# Information Security Risk Management using Cognitive Modeling

Svitlana Shevchenko[1], Yuliia Zhdanova[1], Halina Shevchenko[2], Olena Nehodenko[3], and Svitlana Spasiteleva[1]

[1] Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine
[2] The National University of Ostroh Academy, 2 Seminarska str., Ostroh, 35800, Ukraine
[3] State University of Telecommunications, 7 Solomyanska str., Kyiv, 03110, Ukraine

**Abstract**

Making decisions by an individual is an element of managing any process in society; therefore, theories of cognitive science are applicable in various fields, including information and cyber security systems. This study proposes the development of a cognitive model of "danger-risk" in the process of managing information risks in information and cyber security systems. Based on the analysis of scientific literature, the concepts of "cognitive modeling" and "cognitive map" are defined. The views of scholars on methods for creating cognitive maps and mechanisms for simulating problem situations are presented. The main tasks addressed within cognitive analysis and modeling are outlined, and the advantages and disadvantages of cognitive models are identified. In the second part of the study, the main stages of developing the cognitive model of "danger-risk" in the field of information and cyber security are considered: identification of complex situations and issues, construction of a cognitive map, modeling and verification of model adequacy, and dynamic situation analysis. A theoretical model of "danger-risk" is developed, and its elements are highlighted. A list of risk management concepts in information security is characterized, and cause-and-effect relationships between them are justified using SWOT analysis. As an example, for a specific information asset (a database), threats and vulnerabilities are identified, and the risk level for each connection is calculated as the product of the probability of each threat's realization and the probability of corresponding damages. The model of cognitive risk maps in information security is represented in a static form as an oriented graph, with a subsequent selection of methods for handling these risks.

**Keywords**

Information security risks, information security system, cyber system, cyber risks, cognitive modeling, cognitive danger-risk model, SWOT analysis.

## 1. Introduction

The informational component is one of the most valuable assets for any organization. Information can be stolen, distorted, become inaccessible, and lose its integrity and confidentiality, all of which result in significant material and reputational losses for the enterprise. Every 39 seconds, a new attack occurs somewhere on the internet, costing trillions of dollars annually [1]. Every company should have experts with practical knowledge of information confidentiality, availability, and integrity safeguards [2]. Therefore, there is a constant focus on implementing protective software and upgrading security technologies for research in the field of security [3–4].

As a methodology for managing an enterprise's information security system, a risk-oriented approach is chosen. The

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); halyna.shevchenko@oa.edu.ua (H. Shevchenko); negodenkoav@i.ua (O. Nehodenko); s.spasitielieva@kubg.edu.ua (S. Spasiteleva)
ORCID: 0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0002-8717-4358 (H. Shevchenko); 0000-0001-6645-1566 (O. Nehodenko); 0000-0003-4993-6355 (S. Spasiteleva)

formation of the existing spectrum of information risks during the activities of a specific organization, the minimization of these risks, and their transfer or avoidance while continuously monitoring the risk situation, is a crucial step in the organization's information security system [5].

On the other hand, the implementation and application of the information security risk management methodology require significant efforts and resources in constant process monitoring. This prompts researchers and information security specialists to seek optimal and effective risk management practices.

Information and cyber security is a complex system with a lack of sufficient analytical data for uncertainty removal and forecasting. Therefore, most approaches rely on expert assessment, fuzzy logic theory, and graph theory [6].

Modeling various scenarios in information and cyber security is the tool that allows risk analysis for management and future prediction. This is evident from the extensive research in this direction. In scientific development [7], researchers used stochastic modeling methods to determine the possibilities of applying various risk theories to study the nature and properties of cyber risks. In research [8], risk behavior models are proposed based on the use of the theory of complex variable function. The risk-oriented approach in cyber security protection systems is described in [9], where different cognitive risk models, methods of their analysis, and processing are defined. Mathematical models of reflexive risks, the structure and set of which are determined by typical "attack/defense" scenario developments, are developed in [10, 11]. Qualitative assessment using SWOT analysis is conducted in scientific works [12, 13].

Information and cyber security are closely intertwined with human activity, allowing the integration of cognitive science theories into information protection-related developments. Cognitive science, or cognitology, is an interdisciplinary scientific direction that combines the theory of cognition, cognitive psychology, neurophysiology, cognitive linguistics, and artificial intelligence theory.

