DOI 10.20535/2411-1031.2025.13.2.344595
UDC 004.056

SERGEY SMIRNOV,
VIKTORIIA POLUTSYHANOVA

RISK ASSESSMENT AND ANALYSIS FOR THREATS AND VULNERABILITIES OF THE CORPORATE INFRASTRUCTURE INFORMATION SYSTEM

This article presents a methodological approach to assessing risks associated with the threats and vulnerabilities of the information system of a corporate infrastructure object (ISCIO). The relevance of this topic is due to the growing number and complexity of cyber threats and the need for more accurate risk assessment tools that account for the structure of interdependencies between potential vulnerabilities and attacks.

The main problem addressed in the study is the insufficient precision of traditional risk assessment methods that do not reflect the composite nature of threats within complex systems. To solve this issue, the authors employ an extended Q-analysis methodology, which considers the structural relationships between threats and vulnerabilities to form a more detailed risk model.

The purpose of the study is to apply the theoretical foundations of extended Q-analysis to a practical example using real expert data. As part of this, the authors construct an incidence matrix between threats and vulnerabilities, form a simplex complex, and build a structural tree to visualize interdependencies. Based on these models, calculations are performed to estimate the loss values associated with each threat and their combinations (“gluing”). Using optimization methods, including the Lagrange method, the authors identify conditions for maximum and minimum risk, analyze the behavior of the risk function under different probability distributions, and construct comparative graphs.

The results demonstrate that the refined methodology allows a reduction in overall risk by up to 23.3% compared to linear models, depending on the threat distribution. The findings confirm the practical value of the proposed approach, offering more accurate risk estimates and improved decision-making support in cybersecurity management of complex information systems.

Keywords: risk assessment, infrastructure, Q-analysis, information system.

Introduction. Recently, the popularity of risk assessment methods and approaches has increased significantly. More and more regulations and standards are being adopted that contain risk assessment rules and provide for their application in various areas. This contributes to the development and improvement of relevant methodological approaches. Given the above, it is expected that this trend will continue to remain relevant [1].

The main goal of risk analysis is to provide sound recommendations for decision-making. In the process of making decisions related to risks, it is important to understand their sources. Risk assessment methods help to solve a wide range of issues - from global ones, such as the choice of location of production facilities, to technical aspects of system operation, including human and organizational factors.

Risk assessment should provide objective data that will allow finding a balance between increasing profits and minimizing negative consequences. This is an iterative process that contributes to the constant improvement of decision-making, and ideally - increasing efficiency.

In addition, risk assessment is an important element of the quality control system. The implementation of quality standards involves the use of various methods and sources of information that meet the needs of users. Just like risk, the quality level of an institution is determined by its institutional environment and strategic goals. The institutional environment significantly affects the organization's tolerance for risk in achieving its goals.

The risk assessment and management process includes several stages: establishing a framework, identifying risks, analyzing their likelihood and consequences, assessing risks, and finally developing response measures. This study focuses primarily on the risk assessment stage, while complementing the methodology of the entire risk management cycle in complex systems.

Methodology for collecting information for risk assessment based on extended Q-analysis.

In previous works [5]-[7], the methodology of extended Q-analysis of risk assessment based on the interdependence between threats and vulnerabilities of cybernetic systems was presented, as well as the specifics of its application in risk assessment and construction of loss functions. This study presents scientific approaches to the practical application of the obtained theoretical results and their use in real systems.

The preliminary stage is the collection of data and its presentation in the form necessary for the application of the methodology. Depending on the characteristics of the collected information, several options for its primary processing are envisaged.

The first case is considered the best, but practically does not occur. This is the case when the data is already presented in the form of a structural dependence, that is, in the form of a symlecial complex.

The second case is more likely. This is the case when the collected primary data is presented in the form of an incidence matrix between vulnerabilities and threats. In this form, the collected data is sometimes found.

The third case is the most common. The collected data are confidential, or they are quite specific with a narrow subject area of application. In this case, it is advisable to use the inverse problems of Q-analysis to construct a symplectic complex for the purpose of further analysis.

To conduct a study of the practical application of the methodology of extended Q-analysis, within the framework of the dissertation research, data from the system of threats and vulnerabilities of the information system of the corporate infrastructure object (hereinafter – ISCIO), given in the work of V. Kuz [2].

Vulnerabilities used for the study, as well as the assessment of the specified list of threats $\{u_k\}$ for a conditional corporate infrastructure object obtained as a result of an expert analysis of ISOKI. Based on the results of the expert analysis, a list was also formed $\{b_l\}$, $l = \{1, 2, \ldots, L\}$ elements that indicate vulnerabilities [2]. The latter are interconnected with potentially vulnerable components, which are the ones that can be targeted by attacks.

