# Fuzzy cognitive mapping as a scenario approach for information security risk analysis

Svitlana Shevchenko[1,*,†], Yuliia Zhdanova[1,†], Olha Kryvytska[2,†], Halyna Shevchenko[2,†] and Svitlana Spasiteleva[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

[2] *National University of Ostroh Academy, 2 Seminarska str., 35800 Ostroh, Ukraine*

## Abstract

To avoid damaging their reputation in the field of information and cyber security, companies tend to keep incidents and attacks that affect their operations under wraps. Insufficient information prevents a more accurate risk assessment; as statistical analysis requires a large volume of historical data. Thus, a quantitative-qualitative approach to risk analysis in cybersecurity, particularly scenario analysis, is most commonly applied. The scenario approach to information security risk assessment is a powerful tool for proactive information protection. Forecasting potential consequences, rather than responding to them, allows companies to avoid significant and unnecessary costs. Scenario analysis enables the modeling of various cyberattack situations, risk assessment, and management of information security risks. This research is dedicated to the application of the "What-if" scenario analysis method for assessing information security risks. The paper presents a detailed description of this methodology and the stages of the process. The advantages and disadvantages of the scenario approach and its potential use in information security risk management are identified. The scenarios are modeled using fuzzy cognitive maps. An influence matrix was developed, and the key concepts were calculated. Potential scenarios were generated using the Mental Modeler software tool.

## Keywords

information security risk, information security system, cybersystem, cyber risk, cognitive modeling, scenario analysis, fuzzy cognitive map

## 1. Introduction

Information in today's world has become one of the most valuable assets of an enterprise. Its loss, leakage, or destruction can lead to negative consequences for the organization, ranging from financial losses to reputational damage, potentially even resulting in bankruptcy. Cybercriminals, who continually develop and refine increasingly sophisticated attack methods, often count on such outcomes. Organizations frequently do not know where an attack may come from or even if it is happening. Just one asset vulnerability can grant an attacker access to the entire company's information assets. Therefore, information protection is a priority task for every organization.

A sufficient number of methodologies dedicated to information protection systems have been developed, but this field cannot remain static. Therefore, the improvement of methods and the development of new ones remain and will continue to be a relevant issue. At present, a risk-based approach is highlighted as a key system for information protection [1]. Implementing it allows for the following:

- Timely identification of potential vulnerabilities in the information system and the development of effective protection measures in advance.
- Focusing efforts and resources on the most valuable and critically important assets through the prioritization of risks, starting with the highest ones.
- Avoiding unnecessary expenses by identifying appropriate means of information protection.
- Ensuring maximum compliance with the necessary legal requirements in the information and cybersecurity system.
- Enhancing the company's reputation strategies and customer trust by ensuring a high level of confidentiality and integrity of their data.

The complexity and multifaceted nature of the elements in the information and cybersecurity system complicates the process of predicting information protection needs. A

*CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine*

[*] Corresponding author.

[†] These authors contributed equally.

s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); olha.kryvytska@oa.edu.ua (O. Kryvytska); halyna.shevchenko@oa.edu.ua (H. Shevchenko); s.spasitielieva@kubg.edu.ua (S. Spasiteleva)

0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0002-0844-3362 (O. Kryvytska); 0000-0002-8717-4358 (H. Shevchenko); 0000-0003-4993-6355 (S. Spasiteleva)

productive and effective method for research and forecasting in this area is modeling possible situations and consequences. This approach allows for the analysis of potential threats, risk assessment, and the development of effective protection strategies. Numerous studies in this field support this claim.

In the scientific work [2], researchers propose a model for information security risk assessment based on decision theory, fuzzy logic, and fault tree analysis. In the study [3], a cognitive model is described, which enables the investigation of the impact of potential threats on the security level of a critical infrastructure object, and scenario modeling of this impact is conducted. A risk-based approach in the cybersecurity protection system is described in [4], where the model of decision-making delays in information protection and its effect on security risks is explored using logistic equations and Hutchinson's equation. "Attacker-defender" situations are modeled using cognitive modeling in [5]. The adaptation of SWOT analysis for assessing information and cybersecurity risks is carried out in scientific articles [6, 7]. The authors of [8] present a method for assessing information security risks based on scenarios involving advanced persistent threat attacks. The researchers build risk scenarios for high-level vulnerabilities, analyze the likelihood of each risk, and make decisions regarding both technical and business risks. In the study [9], a model of cognitive maps for information security risks is presented in a static form as an oriented graph, with further selection of methods for handling these risks.

