs at a certain point in time and assumes that the risk may regularly change with the emergence of new threats from which the implemented set of means and measures of protection is not able to protect the organization;
– the development and implementation of new means and measures of protection occurs with a delay, which can lead to a change in the level of losses;
– the optimal interval for reassessment of information security risks is an interval equal to one month.

3. Results and Discussion

3.1. Quantitative risk assessment models

Taking into account the above, the mathematical apparatus is described below, that forms the basis of the method proposed in this article for forming optimal options for information security risks treatment, which is based on quantitative assessment models. Investing money in the implementation of security measures and tools should have a certain economic effect. One of the tasks of creating a risk-oriented information security system is to find alternative options for implementing means and measures of protection. Implementing means and measures of protection is a kind of investment.

For investment projects, the assessment of the economic feasibility of investment can be carried out by calculating net present value *NPV*. The calculation of net present value *NPV* can be done using the following equation [10]

$$NPV = \sum_{i=1}^{n} \frac{CF_i}{(1+r)^i} - IC, \quad (1)$$

where CF_i – cash flow in *i*-th period and is equal to the difference between the inflows and outflows of all types of resources in monetary terms; *IC* – cost of the investment package; *r* – discount rate; *n* – total number of periods (intervals, steps) $i = 0,1,2,...,n$ for all investment periods.

In the context of the implementation of means and measures of protection, the discount rate can be considered equal to zero $r = 0$, cash flow in *i*-th period CF_i can be represented by the difference between information security risks before the implementation of the set of means and measures of protection *RTB* information security risks after its implementation *RTA*. This allows it to neglect the investment component of costs and focus on information security risks, in particular, losses that can occur with a certain likelihood before and after the implementation of means and measures of protection. Taking into account the above, it is proposed to calculate the simplified net present value of implementing a set of means and measures of protection against a certain set of threats over a certain period using the equation

$$NPV = \sum_{i=1}^{n} (RTB - RTA)_i - IC, \quad (2)$$

where *RTB* – risk of information security before implementation of the set of means and measures of protection against certain set of threats in *i*-th time period; *RTA* – total information security risk after implementation of the set of means and measures of protection against the specific set of threats in *i*-th time period; *IC* – cost of implementation of the set of means and measures of protection against the certain set of threats over time period *n*; *n* – total number of periods (months) that is used the set of means and measures of protection against the specific set of threats. It should be noted that the set of measures and means of protection can consist of one measure or means of protection or the set of them. The total risk to the implementation of the set of means and measures of protection against certain set of threats in the *i*-th period of time in EUR is calculated by the equation

$$RTB = \sum_{j=0}^{m} RB_j, \quad (3)$$

where RB_j – information security risk from realization of *j*-th threat to the implementation of the set of means and measures of protection against it in EUR; *m* – number of identified threats from the impact of which can reduce the information security risks of implementation of the set of means and measures of protection.

The total risk after implementation of the set of means and measures of protection against the certain set of threats in the *i*-th period of time in EUR is calculated by the equation

$$RTA = \sum_{j=0}^{m} RA_j, \quad (4)$$

where RA_j – information security risk from implementing a certain *j*-th threat after implementation of the set of means and measures of protection against it in EUR; *m* – the number of identified threats, the impact of which reduces information security risks by implementation of the set of means and measures of protection.

The risk of the implementation of a certain *j*-th threat before RB_j and after RA_j implementation of the set of means and measures of protection against it in EUR is calculated according to the equation:

$$RB_j = PB_j \cdot DB_j, \quad (5)$$

$$RA_j = PA_j \cdot DA_j, \quad (6)$$

where PB_j – potential damage caused from the realization of the *j*-th threat to implementation of means and measures of protection in EUR; DB_j – potential damage caused from the realization of the *j*-th threat to the implementation of means and measures of protection; PA_j – certain likelihood of realization of the *j*-th threat after the implementation of means and measures of protection in EUR; DA_j – certain likelihood of realization of the *j*-th threat after the implementation of means and measures of protection. When calculating the information security risk from the implementation of the set of means and measures of protection, which consists of more than one means or measure of protection against the impact of a certain threat, it is proposed to use the value of the likelihood of realization of a certain threat, which is minimal from the implementation of this set.