As claimed by researchers [14], cognitive modeling holds significant prospects and possibilities in the field of cyber security and can become a powerful tool for exploring different scenarios and making decisions by responsible individuals. All of the above allows for the identification of the research purpose, which is the development of a cognitive model of "danger-risk" based on SWOT analysis in information security risk management.

## 2. Cognitive Modeling

One of the contemporary trends in scientific research is the cognitive approach, which is being implemented in studies across various fields. "The cognitive approach aims to understand how people decode information about reality and organize it to make decisions or solve pressing tasks" [15, p. 198]. Notable scientific works in this regard include research by R. Axelrod [16], B. Kosko [17], F. Roberts [18], Y. Milyavsky [19], and others.

Cognitive modeling involves representing a complex problem situation of a given system in a simplified form, typically in a graphical format. Scientific developments in this field began with the formation of cognitive maps, as proposed by Robert Axelrod (1976) for the analysis and decision-making in social sciences. Axelrod's cognitive maps are iconic oriented graphs, with the principle of operation as follows: the concepts used by the decision-maker are presented as nodes, and the cause-and-effect relationships between these concepts are represented as edges. A positive connection between node A and node B means that an increase in A leads to an increase in B, whereas a negative connection between A and B implies that an increase in A results in a decrease in B [17]. This depiction is presented in Fig. 1, and the matrix form in Fig. 2. The matrix is square, and at the intersection of the row elements $C_i$ and column elements $C_j$, a +1 is placed if there is an edge ($C_i$, $C_j$) with a "+" sign, −1 if there is an edge ($C_i$, $C_j$) with a "–" sign, and 0 if there is no edge ($C_i$, $C_j$).

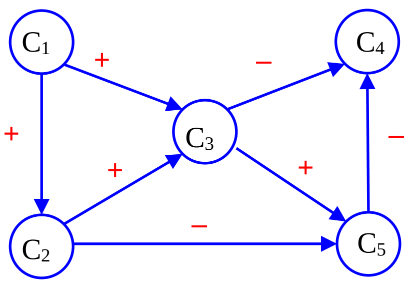


**Figure 1**: Cognitive map

$$
\begin{array}{c}
 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5
\end{array}
\begin{array}{c}
\begin{array}{ccccc} C_1 & C_2 & C_3 & C_4 & C_5 \end{array} \\
\begin{pmatrix}
0 & +1 & +1 & 0 & 0 \\
0 & 0 & +1 & 0 & -1 \\
0 & 0 & 0 & -1 & +1 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0
\end{pmatrix}
\end{array}
$$

**Figure 2**: Cognitive map in matrix form

Later, researcher Bart Kosko [17] introduced fuzzy cognitive maps, initially developed as a means to explain decision-making processes in politics, and they now form the foundation of cognitive modeling.

## 2.1. Fuzzy Cognitive Map

The cognitive Situation Map is a fundamental representation of the static and dynamic aspects of a complex system in cognitive modeling. As evidenced by scientific research [16–25], cognitive maps are used for both statistical and dynamic analysis of systems (Table 1).

**Table 1**
The use of fuzzy cognitive maps for system studies

| Static | Dynamic |
|---|---|
| Evaluation of the influence of one factor on others | Generation of scenario development in time |
| Overall situation stability | Analysis of scenario development in time |
| Search for structural changes to obtain stable structures | Consequences of influence on system elements or changes like relationships |

A fuzzy cognitive map by Kosko, in addition to cause-and-effect relationships between factors, also denotes their weight on the edges, with values ranging from [–1; 1], thus determining the level of this influence (Fig. 3).

Today, there are various modifications of cognitive maps, including iconic cognitive maps, fuzzy cognitive maps by Kosko, modified fuzzy cognitive maps by Kosko, fuzzy relational cognitive maps, and others. They are all characterized by different interpretations of edge weights and factor values within the cognitive map. Deterministic and non-deterministic cognitive maps are distinguished, and each of them includes iconic, quantitative, qualitative, and fuzzy cognitive maps [19].