Thus, experts' interest in information security risk management promotes the introduction of mathematical methods in this field [10, 11]. We agree with the authors who consider cognitive modeling appropriate for use in information protection systems, as risk assessment is characterized by a high degree of uncertainty, difficulty in strict formalization, and subjective nature.

Cognitive modeling, as researchers argue in [5], is an invaluable tool for identifying vulnerabilities in security systems and developing measures to eliminate them. It provides decision-makers with a valuable tool for analyzing different scenarios and making informed decisions. The complexity of applying this method requires practical developments and the use of information and communication technologies. The above allows us to highlight the goal of this paper—to study the application of fuzzy cognitive maps in constructing various dynamic scenarios using the Mental Modeler software.

## 2. Cognitive modeling: Fuzzy cognitive map and execution stages

Cognitive modeling is based on the construction of a fuzzy cognitive map, which is an oriented graph where the vertices (concepts) represent system variables, and the weighted edges reflect the strength of one concept's influence on another [12]. As is known, Kosko's fuzzy cognitive map is a weighted directed graph in which the weights on the edges have values within the range of [-1; 1], thus determining the level of influence one factor (concept) has on another. Using a cognitive map, both static and dynamic analyses can be performed (see Fig. 1).

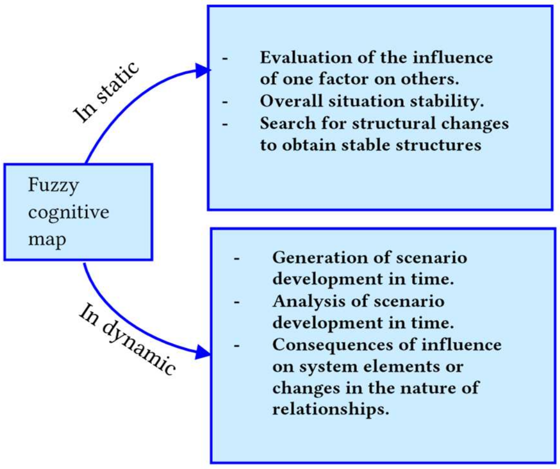
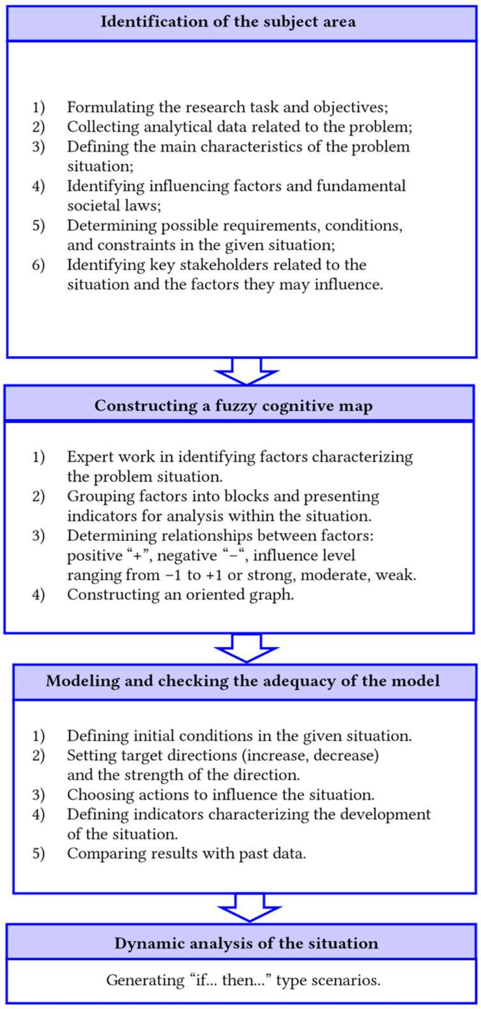

Fuzzy cognitive map
In static
In dynamic
- Evaluation of the influence of one factor on others.
- Overall situation stability.
- Search for structural changes to obtain stable structures
- Generation of scenario development in time.
- Analysis of scenario development in time.
- Consequences of influence on system elements or changes in the nature of relationships.