Application of the risk assessment method based on structural Q-analysis. According to the methodology of extended Q-analysis [8], using the above lists of elements denoting vulnerabilities and threats from attacks, an incidence matrix (q-connectivity) between vulnerabilities and threats for ISCIO was constructed (table 1).

Table 1 – Incidence matrix between vulnerabilities and threats for ISCIO

Threats of computer attacks	Vulnerability of ISCIO information resources to the implementation of threats of computer attacks														
	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
u_1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
u_2	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1
u_3	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1

Threats of computer attacks	Vulnerability of ISCIO information resources to the implementation of threats of computer attacks														
	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
u_4	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
u_5	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
u_6	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
u_7	1	1	1	0	0	0	1	0	0	0	0	0	1	0	0
u_8	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_9	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_{10}	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1
u_{11}	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0
u_{12}	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0
u_{13}	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0
u_{14}	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0

The next step is to construct the q-connectivity matrix for the threat system depending on the vulnerabilities b_l, which is given in Table 2.

Table 2 – Simplex complex matrix for the threat system depending on the vulnerabilities

Threats	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}
u_1	7	5	6	7	4	6	2	4	4	4	2	3	3	2
u_2	5	9	9	9	3	7	1	3	3	3	2	2	4	1
u_3	6	9	12	12	6	10	4	6	6	6	4	3	5	4
u_4	7	9	12	14	6	12	5	7	7	7	4	4	6	4
u_5	4	3	6	6	6	6	4	5	5	5	3	1	1	4
u_6	6	7	10	12	6	12	5	7	7	7	3	3	4	4
u_7	2	1	4	5	4	5	5	4	4	4	3	1	1	4
u_8	4	3	6	7	5	7	4	7	7	6	3	2	2	4
u_9	4	3	6	7	5	7	4	7	7	6	3	2	2	4
u_{10}	4	3	6	7	5	7	4	6	6	7	3	2	2	4
u_{11}	2	2	4	4	3	3	3	3	3	3	4	1	2	3
u_{12}	3	2	3	4	1	3	1	2	2	2	1	4	4	1
u_{13}	3	4	5	6	1	4	1	2	2	2	2	4	6	1
u_{14}	2	1	4	4	4	4	4	4	4	4	3	1	1	4

The next stage is to conduct a structural Q-analysis to identify possible compatible implementations of vulnerabilities that manifest themselves through a complex structure of interdependencies between vulnerabilities and threats. Based on the developed and presented in [5], we build local maps and a structural tree, which are shown below in Figure 1 and 2.

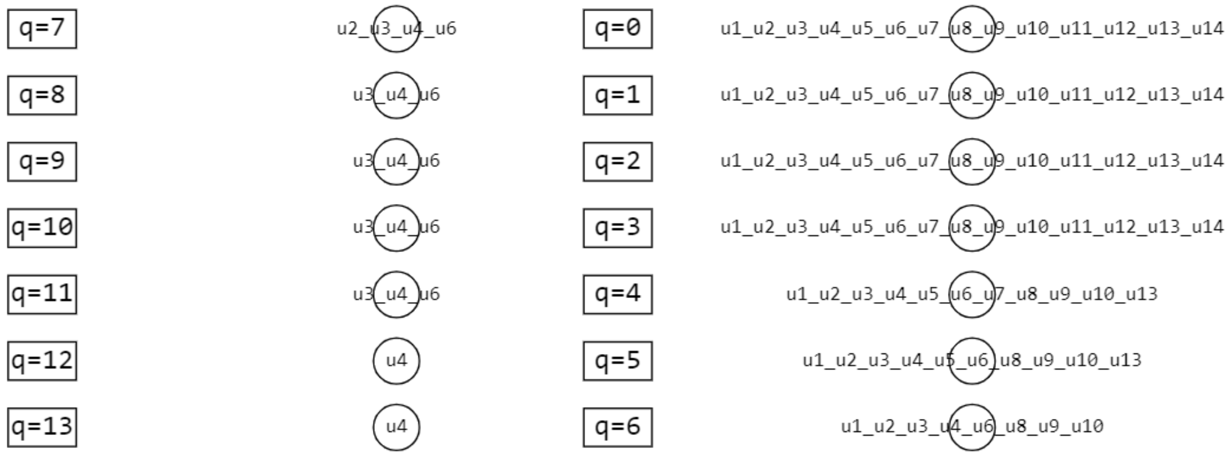
q=7
u2_u3_u4_u6
q=8
u3_u4_u6
q=9
u3_u4_u6
q=10
u3_u4_u6
q=11
u3_u4_u6
q=12
u4
q=13
u4
q=0
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=1
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=2
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=3
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=4
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u13
q=5
u1_u2_u3_u4_u5_u6_u8_u9_u10_u13
q=6
u1_u2_u3_u4_u6_u8_u9_u10