Likelihood of realization of *j*-th consecutive threat, i. e. a threat that may occur after the successful implementation of number of other threats, before and after the implementation of means and measures of protection, respectively, is calculated by the formulas:

$$PB_j = \prod_{c=0}^{s} PB_c, \quad (7)$$

$$PA_j = \prod_{c=0}^{s} PA_c, \quad (8)$$

where PB_c – likelihood of realization of *s*-th consecutive threat relative to the current *j*-th threat before the implementation of means and measures of protection; PA_c – likelihood of realization of the *s*-th consecutive threat relative to the current *j*-th threat after the implementation of measures of protection; *s* – number of consecutively realized threats, including the current *j*-th threat.

By substituting equation (3) and (4) into equation (2), and also taking into account the fact that the implementation of the set of means and measures of protection in the amount of *l* provides protection against the set of threats in the amount of *m*, the calculation of the net present value *NPV* for a certain period of time for the information security system in EUR can be calculated using the equation

$$NPV = \sum_{i=1}^{n} \left(\sum_{j=0}^{m} RB_j - \sum_{j=0}^{m} RA_j \right)_i - \sum_{k=0}^{l} IC_k, \quad (9)$$

where RB_j – information security risk from the realization of the certain *j*-th threat before the implementation of a set of means and measures of protection against it in the *j*-th period of time in EUR; RA_j – information security risk from the realization of the certain *j*-th threat after the implementation of the set of means and measures of protection against it in the *j*-th period of time in EUR; IC_k – cost of the *k*-th means or measure of protection in EUR, which is included in the set of means and measures of protection against *m*-threats for the period of time *n*; *m* – number of threats from which the set of *l* means and measures

ISSN-L 2664-9969; E-ISSN 2706-5448

of the protection against it provides protection; l – set of means and measures of protection against m threats; n – total number of periods (months) that the set of l means and measures of protection against the certain set of threats are used.

Taking into account that fact that implemented means and measures of protection at a certain point in time cannot provide protection against new threats over time, it is advisable to add the coefficient of the emergence of new threats rt to equation (9). Based on this, the Equation for calculating the net present value NPV for information protection systems in EUR is proposed to be expressed as follows

$$NPV = \sum_{i=1}^{n} \frac{\left(\sum_{j=0}^{m} RB_j - \sum_{j=0}^{m} RA_j \right)_i}{(1+rt)^i} - \sum_{k=0}^{l} IC_k, \quad (10)$$

where RB_j – information security risk from the realization of the certain j-th threat before the implementation of the set of means and measures of protection against it in the j-th period of time in EUR; RA_j – information security risk from the implementation of the certain j-th threat after the realization of the set of means and measures of protection against it in the j-th period of time in EUR; IC_k – cost of the k-th means or measure of protection in EUR, which is included in the set of means and measures of protection against m-threats for the period of time n; rt – coefficient of emergence of new threats, from which the implemented set of means and measures of protection cannot effectively protect; m – number of threats from which the set of l means and measures of protection provides protection; l – set of means and measures of protection that provides protection against m threats; n – total number of periods (months) that the set of l means and measures of protection against the certain set of threats is used.

This allows it to more accurately assess the effect of reducing information security risks from the implementation of means and measures of protection over time and to take into account the fact that the effectiveness of the implemented means and measures decreases over time.

Equation (10) assumes that the costs for improving the information security system were incurred once, that is, the information security system functions without modernization (improvements). In practice, the information security system undergoes continuous periodic improvement (modernization). In this regard, it is appropriate to consider the following equation [11] for calculating the present net value for investment costs that may occur over the number of periods

$$NPV = \sum_{i=1}^{n} \frac{CF_i}{(1+r)^i} - \sum_{i=0}^{n} \frac{IC_i}{(1+r)^i}, \quad (11)$$

where CF_i – cash flow in the i-th period and is equal to the difference between the inflows and outflows of all types of resources in monetary terms; IC_i – cost of the investment package in the i-th period; r – discount rate; n – the total number of periods (intervals, steps) for the total investment period.