**Figure 1**: Using a fuzzy cognitive map for modeling

Fig. 2 illustrates the modeling mechanism based on cognitive modeling.


Identification of the subject area

1) Formulating the research task and objectives;
2) Collecting analytical data related to the problem;
3) Defining the main characteristics of the problem situation;
4) Identifying influencing factors and fundamental societal laws;
5) Determining possible requirements, conditions, and constraints in the given situation;
6) Identifying key stakeholders related to the situation and the factors they may influence.

Constructing a fuzzy cognitive map

1) Expert work in identifying factors characterizing the problem situation.
2) Grouping factors into blocks and presenting indicators for analysis within the situation.
3) Determining relationships between factors: positive "+", negative "–", influence level ranging from −1 to +1 or strong, moderate, weak.
4) Constructing an oriented graph.

Modeling and checking the adequacy of the model

1) Defining initial conditions in the given situation.
2) Setting target directions (increase, decrease) and the strength of the direction.
3) Choosing actions to influence the situation.
4) Defining indicators characterizing the development of the situation.
5) Comparing results with past data.

Dynamic analysis of the situation

Generating "if… then…" type scenarios.

**Figure 2**: Modeling mechanism based on cognitive approach

# 3. Scenario modeling based on cognitive modeling

## 3.1. Task formulation

1. Define the Structure of the Fuzzy Cognitive Map [8].
2. Let represent a directed graph, $\bar{G} = \{C, \bar{E}, W\}$,where $C = \{C_i\}$—is the set of factors (concepts); in our case, this is the set of possible threats to a specific information asset, vulnerabilities that the threat can exploit, and the possible consequences of threat realization; $\bar{E} = \{e_i\}$ is the set of edges representing causal relationships between factors.
3. $W = \{w_i\}$ is the set of edge weights (strength of influence). In our case, $w_i = r_i = p_i q_i$, $0 \leq w_i \leq 1$, where $r_i$ being the risk level, $p_i$ is the probability of each threat's realization; $q_i$ is the probability of corresponding losses. These values are calculated based on expert assessments and using SWOT analysis.
4. Characterize the Strength of Influence Between Each Pair of Concepts.
5. This is done using the risk level and qualitative expert evaluations. Experts assess the likelihood of each threat and the impact it would have on the information asset, which contributes to determining the strength of influence between concepts.
6. Build the Model.
7. Construct a weighted directed graph based on the fuzzy cognitive map for evaluating information security risks. Each edge in the graph is assigned a weight corresponding to the calculated risk level, thus representing the impact one concept (e.g., a threat or vulnerability) has on another.
8. Identify Critical Risks.
9. Identify the risks with the highest degree of influence, as they pose the greatest threat. These critical risks should be the focus of the analysis and security measures.
10. Model Scenarios.
11. Using the Mental Modeler software, simulate scenarios to analyze the impact of the most significant concepts. This enables the exploration of how different risk factors interact and affect the overall security posture of the information asset.

## 3.2. Building the fuzzy cognitive map as a graph and matrix

Once the structure is defined, construct the fuzzy cognitive map as a weighted directed graph. Each node represents a concept (such as a threat or vulnerability), and the edges between them represent the causal relationships. The weights on the edges quantify the strength of these relationships. Additionally, the graph can be represented as an adjacency matrix, where each element denotes the weight of the edge from concept to concept. This matrix form is useful for further analysis, including determining the most influential nodes (critical risks) and simulating the dynamic behavior of the system under different scenarios. Building a Fuzzy Cognitive Map is a flexible process that can involve various numbers of participants and utilize different information sources. One person may create a map based on personal experience, while a group of experts can develop it based on data collected from the organization or obtained through surveys. Additionally, all participants can be involved in the process to achieve a more objective picture. In our research, we propose using SWOT analysis to identify the system and influence weights during a brainstorming session, following the methods described in studies [6, 7, 9].