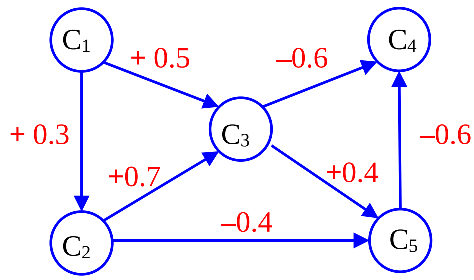


**Figure 3**: Fuzzy cognitive map

The adjacency matrix of such an oriented graph is as follows (Fig. 4):

$$
\begin{array}{c}
 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \\ C_5
\end{array}
\begin{array}{c}
\begin{array}{ccccc} C_1 & C_2 & C_3 & C_4 & C_5 \end{array} \\
\begin{pmatrix}
0 & +0{,}3 & +0{,}5 & 0 & 0 \\
0 & 0 & +0{,}7 & 0 & -0{,}4 \\
0 & 0 & 0 & -0{,}6 & +0{,}4 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -0{,}6 & 0
\end{pmatrix}
\end{array}
$$

**Figure 4**: Fuzzy cognitive map in matrix form

It's worth noting that cognitive maps do not provide an exact description of the entire system under study but rather reflect the subjective assessments of experts in a given situation. They serve as a model for representing their knowledge. As a drawback, it should also be mentioned that solving cognitive modeling tasks can be challenging, hence the need for software resources, especially with a library of information assets, their vulnerabilities, and threats for more effective monitoring of information security risks.

## 2.2. Stages of Cognitive Modeling

In scientific literature, various stages, schemes, and mechanisms for modeling a problem situation based on a cognitive approach are proposed. We favor the process of construction outlined in the study [19] and presented in Table 2.

**Table 2**
Stages of modeling a problem situation based on a cognitive approach

| Stage | Actions |
|---|---|
| I. Identification of a complex situation or problem | 1) Formulating the research task and objectives;<br>2) Collecting analytical data related to the problem;<br>3) Defining the main characteristics of the problem situation;<br>4) Identifying influencing factors and fundamental societal laws;<br>5) Determining possible requirements, conditions, and constraints in the given situation;<br>6) Identifying key stakeholders related to the situation and the factors they may influence. |
| II. Constructing a cognitive map | 1) Expert work in identifying factors characterizing the problem situation;<br>2) Grouping factors into blocks and presenting indicators for analysis within the situation;<br>3) Determining relationships between factors: positive "+," negative "–," influence level ranging from -1 to +1 or strong, moderate, weak;<br>4) Constructing an oriented graph. |
| III. Modeling and checking the adequacy of the model | 1) Defining initial conditions in the given situation;<br>2) Setting target directions (increase, decrease) and the strength of the direction; |
| IV. Dynamic analysis of the situation | 3) Choosing actions to influence the situation;<br>4) Defining indicators characterizing the development of the situation;<br>5) Comparing results with past data.<br>Generating "IF... THEN..." type scenarios. |

# 3. Developing a Cognitive Model of "Danger-Risk" based on Conducting a SWOT Analysis of Information Security Risks

The information and cyber security system is a complex framework with a large amount of unstructured data. The application of cognitive analysis allows these data to be presented in a form that provides a combination of different scenarios and solutions.

Within the "threat-risk" model, it is considered that the existence of threats results in the formation of a set of risks to the object, each of which is characterized by the probability of its realization and a certain harm when the threat exploits the vulnerability of the object.

Let's denote $\bar{G}_1 = \{C, \bar{E}, W\}$ an oriented graph, where

$C = \{C_i\}$ represents the set of factors (concepts); in this case, it's the set of possible threats to a given information asset, vulnerabilities that the threat can exploit, and possible consequences in case of the threat's realization.

$\bar{E} = \{e_i\}$ represents the set of edges reflecting cause-and-effect relationships between factors.

$W = \{w_i\}$ represents the set of weights on edges (strength of influence); in this case, $w_i = r_i = p_i q_i$, $0 \leq w_i \leq 1$, where $r_i$ is the degree of risk, $p_i$ is the probability of each threat's realization, and $q_i$ is the probability of corresponding damages, calculated based on expert assessment and using SWOT analysis.

Researchers propose scenario modeling in three main directions:

- Development of the situation occurs independently of the system (self-contained).
- Development of the situation occurs through programmed actions (direct task).
- Synthesis of a set of influences that allowed achieving a specific change in the situation (inverse task).

## 3.1. Quality Risk Analysis using SWOT Analysis

Constructing a cognitive map can be done by a single individual making decisions based solely on their experience, or by a group of experts using information provided by the organization or through a questionnaire. Additionally, it is possible to obtain results by openly conducting surveys and polling participants in the process.

In our research, to build a fuzzy cognitive map, we propose identifying the system and influence weights using SWOT analysis after conducting brainstorming.