Equation (11) is also convenient for calculations when the information security system is based on means, that is implemented by purchasing a periodic subscription (for example, per month). Considering the above assumptions, it is proposed to express the Equation for calculating net present value NPV for the certain period of time for information security systems in EUR as follows

$$NPV = \sum_{i=1}^{n} \frac{\left(\sum_{j=0}^{m} RB_j - \sum_{j=0}^{m} RA_j \right)_i}{(1+rt)^i} - \sum_{i=0}^{n} \sum_{k=0}^{l} IC_{k,i}, \quad (12)$$

where RB_j – information security risk from the realization of the certain j-th threat before the implementation of the set of means and measures of protection against it in the i-th period of time in EUR; RA_j – information security risk from the realization of the certain j-th threat after the implementation of the set of means and measures of protection against it in the i-th period of time in EUR; $IC_{k,i}$ – cost of the k-th means or measure of protection from set of means and measures protection against m-threats in the i-th period of time in EUR; rt – coefficient of emergence of new threats from which the implemented set of means and measures of protection cannot effectively protect; m – number of threats from which the set of l means and measures of protection provides protection; l – set of means and measures of protection that provides protection against m threats; n – total number of periods (months) that is used the set of l means and measures of protection against the certain set of threats.

When launching investment projects, it is important for an investor to know the payback period of project DPP. The payback period of project DPP can be calculated using the equation [11]

$$\sum_{i=1}^{DPP} \frac{CF_i}{(1+r)^i} = \sum_{i=1}^{DPP} \frac{IC_i}{(1+r)^i}, \quad (13)$$

where CF_i – cash flow in the i-th period and is equal to the difference between the inflows and outflows of all types of resources in monetary terms; IC_i – cost of the investment package in the i-th period; r – discount rate; i – serial number of the period (year).

Taking into account the assumptions described above, the payback period of project DPP for information security systems in months can be calculated using the equation

$$\sum_{i=1}^{DPP} \frac{\left(\sum_{j=0}^{m} RB_j - \sum_{j=0}^{m} RA_j \right)_i}{(1+rt)^i} = \sum_{i=1}^{DPP} \sum_{k=0}^{l} IC_{k,i}, \quad (14)$$

where RB_j – information security risk from the implementation of the certain j-th threat before the implementation of the set of means and measures of protection against it in the i-th period of time in EUR; RA_j – information security risk from the implementation of the certain j-th threat after the implementation of the set of means and measures of protection against it in the i-th period of time in EUR; $IC_{k,i}$ – cost of the k-th means or measure of protection from the set of means and measures of protection against m-threats in the i-th period of time in EUR; rt – coefficient of emergence of new threats from which the implemented set of means and measures of protection cannot effectively protect; m – number of threats from which set of l means and measures of protection provides protection; l – set of means and measures of protection that provides protection against m threats; i – serial number of the period (month) during which the set of l means and measures of protection against the certain set of threats is used.

Calculating the payback period of project DPP for information security systems that allow to estimate the number of months in which the result of reducing information security risks from implementation of the set of means and measures of protection can equal the cost of implementation the set of means and measures of protection. Calculating the payback period of project DPP allows to assess whether it makes sense to implement the certain set of means and measures of protection or whether it needs to look for other options for reducing information security risks.

3.2. Method for forming optimal options of risk treatment

Taking into account the described mathematical apparatus, a method for forming optimal options of information security risks treatment is proposed, based on quantitative assessment models, consisting of the following stages:

Stage 1 – Identification of initial information security risks and carrying out their quantitative assessment.

Assets of the organization, including existing means of protection, as well as their characteristic threats and vulnerabilities, should be

identified. Based on the results of the identification of information security risks, their quantitative assessment should be carried out. These actions should be taken to form a clear understanding of the starting point for the modernization of the information security system.

Identification of information security risks and their quantitative assessment can be carried out using the information security risk assessment method, which is based on the use of a simulation model based on the theory of colored Petri nets. The features of the application of this method are described in [12].

Stage 2 – Conducting information security risk evaluation and searching for optimal options for implementation of means and measures of protection.

For conducting the evaluation, it is necessary:

Step 2.1. Create a list of options for information security risks treatment (in other words, a list of means and/or measures of protection) to improve the information security system.

Step 2.2. Choose the most effective option for implementation of the set of means and measures of protection. For this, it can be used one of the mathematical methods or the widely used ABC analysis method. In this work, it is recommended to use the ABC analysis method. The features of the application of the ABC analysis method in information protection issues are described [6].