As a sample, we will highlight an information asset, such as the organization's database, and conduct the identification of threats and vulnerabilities associated with this asset (see Table 1).

**Table 1**
Vulnerabilities and threats of an information asset

| Availability | | Integrity | | Confidentiality | |
|---|---|---|---|---|---|
| Vulnerability | Threat | Vulnerability | Threat | Vulnerability | Threat |
| Database protection is missing | Physical damage to databases (intentional or unintentional) | Database protection is missing | Physical damage to databases (intentional or unintentional) | Database protection is missing | Unauthorized access (direct and remote |
| Weak cryptographic protection | Theft and data falsification | Weak passwords for data access | Theft and data falsification | Weak cryptographic protection | Theft and data falsification |
| Uninterruptible power supply systems are missing | Equipment failure and loss of unsaved data | Absence of access rights segmentation | Modification of data (intentional or unintentional) | Two-factor authentication is absent | Unauthorized access (direct and remote) |
| The system for regular data backup is absent | Data loss | The system for regular data backup is absent | Data loss | Absence of access rights segmentation | Unauthorized access (direct and remote) |

Let's define the following concepts:

- $C_1$ is physical damage to databases (intentional and unintentional)
- $C_2$ is data theft and falsification
- $C_3$ is data modification (intentional and unintentional)
- $C_4$ is unauthorized access (direct and remote)
- $C_5$ is equipment failure and loss of unsaved data
- $C_6$ is data loss
- $C_7$ is lack of a regular data backup system
- $C_8$ is weak passwords for data access
- $C_9$ is lack of uninterruptible power supplies
- $C_{10}$ is lack of two-factor authentication
- $C_{11}$ is lack of database protection
- $C_{12}$ is lack of access rights segregation
- $C_{13}$ is weak cryptographic protection.

To determine the risk level for each factor (Table 2), we will apply the formula $w_i = r_i = p_i q_i$, $0 \le w_i \le 1$, where $r_i$ is the risk level, $p_i$ is the probability of each threat occurring; $q_i$ is the probability of the corresponding losses.

**Table 2**

Determination of the degree of risk for each factor

| Factors | $p_i$ | $q_i$ | $r_i$ |
|---|---|---|---|
| $C_1$ | 0,165 | 0,246 | 0,04059 |
| $C_2$ | 0,165 | 0,216 | 0,03564 |
| $C_3$ | 0,25 | 0,52 | 0,13 |
| $C_4$ | 0,165 | 0,32 | 0,0528 |
| $C_5$ | 0,165 | 0,41 | 0,06765 |
| $C_6$ | 0,09 | 0,384 | 0,03456 |
| $C_7$ | 0,2 | 0,394 | 0,788 |
| $C_8$ | 0,2 | 0,39 | 0,78 |
| $C_9$ | 0,132 | 0,31 | 0,04092 |
| $C_{10}$ | 0,132 | 0,422 | 0,055704 |
| $C_{11}$ | 0,072 | 0,338 | 0,024336 |
| $C_{12}$ | 0,132 | 0,476 | 0,062832 |
| $C_{13}$ | 0,132 | 0,376 | 0,049632 |

The fuzzy cognitive map modeling will be carried out using the software Mental Modeler [13]. Fig. 3 shows the cause-and-effect relationships between the system elements (concepts), demonstrating how changes in one element can lead to changes in others.