Figure 1 – Local maps

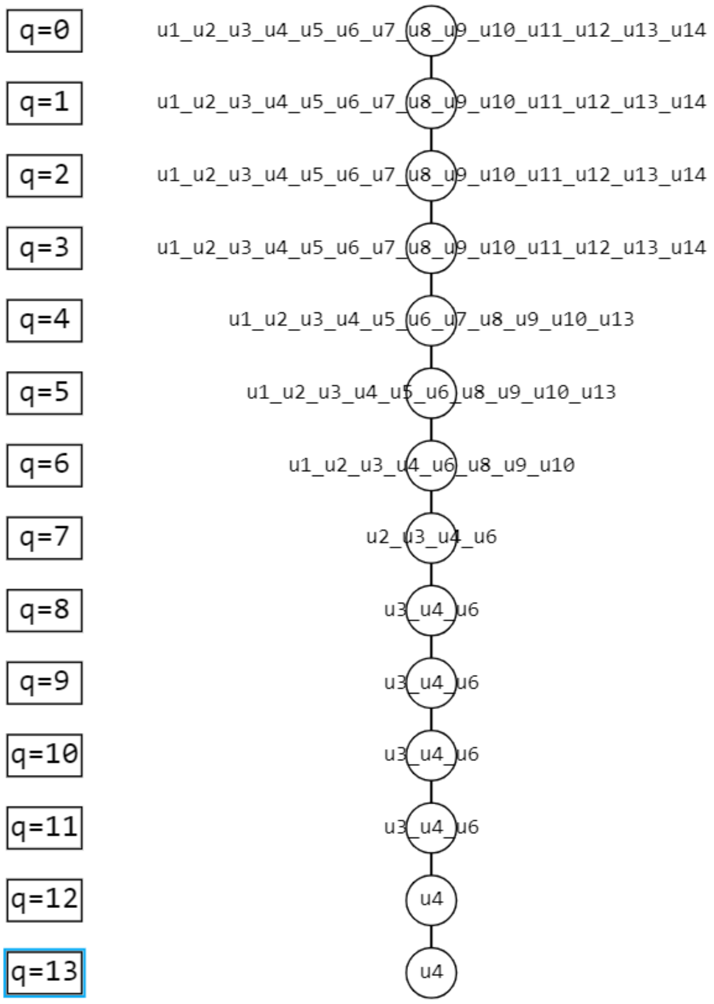
q=0
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=1
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=2
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=3
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u11_u12_u13_u14
q=4
u1_u2_u3_u4_u5_u6_u7_u8_u9_u10_u13
q=5
u1_u2_u3_u4_u5_u6_u8_u9_u10_u13
q=6
u1_u2_u3_u4_u6_u8_u9_u10
q=7
u2_u3_u4_u6
q=8
u3_u4_u6
q=9
u3_u4_u6
q=10
u3_u4_u6
q=11
u3_u4_u6
q=12
u4
q=13
u4

Figure 2 – Structural tree

An important stage is the calculation of losses for each threat due to potential losses from vulnerabilities. In conditions of increasing risk for ISCIO, in particular due to the spread of phishing attacks, botnets, the use of virus-infected software, “ransomware”, etc. [3], a specific approach is to identify vulnerabilities in information resources (hereinafter - IR) of ISCIO. To determine the risk of possible attacks, it is proposed to apply calculation methods for assessing potential threats.

To calculate losses from the implementation of threats (attacks), the values of the destruction coefficients of vulnerable components of the ISCIO IR are required. Their values must correspond to the costs of restoring the standard state of the relevant components and can be accurately estimated based on the estimates of the relevant restoration works. Of course, the external (system) effect of destruction can significantly exceed the sum of these costs, so its assessment should be carried out separately on the basis of expert opinions.

Within the framework of this study, for a demonstration example of calculating losses and risks from attacks, we will limit ourselves to rough estimates, using the categorical scale given in Table 3.

For further risk calculations, only the estimate of total losses given in the last row of Table 3 is actually used.

At the same time, Table 3 itself reflects one of the methods of assessing losses generated by the implementation of the relevant vulnerability as a result of the attack.

Table 3 – Categorical estimates of destruction from CI vulnerabilities

Destruction	Vulnerabilities														
	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
Soft	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
Hard	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1
Data	0	0	0	0	1	0	0	0	1	1	1	1	1	0	0
External Effect	1	1	1	1	2	2	3	3	3	3	3	4	4	1	1
Total Losses	**2**	**2**	**2**	**2**	**4**	**3**	**4**	**5**	**5**	**6**	**6**	**6**	**6**	**2**	**2**

To calculate risks, in addition to losses, we need to determine their probability. But the probability distribution of joint implementation of vulnerabilities depends on the characteristics of real attacks [4]. In real incidents, risk assessments based on the fact of threat implementation may differ. In the case when there is a statistical distribution of the occurrence of certain losses from the implementation of threats, which, in particular, depend on the presence in the system of a list of vulnerabilities that jointly affect their occurrence, it is possible to use the frequency of threat occurrence to assess the probability of vulnerabilities, as well as apply such indicators as the level of influence of individual threats. Table 4 shows indicators (calculations) of the total level of losses depending on the individual identified threats.