As a factor based on which the objects of analysis will occur differentiation, it is proposed to choose the indicator of the effectiveness of the means or measure of protection E, which is calculated using the following equation

$$E = \frac{\sum_{i=1}^{n}\left(\sum_{j=0}^{m} RB_j - \sum_{j=0}^{m} RA_j\right)_i}{\sum_{i=0}^{n}\sum_{k=0}^{l} IC_{k,i}}, \quad (15)$$

where RB_j – information security risk from realization of j-th threat to the implementation of the set of means and measures of protection against it in the i-th time period in EUR; RA_j – information security risk from the realization of the certain j-th threat after the implementation of the set of means and measures of protection against it in the i-th time period in EUR; $IC_{k,i}$ – cost of the k-th means or measure of protection from the set of means and measures of protection against m-threats in the i-th time period in EUR; m – number of threats against which the set of l means and measures of protection provides protection; l – set of means and measures of protection that provides protection against m threats; n – total number of periods (months) that the set of l means and measures of protection are used against the certain set of threats.

It will allow choosing the means and/or measures of protection that allow it to reduce information security risks as quickly as possible and direct key costs to means and protection measures that minimize information security risks from the implementation of most threats. At the same time, other threats, depending on the probability of their implementation, can either be ignored or the risks from their implementation can be transferred to a third party (for example, an insurance company) or free or minimally expensive means and measures of protection can be implemented (for example, open-source means protection).

Step 2.3. Calculate the net present value *NPV* of implementing each means or measure of protection separately, as well as their set (if any) according to Equation (12). The key purpose is to make sure that the implementation of means and/or measures of protection is not at a loss for the organization.

After that, it is necessary to calculate the payback period of the *DPP* project for the set of means and measures proposed to be implemented, according to Equation (14). The key purpose is to show the investor how quickly the investment in the modernization of the security system will pay off.

This, unlike existing models, allows verifying that the implementation of means and measures of protection is carried out in a manner that is not loss-making to the organization.

Step 2.4. After selecting and implementing means and measures of protection, update the information about information security risks by conducting their re-assessment. The specified assessment must be carried out using the method selected at Stage 1.

When building a risk-oriented information security system, the actions specified in Stage 2 could be performed on a cyclical basis at each iteration of the modernization of the information security system.

In general, the method described above will allow creating risk-oriented information security system in which the selection of means and measures of information protection is based on a quantitative assessment of information security risks. This method, unlike existing ones, allows the comprehensive assessment of risks, the selection of more effective means and measures to counter threats from a variety of potential means and measures, and the verification that treatment of information security risks is carried out at a break-even price.

3.3. Example of risk treatment using the proposed method

Below is an example of information security risk treatment using the method described in Section 3 of this article.

Stage 1 – Identification of initial information security risks and carrying out their quantitative assessment.

Below is a description of the information security environment treatment (identification of assets and available protection means) in order to formulate the task of optimizing information security risks.

The information system of Organization 1 exchanges data with the information system of Organization 2 through electronic interaction using REST services and REST clients deployed on the application servers of both organizations. Organization 2 is a subsidiary of Organization 1. The organizations sell airline tickets. As part of the data exchange, personal customer data is exchanged, including information about bank accounts. Data exchange is carried out using the HTTPS protocol without mutual authentication check. Authorization of various REST services is carried out by login and password. Application servers of both organizations operate under the control of operating systems deployed in containers in the clouds of different providers, which guarantee constant connection to the Internet and guarantee protection up to the level of the containerization system. On the application servers, in addition to REST services and REST clients used for interaction between Organization 1 and Organization 2, other REST services and REST clients operate for interaction with other organizations. One REST service is used for interaction with multiple organizations. Container administration is carried out using CI/CD scripts that are launched from the providers' cloud platform. Access of DevOps engineers of both information systems to the providers' cloud platforms is carried out using a software key that is stored on the administrators' laptops. Organizations 1 and 2 plan to provide services for the next 60 months.

The described environment of information treatment is exposed to the following threats:

TR.1. Violation of the confidentiality of personal data of some customers due to data interception as a result of MITM attack.

TR.2. Violation of the confidentiality of personal data of all customers due to theft of the DevOps engineer's access key to the cloud platform and gaining access to the operating system with the application server.

TR.3. Violation of the confidentiality of personal data of all customers due to the implementation of SQL/NoSQL injection in relation to the REST service.

TR.4. Violation of the confidentiality of personal data of some or all customers due to gaining access to the login and password for accessing the REST service, which was stored in the CI/CD script as a result of gaining access to the DevOps engineer's workstation.