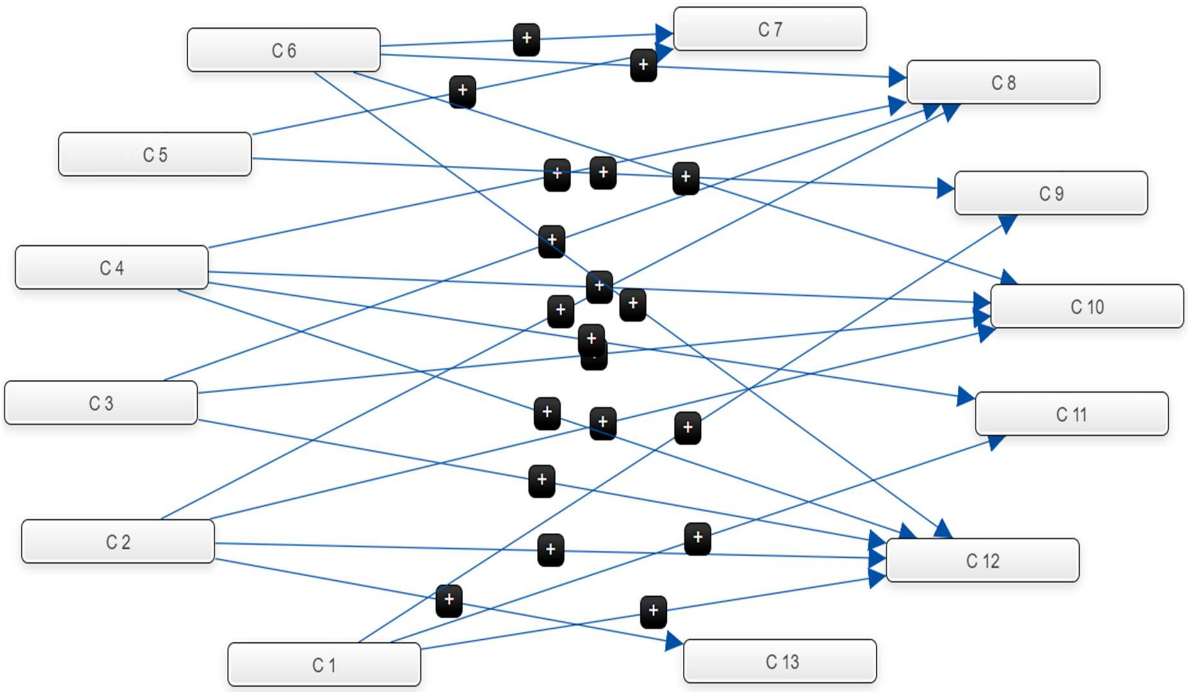


**Figure 3**: Fuzzy Cognitive Map for Information Security Risk Management

As a characteristic of the cognitive map, researchers suggest calculating its density (clustering coefficient) using the following formula:

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

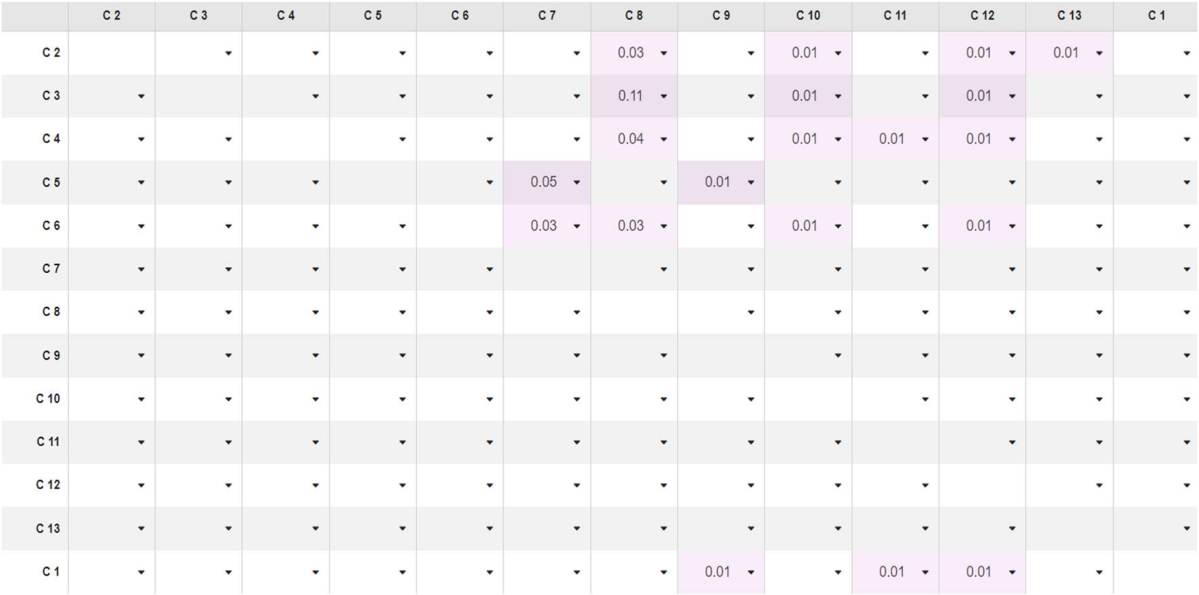
where $n$ is the total number of connections, $N$ is the total number of concepts.