SWOT analysis is a research procedure whose idea revolves around a comprehensive description of strengths, weaknesses, opportunities, and threats when developing an organizational strategy. SWOT analysis serves as the initial stage of organizational strategy planning, serving as a starting point for a more in-depth examination of issues related to information security risks. It is relatively straightforward to use and does not require experienced experts to conduct it. A more detailed procedure for conducting a SWOT analysis for managing information and cyber security risks is described in works [12–13].

As an example, let's select an information asset, such as the organization's database, and conduct the identification of threats and vulnerabilities for this asset (Table 3).

We will determine the risk level for each factor (Table 4) using the probability multiplication formula for independent events.

**Table 3**
Vulnerabilities and threats of an information asset

| Availability | | Integrity | | Confidentiality | |
|---|---|---|---|---|---|
| Vulnerability | Threat | Vulnerability | Threat | Vulnerability | Threat |
| Missing database protection | Physical damage to databases (intentional and unintentional) | Lack of database protection | Physical damage to databases (intentional and unintentional) | Lack of database protection | Unauthorized access (direct and remote) |
| Weak encryption | Data theft and falsification | Weak passwords for data access | Data theft and falsification | Weak encryption | Data theft and falsification |
| Lack of uninterrupted power sources | Equipment failure and loss of unsaved data | Absence of access rights segregation | Data modification (unintentional or intentional) | Absence of two-factor authentication | Unauthorized access (direct and remote) |
| Missing regular data backup system | Data loss | Missing regular data backup system | Data loss | Absence of access rights segregation | Unauthorized access (direct and remote) |

**Table 4**
Determination of the degree of risk for each factor

| Factors | Description | $p_i$ | $q_i$ | $r_i$ |
|---|---|---|---|---|
| $C_1$ | Physical damage to databases (intentional and unintentional) | 0.165 | 0.246 | 0.04059 |
| $C_2$ | Data theft and falsification | 0.165 | 0.216 | 0.03564 |
| $C_3$ | Data modification (unintentional or intentional) | 0.250 | 0.520 | 0.13000 |
| $C_4$ | Unauthorized access (direct and remote) | 0.165 | 0.320 | 0.05280 |
| $C_5$ | Equipment failure and loss of unsaved data | 0.165 | 0.410 | 0.06765 |
| $C_6$ | Data loss | 0.090 | 0.384 | 0.03456 |
| $C_7$ | Lack of a regular data backup system | 0.200 | 0.394 | 0.78800 |
| $C_8$ | Weak passwords for data access | 0.200 | 0.390 | 0.78000 |
| $C_9$ | Lack of uninterrupted power sources | 0.132 | 0.310 | 0.04092 |
| $C_{10}$ | Absence of two-factor authentication | 0.132 | 0.422 | 0.05570 |
| $C_{11}$ | Lack of database protection | 0.072 | 0.338 | 0.02434 |
| $C_{12}$ | Absence of access rights segregation | 0.132 | 0.476 | 0.06283 |
| $C_{13}$ | Weak encryption | 0.132 | 0.376 | 0.04963 |

Using SWOT analysis, the organization's strategy was determined (Table 5) regarding countering threats, taking into account the company's weaknesses (vulnerabilities of the information asset).

The priority threat is the one with the most connections to weaknesses. After the comparison, the priority threat is "Data Loss."

Let's determine the degree of impact using cognitive maps. After identifying information characterizing the database security, we will construct a matrix of the strength of relationships between the concepts $C_i$ (Table 6).

**Table 5**. Interaction of threats and vulnerabilities

| | Vulnerabilities | | | | | | |
|---|---|---|---|---|---|---|---|
| Threats | W1 | W2 | W3 | W4 | W5 | W6 | W7 |
| T1 | – | – | + | – | + | + | – |
| T2 | – | + | – | + | – | + | + |
| T3 | – | + | – | + | – | + | – |
| T4 | – | + | – | + | + | + | – |
| T5 | + | – | + | – | – | – | – |
| T6 | + | + | + | + | – | + | + |