ISSN-L 2664-9969; E-ISSN 2706-5448

TR.5. Temporary unavailability of the REST service due to Denial of Service due to an unintentional failure of one of the components.

TR.6. Temporary unavailability of the REST service due to DDoS attack on the application server.

Table 1 shows the results of the assessment of the initial (before the implementation of means and measures of protection) information security risks per month from the impact of the certain threat RB_j. The calculation of the indicator RB_j was carried out according to Equation (5). Considering the fact that the main purpose of this article is to demonstrate a new mathematical apparatus, the fragment of the colored Petri net will not be displayed.

Table 1

Results of the assessment of the initial risks of information security per month from the impact of certain threat

Threat number (j)	Likelihood of threat realization before the implementation of means and measures of protection (PB_j) per month	Potential consequences to the implementation of means and measures of protection (DB_j), EUR	Risks before the implementation of means and measures of protection (RB_j) per month
TR.1	0.00007	500,000	35
TR.2	0.0002	500,000	100
TR.3	0.00007	500,000	35
TR.4	0.00007	500,000	35
TR.5	0.002	10,000	20
TR.6	0.00007	10,000	0.7

The total risk before the implementation of means and measures of *RTB* protection, which is calculated according to Equation (3), is 13,542 EUR for 60 months:

Stage 2 – Conducting the assessment of information security risks and searching for optimal options of implementation of means and measures of protection.

Step 2.1. For improving the information security system, the following list of means and measures of protection is proposed that can be used to reduce information security risks:

SM.1. Using decentralized secure data exchange platform.

SM.2. Placing the DevOps engineer key on physical token.

SM.3. Using WAF from cloud service provider.

SM.4. Installing antivirus software with signature and heuristic analysis functionality.

SM.5. Compiling sheet (list) of information about the information systems of organizations with which data is exchanged, and access is provided exclusively from the list of allowed IP addresses.

SM.6. Purchasing Anti-DDoS protection tools.

SM.7. Creating backup node for all components.

Purchasing means and measures of protection under items *SM.1*, *SM.3*, *SM.4*, *SM.6* and *SM.7* can be carried out in stages by purchasing a subscription. For simplifying the calculations, the example above assumes that the expenses will be incurred immediately for a period of 60 months.

Step 2.2. Table 2 provides information on the cost of the means and measures of protection IC_k, the coefficient of emergence of new threats *rt*, the list of threats affected by the implementation of the means and measures of protection, including information on the change in the likelihood of threat realization after their implementation PA_j, as well as the value of the effectiveness indicator of the mean or measure of protection *E*, which is calculated using Equation (15).

Table 3 shows the results of the ABC analysis, which is aimed at selecting means and/or measures of protection that should be implemented as a priority to optimize information security risks.

Table 3 shows that the means and measures of protection are divided into 3 groups (A, B, C). Group A consists of the most effective means or measures of protection; group B – effective; C – weakly effective.

When processing risks, it is proposed to implement means and measures of protection that fall into groups A and B, if they provide for reduction in risks at price that is not unprofitable for the organization.

Step 2.3. Table 4 shows the results of calculating the net present value *NPV* from the implementation of each individual means or measure of protection.

Table 4 shows that all the proposed means and measures of protection reduce information security risks at non-loss cost. Since each of the means and measures that form the set of means and measures of protection affects the likelihood of threat realization, it is necessary to calculate net present value *NPV* from the implementation of the set of means and measures of protection. Table 5 provides information on the likelihood of threat realization from the implementation of the set of means and measures of protection. The likelihood of threat realization is taken as its minimum value, that is, the value from the implementation of the most effective means or measure of protection to reduce the impact of a particular threat.