Thus,

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

It is evident that the more connections there are, the higher the density, and therefore, the greater the potential for changes. In our case, the density is moderate. This is reasonable due to the selection of a small number of factors (threats and vulnerabilities).

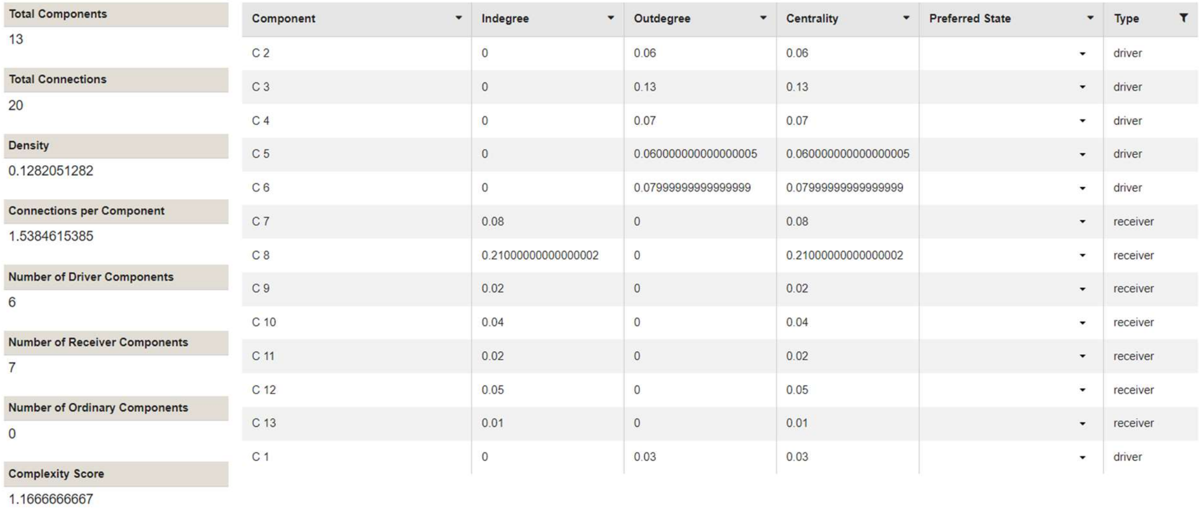
For the systematic analysis of the fuzzy cognitive map, we use the matrix method. This method allows for formalizing knowledge about the system and identifying patterns in its functioning. The results are presented in Fig. 4.



| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C 2 | | | | | | | 0.03 | | 0.01 | | 0.01 | 0.01 | |
| C 3 | | | | | | | 0.11 | | 0.01 | | 0.01 | | |
| C 4 | | | | | | | 0.04 | | 0.01 | 0.01 | 0.01 | | |
| C 5 | | | | | | 0.05 | | 0.01 | | | | | |
| C 6 | | | | | | 0.03 | 0.03 | | 0.01 | | 0.01 | | |
| C 7 | | | | | | | | | | | | | |
| C 8 | | | | | | | | | | | | | |
| C 9 | | | | | | | | | | | | | |
| C 10 | | | | | | | | | | | | | |
| C 11 | | | | | | | | | | | | | |
| C 12 | | | | | | | | | | | | | |
| C 13 | | | | | | | | | | | | | |
| C 1 | | | | | | | | 0.01 | | 0.01 | 0.01 | | |

**Figure 4**: Cognitive Matrix for Information Security Risk Management

To assess the properties of a fuzzy cognitive map, we use the formal apparatus of graph theory, specifically the transitive closure operation, which allows us to build a complete graph of interactions between concepts and calculate various indicators based on it: consonance, dissonance, and the impact of concepts on risk assessment. The results are presented in Fig. 5.