Table 4 – Level of losses for each threat in the system

	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}	**Σ**
Total loss rate (V_i)	25	42	48	55	16	43	16	22	22	22	16	16	28	12	**383**

Table 5 shows the indicators (calculations) of losses from gluing for each gluing of threat simplexes in the system.

After the calculations are made, an assessment of threats and risks is carried out, the probability of which is the highest in practice. To calculate risks, it is assumed that the joint realization of adverse events, in particular from an attack, is independent in terms of losses. Therefore, risks are calculated as a sum, and the probability of an event as a product.

Table 5 – Loss level for each gluing of threat simplexes in the system

Gluing	Gluing losses
$V_{\{u3,u4\}}$	48
$V_{\{u2,u3\}}$	42
$V_{\{u1,u4\}}$	25
$V_{\{u8,u4\}}$	22
$V_{\{u4,u9\}}$	22
$V_{\{u4,u10\}}$	22
$V_{\{u4,u5\}}$	16
$V_{\{u4,u13\}}$	28
$V_{\{u4,u7\}}$	16
$V_{\{u3,u11\}}$	16
$V_{\{u4,u12\}}$	16
$V_{\{u4,u9\}}$	12
$V_{\{u3,u14\}}$	43
Σ	328

The total risk is calculated according to formula (1).

$$R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = \sum_{i=1}^{14} p_{u_i} V_{u_i} - \\ - \sum_{i=1}^{\{1,3,5,6,7,8,9,10,12,13\}} p_{u4} p_{u_i} V_{\{u_4,u_i\}} - \sum_{i=2}^{\{11,14\}} p_{u3} p_{u_i} V_{\{u_3,u_i\}} \tag{1}$$

Since for the studied ISCIO, loss indicators (calculations) have already been calculated for each threat in the system and for each gluing of threat simplexes in the system, the corresponding valuesare given in Tables 4 and 5.

Taking into account the above indicators, the total risk for the studied ISCIO is calculated according to formula (2) and depends only on the probability of events occurring.

$$R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} = 25p_{u_1} + 42p_{u_2} + 48p_{u_3} + 55p_{u_4} + \\ +16p_{u_5} + 43p_{u_6} + 16p_{u_7} + 22p_{u_8} + 22p_{u_9} + 16p_{u_{11}} + 28p_{u_{13}} + 12p_{u_{14}} - \\ -43p_{u_4}p_{u_6} - 48p_{u_2}p_{u_4} - 42p_{u_2}p_{u_3} - 25p_{u_1}p_{u_4} - 22p_{u_4}p_{u_8} - 22p_{u_4}p_{u_9} - \\ -16p_{u_4}p_{u_5} - 28p_{u_4}p_{u_{13}} - 16p_{u_3}p_{u_{11}} - 16p_{u_4}p_{u_{12}} - 12p_{u_3}p_{u_{14}} \tag{2}$$

The given formula 2 shows that the dependence of the total risk on the probability of the events for the studied ISCIO is described by a quadratic function, which can be investigated analytically to identify extrema and characteristic points.

In addition, additional conditions are imposed on the determination of probabilities p_{u_i} (formulas (3) – (4)).

$$p_{u_i} \in [0,1]. \tag{3}$$

$$P = \sum_{i=1}^{14} p_{u_i} = 1. \tag{4}$$

The function described by formula (1), and taking into account the conditions described by formulas (3) – (4), refers to linear programming (optimization) problems that can be solved using the Lagrange method.

Formulas (5) – (6) describe the Lagrange function and derivatives with respect to all parameters.

$$L = R_{u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14} - \lambda P. \tag{5}$$

$$\begin{cases} \dfrac{\partial L}{\partial p_{u_i}} = 0 \\ \dfrac{\partial L}{\partial \lambda} = 0 \end{cases}. \tag{6}$$

According to the results of calculations using formulas (5) and (6), we obtain that $\lambda = 0$, all $p_{u_i} = 0$, except $p_{u_3} = 1$ and $p_{u_4} = 1$. It is obvious that they cannot be equal to unity at the same time because constraint (4) is not satisfied. If we substitute the probabilities separately, we get at $p_{u_3} = 1$ the risk value $R = 48$, and at $p_{u_4} = 1$, respectively $R = 55$. It is obvious that the distribution at which only $p_{u_4} = 1$ will be the maximum point in the risk assessment. This is logical, since this component corresponds to the largest level of losses, and in other distributions there is a negative part (probability), which reduces the total risk value in the assessment.