Table 2

Information about potential means and measures of protection against threats

Number of means or measure of protection (k)	Cost of k means or measures of protection (IC_k), EUR	Coefficient of emergence of new threats *rt*	Threat numbers (j), against which the mean k protects	Likelihood of threat realization after implementation of mean or measure of protection (PA_j)	Indicator of the effectiveness of mean or measure of protection *E*
SM.1	15,000.00	0.0001	*TR.1*	0.00	0.260
			TR.3	0.00	
			TR.4	0.00	
			TR.5	0.06	
SM.2	50.00	0.00	*TR.2*	0.00	120.000
SM.3	1,200.00	0.001	*TR.3*	0.00	1.750
SM.4	200.00	0.0005	*TR.2*	0.00001	37.500
			TR.4	0.00001	
SM.5	120.00	0.00	*TR.1*	0.00	52.850
			TR.3	0.00	
			TR.4	0.00	
			TR.6	0.00	
SM.6	3,000.00	0.0001	*TR.6*	0.00	0.014
SM.7	20,000.00	0.0001	*TR.5*	0.0004	0.048

Table 3

Results of ABC analysis of the impact of implementation of means and measures of protection

Number of means or measure of protection (k)	Indicator of the effectiveness of mean or measure of protection E	Share of the factor in the sum of factor value, %	The increasing value of the object's contribution to the overall result in percent (OC), %	The increasing value of the share of objects from the total number in percent (SO), %	Sum of OC and SO, %	Group
SM.2	120	0.56491	0.56491	0.14286	0.70777	A
SM.5	52.85	0.24880	0.81371	0.28571	1.09942	A
SM.4	37.5	0.17654	0.99025	0.42857	1.41882	B
SM.3	1.75	0.00824	0.99848	0.57143	1.56991	B
SM.1	0.26	0.00122	0.99971	0.71429	1.71399	C
SM.7	0.048	0.00023	0.99993	0.85714	1.85708	C
SM.6	0.014	0.00007	1.00000	1.00000	2.00000	C

Table 4

Results of calculating the net present value of implementation of each means and measures of protection

Number of means or measure of protection (k)	Net present value NPV of implementation of mean or measure of protection
SM.2	3838.13
SM.5	6222.00
SM.4	7075.90
SM.3	868.30

Table 5

Information on the likelihood of threats being realized in the event of implementing the set of measures and means of protection

Threat number (j)	Likelihood of threat realization after implementation of the set of means and measures of protection (PA_j) per month
TR.1	0.00
TR.2	0.0002
TR.3	0.00
TR.4	0.00
TR.5	0.002
TR.6	0.00

The net present value *NPV* of implementing the set of means and measures of protection for 60 months, that consists of *SM.2*, *SM.3*, *SM.4* and *SM.5*, taking into account that the coefficient of emergence of new threats *rt* for the proposed set of means and measures of protection is 0.0002, is equal to 10,697.02 EUR. At the same time, the payback period *DPP* project when investing funds in the information security system immediately for 60 months is 8 months. In the case of purchasing a subscription to mean protection, this period may be shorter.

In other words, when requesting funds for means and measures of protection, the organization's management can be informed that the savings from the implementation of the set of means and measures of protection is 10,697.02 EUR, and the payback period of the investment in the modernization of the information security system is 8 months.

Step 2.4. Table 6 shows the results of calculating information security risks from the realization of each identified threat after the implementation of the set of means and measures of protection RA_j. The calculation of the indicator RA_j was carried out according to Equation (6).

The total risk after implementation of means and measures of protection *RTA*, that is calculated by Equation (4), is 1200.00 EUR for 60 months.

As a conclusion, implementation of means in the amount of 1,570.00 EUR will reduce the risks by 12,342.00 EUR in 5 years. Ensuring protection against threat *TR.5* using the proposed means and measures of protection does not appear to be possible. The identified information security risk can either be neglected or transferred to the insurance company.

Table 6

Results of calculating information security risks from the realization of each identified threat after implementation means and measures of protection

Threat number (j)	Likelihood of threat realization after implementation of means and measures of protection (PA_j) per month	Potential consequences after the implementation of means and measures of protection (DA_j), EUR	Risks after implementation of means and measures of protection (RA_j)
TR.1	0.00	500,000	0.00
TR.2	0.0002	500,000	0.00
TR.3	0.00	500,000	0.00
TR.4	0.00	500,000	0.00
TR.5	0.002	10,000	20
TR.6	0.00	10,000	0.00

ISSN-L 2664-9969; E-ISSN 2706-5448

3.4. Discussion

The developed method allows in practice to create a risk-oriented information security system, which will be based on economically justified processing of information security risks. The method, unlike existing ones, has significantly simplified the process of reducing information security risks at the non-profitable price. In particular, the method involves assessing the initial information security risks, forming a list of potential means and measures of protection against identified threats, evaluating the effectiveness of each of the proposed means and measures of protection and their ranking, re-evaluating information security risks after their treatment. The method proposed in this work allows protecting the organization from investments in the information security system that will never pay off and will lead to additional losses. The use of ABC analysis in combination with the calculation of the effectiveness of the implementation of means and measures of protection allows determining the priority of implementing means of protection by implementing, first of all those, that most reduce information security risks.