| | |
|---|---|
| Total Components | 13 |
| Total Connections | 20 |
| Density | 0.1282051282 |
| Connections per Component | 1.5384615385 |
| Number of Driver Components | 6 |
| Number of Receiver Components | 7 |
| Number of Ordinary Components | 0 |
| Complexity Score | 1.1666666667 |

| Component | Indegree | Outdegree | Centrality | Preferred State | Type |
|---|---|---|---|---|---|
| C 2 | 0 | 0.06 | 0.06 | | driver |
| C 3 | 0 | 0.13 | 0.13 | | driver |
| C 4 | 0 | 0.07 | 0.07 | | driver |
| C 5 | 0 | 0.060000000000000005 | 0.060000000000000005 | | driver |
| C 6 | 0 | 0.07999999999999999 | 0.07999999999999999 | | driver |
| C 7 | 0.08 | 0 | 0.08 | | receiver |
| C 8 | 0.21000000000000002 | 0 | 0.21000000000000002 | | receiver |
| C 9 | 0.02 | 0 | 0.02 | | receiver |
| C 10 | 0.04 | 0 | 0.04 | | receiver |
| C 11 | 0.02 | 0 | 0.02 | | receiver |
| C 12 | 0.05 | 0 | 0.05 | | receiver |
| C 13 | 0.01 | 0 | 0.01 | | receiver |
| C 1 | 0 | 0.03 | 0.03 | | driver |

**Figure 5**: Key Indicators of the Fuzzy Cognitive Map for Information Security Risk Management

A static analysis for this process has been modeled. By comparing the obtained risk level with the benchmark outlined in the organization's Security Policy, the information security officer decides on risk treatment: to minimize, transfer, mitigate, or accept the risks. At the next stage, various scenario modeling is conducted depending on the measures chosen by the company's management.

## 3.3. Scenario building based on concept changes

The results of the previous matrix indicate that the most significant concepts, i.e., those with the greatest impact on the system, are:

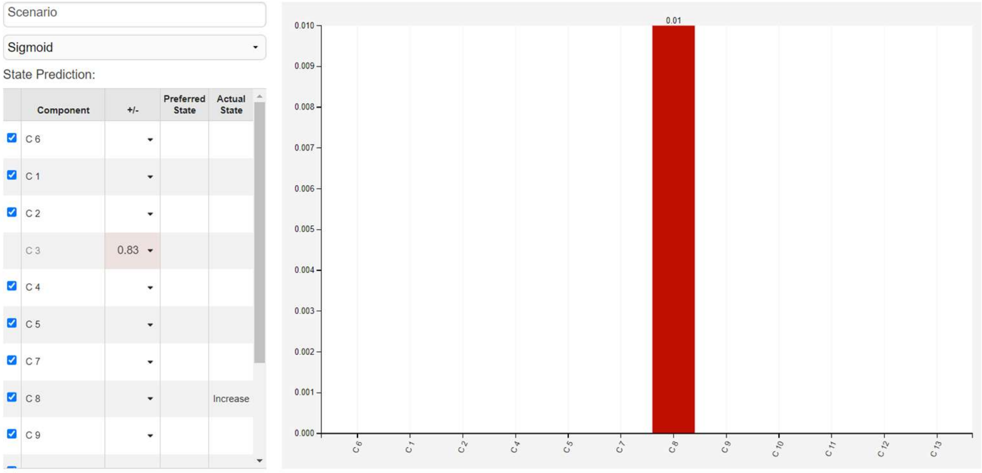
$C_3$ is threat: Data modification (intentional or unintentional).

$C_8$ is vulnerability: Weak passwords for data access.

Let's model situations when these respective values change.

*Situation 1.*

The risk of data modification $C_3$ will have a nearly maximum value if the risk level associated with the vulnerability of weak passwords for data access increases by 0.01 (Fig. 6).