From another point of view, it is also necessary to determine the conditions under which the risk value will be minimal. Since the calculations performed using the Lagrange method do not provide an unambiguous answer to this question, the search for minimal risk values must be carried out at the extreme points of the threat probability distribution values, i.e., alternately zeroing all p_{u_i} except one.

Using the Lagrange method, it was calculated that the maximum risk values become at events $i = 3$ and $i = 4$. By searching through the extreme points, we obtain the result according to which the minimum risk value will be at the event $i = 14$. In other cases, the risk value will grow faster than the negative part (probability) in order to level the increase in the main risk.

Figure 3 shows a graph of the risk assessment value depending on the possible threat probability distributions, according to attack profiles. Due to the multicomponent nature of the probability vector used as an input to the risk assessment function, we will use the segment between two points as the definition domain. It is given as a convex linear combination of the end vectors with coefficients α and $(1-\alpha)$, where $0 \le \alpha \le 1$. Changing $R(p_{u_i})$, which depends on the probability vector, on $R(p_{u_i}(\alpha))$, which depends on one parameter α, to be able to display multidimensional space on a plane. Formula (7) shows the transformation of a multicomponent vector into a single-parameter form.

$$p_{u_i}(\alpha) = \alpha \cdot p_{u_i}^1 + (1-\alpha) \cdot p_{u_i}^2, \tag{7}$$

where $p_{u_i}^1$ – the value of the probability vector corresponding to the minimum of the risk function;

$p_{u_i}^2$ – the value of the probability vector corresponding to the minimum of the risk function.

The graph has a generalized form. The extreme points are of greatest interest for the analysis of the obtained formula (2); therefore, they were chosen as the vectors of the ends of the segment. Accordingly, the maximum and minimum risk are reflected by the extreme points of the graph. The graph of the standard risk assessment corresponds to a linear dependence on the probability distribution without taking into account the structure of the connections between threats. The graph of the refined assessment corresponds to a polynomial risk formula that takes into account the interdependence and compatibility of threat implementations and the probability distribution in the attack profile.

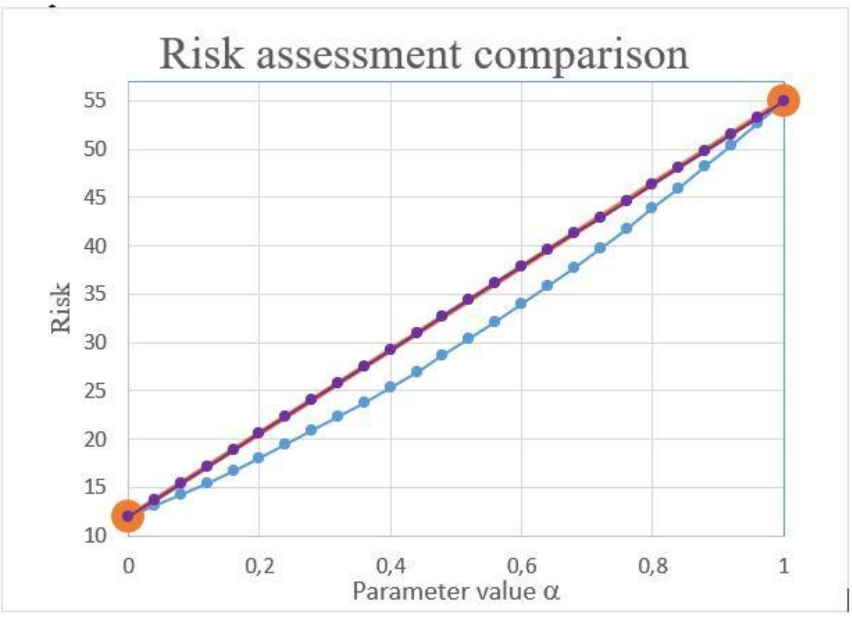

Figure 3 – Comparison of risk assessment values

Assume that the distribution of threats is uniform. In this case, the probabilities are calculated using formulas (8) – (9).

$$p_{u_i} = \frac{1}{14}. \tag{8}$$

$$p_{\{u_i,u_j\}} = \frac{1}{14}\cdot\frac{1}{14}. \tag{9}$$

The calculation of the total risk carried out within the framework of the proposed method is carried out according to formula (10).

$$\begin{aligned} R_{clarified(u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14)} &= \frac{1}{14}\sum_{i=1}^{14} V_{u_i} - \\ -\frac{1}{14^2}(V_{\{u6,u4\}} + V_{\{u3,u4\}} + V_{\{u2,u3\}} + V_{\{u1,u4\}} + V_{\{u4,u8\}} + V_{\{u4,u9\}} + \\ +V_{\{u10,u4\}} + V_{\{u5,u4\}} + V_{\{u4,u13\}} + V_{\{u7,u4\}} + V_{\{u4,u12\}} + V_{\{u3,u11\}} + \\ +V_{\{u3,u14\}}) = \frac{383}{14} - \frac{328}{196} \approx 25,68 \end{aligned}. \tag{10}$$