The proposed method solves number of previously unsolved issues. In particular, the equations given in [7, 8] for calculating the net present value *NPV* and the payback period of project *DPP* focus on the profits and costs received, rather than information security risks, and do not take into account the fact that the means and measures of protection have a lower effectiveness in countering threats over time. Neglecting the coefficient the discount rate *r* and introducing the coefficient of emergence of new threats was introduced, which the implemented set of means and measures of protection cannot effectively protect *rt* allowed to improve the Equations for calculating the net present value and the payback period of project. Besides that, this allowed it to focus attention not on the value of funds, but on losses that can occur with a certain likelihood before and after the implementation of means and measures of protection. In addition, this allows it to more accurately assess the effect of reducing information security risks from the implementation of means and measures of protection over time and to take into account the fact that the effectiveness of the implemented means and measures decreases over time.

The ranking indicators proposed in [5, 6] for conducting ABC analysis allow to choose threats for which information security risk management means should be implemented first. However, these indicators do not allow to choose those that effectively reduce information security risks and should be implemented first, among the many potential means and measures of protection. This issue was solved in this publication through the use of an effectiveness indicator *E*, which demonstrates how effectively a means and/or measure of protection reduces information security risks from the implementation of a threat pool. This allowed ranking means of protection based on the ratio of risk reduction from the implementing means and measure of protection and their cost. In turn, this allowed it to choose from a set of means and measures aimed at protecting the organization from threats, those that most effectively reduce information security risks.

Proposed method allows the comprehensive assessment of risks, the selection of more effective means and measures to counter threats from a variety of potential means and measures, and the verification that treatment of information security risks is carried out at a break-even price. Compared with similar known models and methods, this provides a simplified procedure for information security risk treatment in practice.

The developed method is based on rather simple models and methods, which allow specialists to use it in practice without additional mathematical training. However, it should be taken into account that the number of identified assets and threats can be large, which makes the use of the specified method in practice without automation difficult.

Prospects for further research include activities aimed at typifying and grouping threats to unify the threat identification process, as well as integrating into the method models for calculating potential damage that can be caused to the organization's assets as a result of the impact of threats.

4. Conclusions

1. The following economic theory models were chosen as models for assessing the effectiveness of investments in information security: the indicators net present value *NPV* and payback period of the project *DPP*. Particularly, these indicators are elements of the theory of investments, which are actively used to assess the effectiveness of investment in projects. The implementation of means and measures of protection is an investment project aimed at reducing information security risks. Using these indicators will allow it to assess and ensure that the implementation of means and measures of protection is carried out in a manner that is not loss-making for the organization.

2. For forming an optimal set of means and measures of protection, the specified Equations for calculating the specified indicators were adapted to the issue of forming the optimal set of means and measures of protection. Particularly, it was proposed to neglect the discount rate *r* indicator, since it is possible to assess not the loss of value of funds over time, but the impact on the risk of information security. Taking into account that, the information security system is a system with a delay, instead of this indicator the coefficient of emergence of new threats was introduced, which the implemented set of means and measures of protection cannot effectively protect *rt*. Unlike existing models, this allowed it to take more clearly into account the effectiveness of reducing information security risks by the implemented means and measures of protection at different time intervals.

3. Adaptation of the ABC analysis selected to form the optimal set of means and measures of protection consisted in determining the identifier that would be used for ranking. As such an indicator, the authors proposed to use the indicator of the effectiveness of the means or measure of protection *E*. Unlike [5, 6], this allowed not only to implement means and measures of information protection from the most popular threats, but also to choose from a set of means and measures aimed at protecting the organization from threats those that most effectively reduce information security risks.