**Table 6**.
Cognitive matrix of the strength of connections between concepts in the cognitive map

| | $C_1$ | $C_2$ | $C_3$ | $C_4$ | $C_5$ | $C_6$ | $C_7$ | $C_8$ | $C_9$ | $C_{10}$ | $C_{11}$ | $C_{12}$ | $C_{13}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0017 | 0 | 0.0010 | 0.0026 | 0 |
| $C_2$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0278 | 0 | 0.0020 | 0 | 0.0022 | 0.0018 |
| $C_3$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.1014 | 0 | 0.0072 | 0 | 0.0082 | 0 |
| $C_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0421 | 0 | 0.0029 | 0.0013 | 0.0033 | 0 |
| $C_5$ | 0 | 0 | 0 | 0 | 0 | 0 | 0.0533 | 0 | 0.0028 | 0 | 0 | 0 | 0 |
| $C_6$ | 0 | 0 | 0 | 0 | 0 | 0 | 0.0272 | 0.0270 | 0.0014 | 0.0019 | 0 | 0.0022 | 0.0018 |
| $C_7$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_8$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_9$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{10}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{11}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{12}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $C_{13}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

As a characteristic of the cognitive map, scientists suggest finding its density (cluster coefficient) using the formula

$$d = \frac{n}{N^2},$$

where $n$ is the total number of connections, $N$ is the total number of concepts.

Therefore,

$$d = \frac{22}{13^2} = 0{,}13.$$

It's obvious that the more connections, the higher the density, and thus, more opportunities for change. In our case, the density is a moderate value. This is expected due to the choice of a small number of factors (threats and vulnerabilities).

## 3.2. Fuzzy Cognitive Map for Situational Analysis of Information Security Risks

Based on the identification of the problem situation, specifically for the information asset that requires protection, vulnerabilities, and threats were identified, relationships between them were designed, and their influence strength was determined. We will construct a cognitive map in the form of a weighted directed graph (Fig. 5).

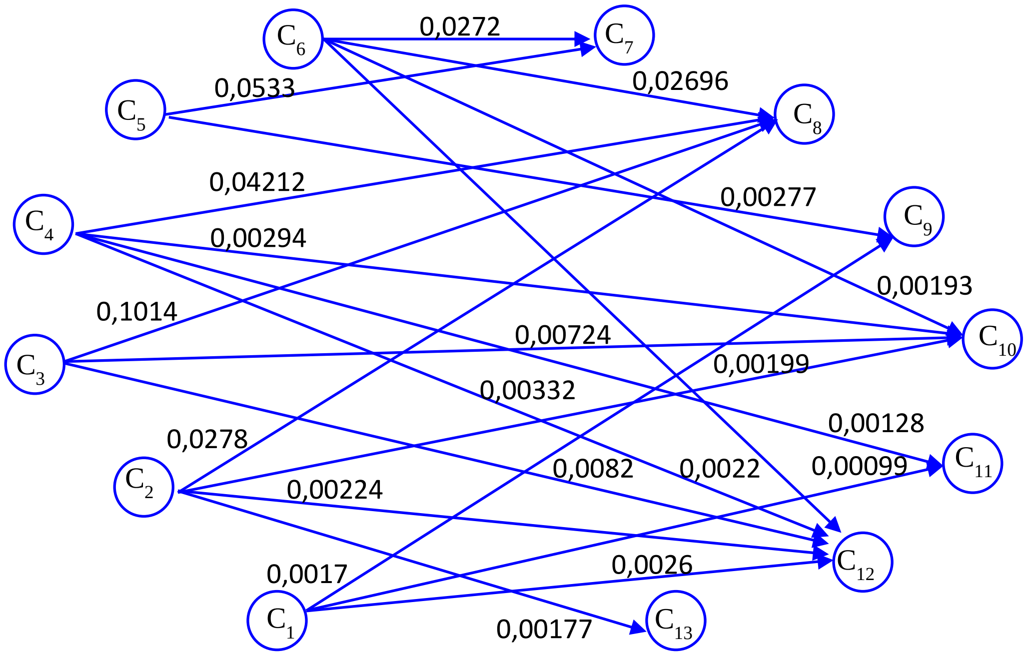


**Figure 5**: Cognitive map for information security risk management.

## 4. Conclusions

This graph represents a scenario modeling the situation's development without influencing the process. By comparing the obtained risk level with the standard outlined in the organization's Security Policy, the leader makes decisions regarding the treatment of these risks: minimize, transfer, prevent, or accept. In the next stage, various scenario modeling is carried out depending on the actions chosen by the leader and the company.

The proposed methodical approach to information and cyber security risk management using modeling and SWOT analysis allows for prioritizing actions to ensure the confidentiality, integrity, and availability of information.

## 5. Acknowledgments

This research was tested in the educational process of Boris Grinchenko Kyiv University with students majoring in Cybersecurity and Information Protection.