The total risk without taking into account the structure of connections in the system is calculated using formula (11).

$$\begin{aligned} R_{s\tan dart(u1,u2,u3,u4,u5,u6,u7,u8,u9,u10,u11,u12,u13,u14)} = \sum_{i=1}^{14} R_{ui} = \\ = \frac{1}{14}\sum_{i=1}^{14} V_{ui} = \frac{383}{14} = 27,36 \end{aligned}. \tag{11}$$

The calculation results obtained by formulas (10) and (11) allow for a comparative analysis of risk values calculated using the generalized risk assessment method and the simplified linear assessment procedure, and to assess the level of risk refinement using formula (12).

$$\varepsilon_R = \frac{R_s - R_c}{R_s} \cdot 100\% \approx \frac{27,36 - 25,68}{27,36} \cdot 100\% \approx 6,1\% . \qquad (12)$$

The obtained result indicates that the practical application of the proposed risk assessment method compared to the simplified linear assessment allowed to reduce the overall risk for the studied corporate infrastructure information system by approximately 6.1%.

An additional clarification is that in the calculations the terms associated with individual risks R_i, are reduced with subtraction on glues, because, taking into account the structures of some threats u_i, they are part of the threat u_j, i.e. they do not carry additional information for risk assessment, because they are already taken into account in the risks R_i.

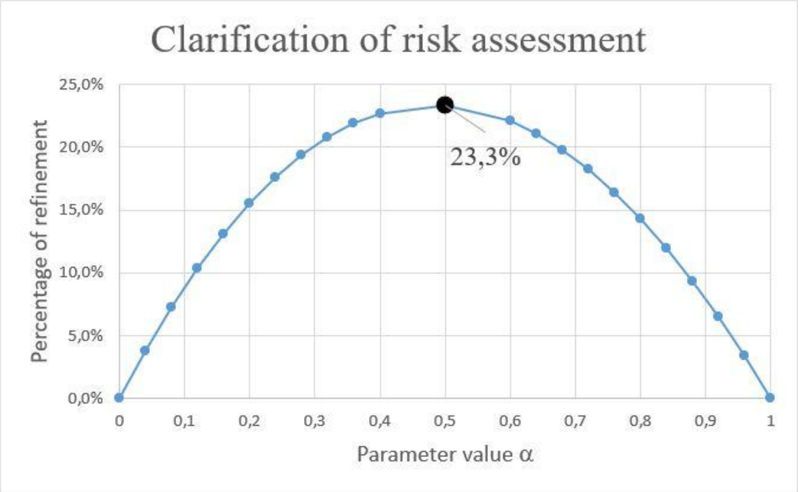

Figure 4 – Clarification of the relative correction in the risk assessment depending on the probability distribution of the occurrence of threats

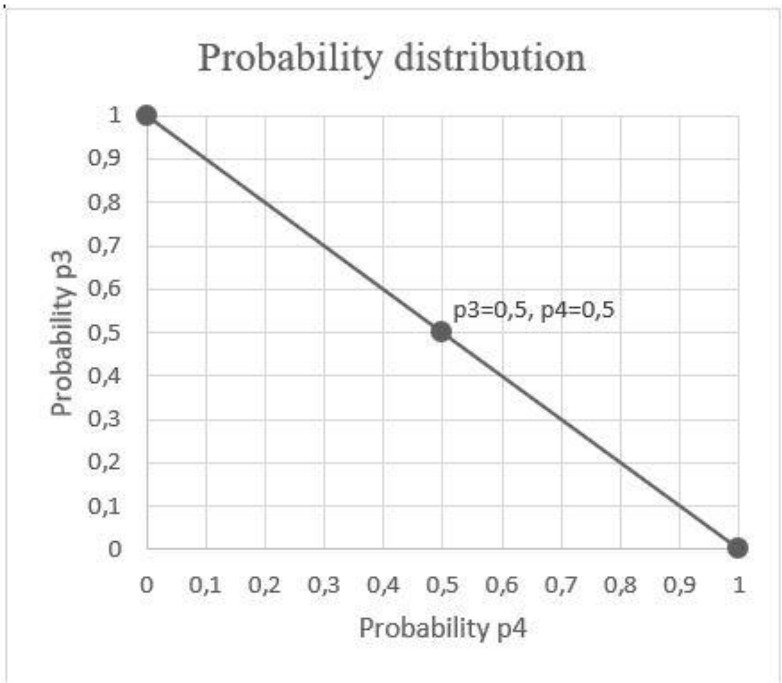

Figure 5 – Interval between probabilities at which the maximum relative refinement of the standard risk assessment changes