4. As a sequence of actions for forming the optimal option for information security risk treatment, the work proposed a method that involves performing a certain set of activities divided into stages. In particular, the method involves identifying initial information security risks, conducting a risk assessment, and searching for optimal options for implementing means and measures of protection. For the initial identification and assessment of information security risks, it is proposed to use a simulation model based on a colored Petri net developed earlier by the authors. For conducting the assessment of information security risks and searching optimal options, it is proposed to use the ABC analysis method, which uses the indicator as a ranking indicator *E*. The proposed method involves calculating net present value *NPV* and payback period of the project *DPP*. This allows the owner of the organization to assess the economic efficiency of implementing the set of means and measures of protection, as well as to understand when the costs of the information security system will pay off. For checking the profitability of implementing means and measures of protection, it involves calculating the net present value *NPV* and payback period of project *DPP*. After implementing means and measures of protection, a reassessment of information security risk is expected. This allowed the creation of information security system based on a risk-based approach.

5. For demonstrating the use of proposed method for forming optimal options of information security risk treatment, an example of its use in the issue of choosing means and measures of protection for protecting electronic interactions between information systems was given. The specified example allowed it to choose the most optimal means and

measures for protecting electronic interactions and demonstrated the possibility of applying the proposed method in practice.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, including financial, personal, authorship or other, which could affect the research and its results presented in this article.

Financing

The research was performed without financial support.

Data availability

The manuscript has no associated data.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (2022). *Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
2. NIS2 Technical Implementation Guidance (2025). *ENISA*. Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls (2022). *International Organization for Standardization*. Available at: https://www.iso.org/standard/75652.html
4. IEC 31010:2019 Risk management – Risk assessment techniques (2019). *International Organization for Standardization*. Available at: https://www.iso.org/standard/72140.html
5. Stefani, E., Costa, I., Gaspar, M. A., Goes, R. de S., Monteiro, R. C., Petrili, B. R. et al. (2025). Information Security Risk Framework for Digital Transformation Technologies. *Systems, 13 (1),* 37. https://doi.org/10.3390/systems13010037
6. Kononovych, V., Kopytin, Yu. (2010). Vykorystannia ABC analizu dlia optymizatsii system zakhystu informatsii. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, 2 (21)*, 26–35. Available at: https://ela.kpi.ua/handle/123456789/9099
7. Brho, M., Jazairy, A., Glassburner, A. V. (2025). The finance of cybersecurity: Quantitative modeling of investment decisions and net present value. *International Journal of Production Economics,* 279. https://doi.org/10.1016/j.ijpe.2024.109448
8. Ofori-Yeboah, A., Addo-Quaye, R., Oseni, W., Amorin, P., Agangmikre, C. (2021). Cyber Supply Chain Security: A Cost Benefit Analysis Using Net Present Value. *2021 International Conference on Cyber Security and Internet of Things (ICSIoT).* France: IEEE, 49–54. https://doi.org/10.1109/icsiot55070.2021.00018
9. Kononovich, V., Kononovich, I., Kopytin, Yu., Staikutsa, S. (2014). Influence of delays decision action for information protection on information security risks. *Ukrainian Scientific Journal of Information Security, 20 (1)*, 83–91. Available at: http://nbuv.gov.ua/UJRN/bezin_2014_20_1_16
10. Kravchenko, V. (2022). Chysta potochna vartist (NPV). *LivingFo*. Available at: https://livingfo.com/chysta-potochna-vartist-npv/
11. Roziasnennia shchodo rozrakhunkiv prohnozovanykh pokaznykiv efektyvnosti investytsiinykh prohram subiektiv hospodariuvannia u sferi teplopostachannia, tsentralizovanoho vodopostachannia ta vodovidvedennia (2013). *Roziasnennia n0079866-13. Natsionalna komisiia, shcho zdiisniuie derzhavne rehuliuvannia u sferi komunalnykh posluh*. Available at: https://zakon.rada.gov.ua/rada/show/n0079866-13#Text
12. Kopytin, Yu. (2014). Developing a model of information security risk assessment based on colored Petri net. *Ukrainian Scientific Journal of Information Security, 20 (3)*, 293–299. https://doi.org/10.18372/2225-5036.20.7558

Yurii Kopytin, *Senior Expert in Information Technology Management, e-Governance Academy Representative Office in Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-1617-6556*

✉***Maryna Kopytina,*** *PhD Student, Department of Management and Marketing, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine, e-mail: myr19@i.ua, ORCID: https://orcid.org/0009-0009-1665-6905*

Volodymyr Korchynskyi, *Doctor of Technical Sciences, Department of Cybersecurity and Technical Protection of Information, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine, ORCID: https://orcid.org/0000-0003-3972-0585*

✉*Corresponding author*