## References


[1] What Businesses Need to Know about Cybersecurity in 2023. https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/what-businesses-need-to-know-about-cybersecurity-in-2023

[2] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.

[3] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th Int. Conf. on Problems of Infocommun., Sci. and Technol. (PICST) (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518.

[4] M. Vladymyrenko, et al., Analysis of Implementation Results of the Distributed Access Control System. in: 2019 IEEE Int. Sci.-Practical Conf. Problems of Infocommun., Sci. and Technol. (2019). doi: 10.1109/picst47496.2019.9061376.

[5] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th Int. Conf. on "Mathematics. Information Technologies. Education:" Modern Machine Learning Technologies and Data Science 2386 (2019) 222–233.

[6] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th Int. Conf. on Problems of Infocommun., Sci. and Technol. (2021). doi: 10.1109/picst54195.2021.9772181.

[7] M. Eling, J. Wirfs, What Are the Actual Costs of Cyber Risk Events? European J. of Operational Research 272(3) (2019) 1109–1119. URL: https://www.sciencedirect.com/science/article/abs/pii/S037722171830626X

[8] V. Mokhor, S. Honchar, Research of Validity of Presentation of Risks by Vectors in the Euclidean Space, Electronic Modeling 41 (2019) 73–84. https://www.emodel.org.ua/images/em/41-4/Mokhor.pdf

[9] O. Arkhipov, Introduction to the Theory of Risks: Information Risks, Nat. Acad. SBU, Kyiv (2015).

[10] O. Arkhypov, Application of a Risk-based Approach using Reflexive Risk Models in Building Information Security Systems, in: 1st Int. Workshop CITRisk (2020) 130–143. https://ela.kpi.ua/bitstream/123456789/41515/1/CITRisk_Risk-Based%20 Approach.pdf

[11] O. Arkhypov, Y. Arkhypova, J. Krejčí, Adaptation of a Risk-based Approach to the Tasks of Building and Functioning of Information Security Systems, in: 2nd Int. Workshop on Computational & Information Technologies for Risk-Informed Systems 3101 (2021) 83–92.

[12] H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309-317.

[13] S. Shevchenko, Y. Zhdanova, K. Kravchuk, Information Protection Model based on Information Security Risk Assessment for Small and Medium-Sized Business. Cybersecur. Edu., Sci., Technique 2(14) (2021) 158–175. doi: 10.28925/2663-4023.2021.14.158175.

[14] V. Veksler, et al., Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior, Frontiers in Psychology 11 (2020).

[15] V. Shapar, Modern Explanatory Psychological Dictionary, Kharkiv, Prapor (2007).

[16] R. Axelrod, The Structure of Decision: Cognitive Maps of Political Elites. Princeton University Press (1976).

[17] B. Kosko, Fuzzy Cognitive Maps. Int. J. Man-Machine Studies 24 (1986) 65–75.

[18] F. Roberts, Discrete Mathematical Models with Applications to Social, Biological, and Environmental Problems. Englewood Cliffs, Prentice-Hall (1976).

[19] Y.L. Miliavskyi Identification and Control of Complex Systems based on Cognitive Maps Impulse Processes Models, Thesis for doctoral degree National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (2021). https://ela.kpi.ua/handle/123456789/43830

[20] O Hordei, B Patsai, The Use of Modeling in the Learning Process in the Formation of the Necessary Competencies, Economic Analysis 32(2) (2022) 62–72.

[21] V. Kazymyr, A. Posadska Researching the Cognitive Maps by Simulation Modeling Technical Sciences and Technologies 1(7) (2021) 98–105.
[22] O. Babak, O. Tatarinov, Cognitive Modelling of the State of an Object based on a Thought Experiment, Control Systems and Computers 5-6 (2021) 35–44.
[23] T. Prokopenko, Complex Model of strategic Management of Organizing-Technical System in Conditions of the Uncertainty Bulletin of Lviv State University of Life Safety 7 (2018) 55–60.
[24] O. Salieva, Y. Yaremchuk, Development of a Cognitive Model for Analyzing the Impact of Threats on the Level of Computer Network Security, Registration, Storage and Processing of Data 21(4) (2019) 28–39.
[25] I. Yaldin, Cognitive Modelling in Forecasting Scenarios of the Strategy of Stable Development of an Integrated Structure of Business, The Problems of Economy 4 (2011) 142–150.