Figure 5 shows a graph of the function that describes the dependence of the value of the relative correction for “glues” in the risk assessment formula on the parameter α, which, as in the case of risk assessment comparison, is introduced to calculate the reduction of a multicomponent probability distribution vector to a single-parameter task on a segment, the ends of which are the probability distribution of threats for a certain attack profile. The graph shows that the value of the relative correction varies from zero (in this case $\alpha = 0$, in probability distributions $p_{u_3} = 1$ and $p_{u_4} = 0$), then increases to a maximum level of $\varepsilon_R = 23{,}3\%$ at $\alpha = 0{,}5$ and decreases to zero. At $\alpha = 1$, the value of the relative correction corresponds to the probability distribution of $p_{u_3} = 0$ and $p_{u_4} = 1$.

Due to the degeneracy of the fourteen-dimensional distribution to a two-dimensional one, it is possible to depict the transition segment from one minimum correction value to another. The corresponding probability distributions are shown in Figure 5 and correspond to the extreme points. The points $p_{u_3} = 0{,}5$ and $p_{u_4} = 0{,}5$ correspond to the maximum of the function in Figure 4.

The obtained result confirms the universality, efficiency and practical significance of the proposed risk assessment method, and allows us to provide additional recommendations for the formation of requirements for input data. In the case when individual simplexes are parts of another simplex (threats are nested in other threats), they can be ignored when assessing the risk. Initial nesting checks can be carried out already at the stage of forming the incidence matrix.

Conclusions. The application of the developed method for calculating the assessment and analysis of risks from threats and vulnerabilities for the information system of a corporate infrastructure object is presented. The main stages of the procedure for identifying and analyzing the compatibility of vulnerabilities with each other and the threat system as a whole are presented.

The algorithm for constructing a simplex complex and a structural tree with subsequent analysis of the relationship between vulnerabilities on the example of an information system of a corporate infrastructure object is considered and applied.

It is proven that some vulnerabilities that are often not detected when collecting data about the system can have a significant, albeit indirect, impact on the reliability, availability and integrity of the system as a whole.

A structural classification of existing threats in the information system of a corporate infrastructure object is carried out based on Q-analysis.

Based on the analysis, a risk assessment was performed for the given information system of a corporate infrastructure object and the corresponding method was applied to real data. A Bayesian risk assessment formula was constructed taking into account the influence of the studied complex structure of the threat system.

Application of the proposed risk assessment method for the studied practical example showed that, in comparison with the simplified linear assessment, the overall risk for the information system of the corporate infrastructure object is reduced from 0 till 23.3% depending on the distribution of threats and the attack profile.

REFERENCES

[1] “NIST 800-30 і Структура оцінки ризиків”, *Lazarus Alliance, Inc*. [Online]. Available:https://lazarusalliance.com/uk/nist-800-30-and-the-risk-assessment-framework. Accessed on: Mar 04, 2025.

[2] Ye. Zhyvylo, and V. Kuz, “Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences”, *Theoretical and Applied Cybersecurity: scientific journal*, vol. 5, no. 2, pp. 68-80, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.2.280377.

[3] V. Mokhor, S. Gonchar, and O. Dybach, “Methods for the Total Risk Assessment of Cybersecurity of Critical Infrastructure Facilities”, *Nuclear and Radiation Safety*, no. 2 (82), pp. 4-8, 2019. doi: https://doi.org/10.32918/nrs.2019.2(82).01.

[4] S. Toliupa, S. Buchyk, O. Kulinich, and O. Buchyk1, “Protection of state management of critical infrastructure objects under the influence of cyber attacks”, *Information and Communication Technologies, Electronic Engineering*, vol. 2, no. 2, pp. 33-41, 2022. doi: https://doi.org/10.23939/ictee2022.02.033.

[5] V. Polutsyhanova, and S. Smyrnov, “Methodology for constructing basic q-analysis metrics and their application”, *Systems Research and Information Technology*, no. 3, pp. 76-88, 2019. doi: https://doi.org/10.20535/srit.2308-8893.2019.3.07.

[6] V. Polutsyhanova, “System construction of cybersecurity vulnerabilities with Q-analysis”, *Theoretical and Applied Cybersecurity*, vol. 5, no. 1, pp. 52-55, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.1.285430.

[7] V. Polutsyhanova, “Vulnerability classification using Q-analysis”, *Theoretical and Applied Cybersecurity*, vol. 5, no. 2, pp. 56-61, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.2.285431.

[8] V. Polutsyhanova, “Risk assessment method based on analysis of the structure of threats and vulnerabilities in cybersystems”, PhD thesis, ES PTI, NTUU “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine, 2024.

The article was received 07.05.2025.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] “NIST 800-30 і Структура оцінки ризиків”, *Lazarus Alliance, Inc.* [Електронний ресурс]. Доступно: https://lazarusalliance.com/uk/nist-800-30-and-the-risk-assessment-framework. Дата звернення: 04.03.2025.

[2] Ye. Zhyvylo, and V. Kuz, “Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences”, *Theoretical and Applied Cybersecurity: scientific journal*, vol. 5, no. 2, pp. 68-80, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.2.280377.

[3] В. Мохор, С. Гончар, та О. Дибач, “Методи загального оцінювання ризиків кібербезпеки об’єктів критичної інфраструктури”, *Ядерна та радіаційна безпека*, № 2 (82), с. 4-8, 2019. doi: https://doi.org/10.32918/nrs.2019.2(82).01.

[4] S. Toliupa, S. Buchyk, O. Kulinich, and O. Buchyk1, “Protection of state management of critical infrastructure objects under the influence of cyber attacks”, *Інформаційні та комунікаційні технології, електронна інженерія*, т. 2, № 2, с. 33-41, 2022. doi: https://doi.org/10.23939/ictee2022.02.033.

[5] В. Полуциганова, та С. Смирнов, “Методологія побудови основних метрик q-аналізу та їх застосування”, Системні дослідження та інформаційні технології, № 3, с. 76-88, 2019. doi: https://doi.org/10.20535/srit.2308-8893.2019.3.07.

[6] V. Polutsyhanova, “System construction of cybersecurity vulnerabilities with Q-analysis”, *Theoretical and Applied Cybersecurity*, vol. 5, no. 1, pp. 52-55, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.1.285430.

[7] V. Polutsyhanova, “Vulnerability classification using Q-analysis”, *Theoretical and Applied Cybersecurity*, vol. 5, no. 2, pp. 56-61, 2023. doi: https://doi.org/10.20535/tacs.2664-29132023.2.285431.

[8] В. Полуциганова, “Метод оцінки ризику на основі аналізу структури зв’язків загроз та вразливостей у кіберсистемах”, дис. д-ра філософії, НН ФТІ, НТУУ “КПІ імені Ігоря Сікорського”, Київ, Україна, 2024 с.

СЕРГІЙ СМИРНОВ,
ВІКТОРІЯ ПОЛУЦИГАНОВА

ОЦІНЮВАННЯ ТА АНАЛІЗ РИЗИКІВ ДЛЯ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ СИСТЕМИ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ

У статті представлено методологічний підхід до оцінювання ризиків, пов'язаних із загрозами та вразливостями інформаційної системи об'єкта корпоративної інфраструктури (ІСКІО). Актуальність теми зумовлена зростанням кількості та складності кіберзагроз, а також потребою у точніших інструментах оцінювання ризиків, що враховують структуру взаємозалежностей між потенційними вразливостями та атаками.

Основною проблемою дослідження є недостатня точність традиційних методів оцінювання ризиків, які не відображають складної структури загроз у комплексних системах. Для вирішення цієї проблеми автори використовують розширений Q-аналіз, який дозволяє враховувати структурні зв'язки між загрозами та вразливостями з метою формування більш деталізованої моделі ризиків.

Метою дослідження є практичне застосування теоретичних основ розширеного Q-аналізу на прикладі з використанням реальних експертних даних. У рамках дослідження сформовано матрицю інцидентності між загрозами та вразливостями, побудовано симплекс-комплекс і структурне дерево для візуалізації взаємозв'язків. На основі цих моделей виконано розрахунки величин втрат для кожної загрози та їх комбінацій (так званих «склеювань»). Із застосуванням методів оптимізації, зокрема методу Лагранжа, визначено умови досягнення максимуму та мінімуму ризику, проаналізовано поведінку функції ризику залежно від розподілу ймовірностей та побудовано порівняльні графіки.

Результати свідчать, що запропонована методика дозволяє зменшити загальний ризик до 23,3% у порівнянні з лінійними моделями, залежно від профілю загроз. Отримані висновки підтверджують практичну цінність підходу та підвищують точність оцінювання ризиків для підтримки прийняття рішень у сфері кіберзахисту складних інформаційних систем.

Ключові слова: оцінювання ризику, інфраструктура, Q-аналіз, інформаційна система.

Smirnov Sergey, candidate of science (Physics and Mathematics), senior researcher, associate professor, Educational and Research Institute of Physics and Technology, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. ORCID 0000-0003-4190-5204, sergsmr@gmail.com.

Polutsyhanova Viktoriia, PhD, assistant, Educational and Research Institute of Physics and Technology, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," Kyiv, Ukraine. ORCID 0000-0002-9729-5786, medvika@ukr.net.

Смирнов Сергій Анатолійович, кандидат фізико-математичних наук, старший науковий співробітник, доцент, Навчально-науковий Фізико-технічний інститут, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

Полуциганова Вікторія Ігорівна, PhD, асистент, Навчально-науковий Фізико-технічний інститут, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.