Scenario

Sigmoid

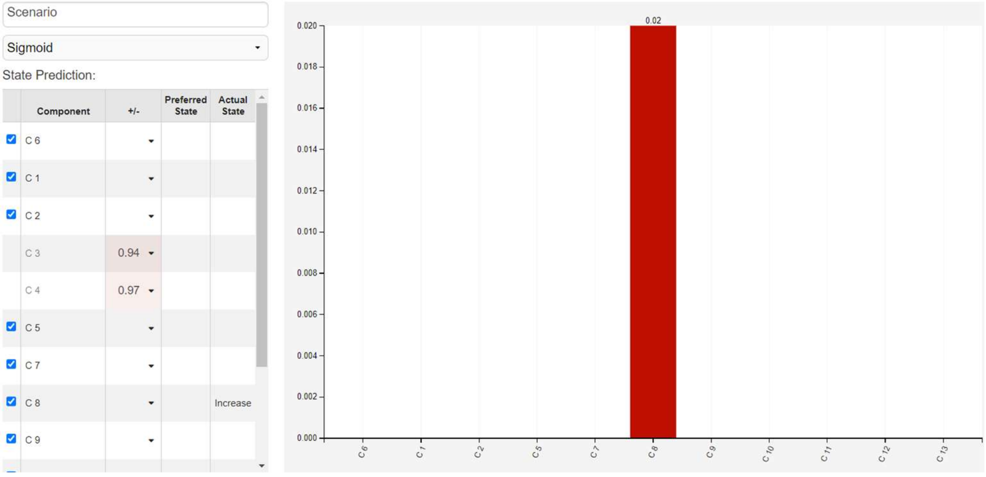
State Prediction:

| | Component | +/- | Preferred State | Actual State |
|---|---|---|---|---|
| ☑ | C 6 | | | |
| ☑ | C 1 | | | |
| ☑ | C 2 | | | |
| | C 3 | 0.83 | | |
| ☑ | C 4 | | | |
| ☑ | C 5 | | | |
| ☑ | C 7 | | | |
| ☑ | C 8 | | | Increase |
| ☑ | C 9 | | | |

**Figure 6**: Simulated Scenario with Changes to $C_3$

*Situation 2.*

The risk of data modification $C_3$ and unauthorized access (both direct and remote) $C_4$ will have a nearly maximum value if the risk level associated with the vulnerability of weak passwords for data access increases by 0.02 (Fig. 7).



Scenario

Sigmoid

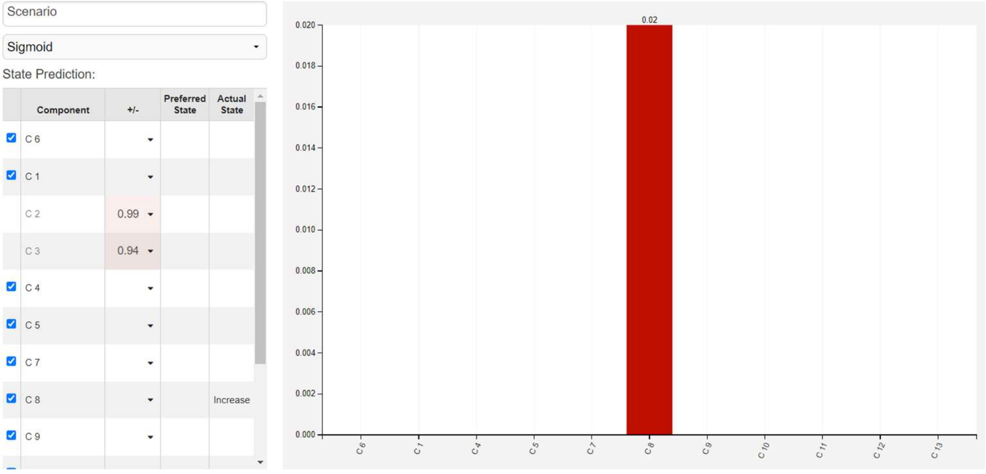
State Prediction:

| | Component | +/- | Preferred State | Actual State |
|---|---|---|---|---|
| ☑ | C 6 | | | |
| ☑ | C 1 | | | |
| ☑ | C 2 | | | |
| | C 3 | 0.94 | | |
| | C 4 | 0.97 | | |
| ☑ | C 5 | | | |
| ☑ | C 7 | | | |
| ☑ | C 8 | | | Increase |
| ☑ | C 9 | | | |

**Figure 7:** Simulated Scenario with Changes in $C_3$ and $C_4$

*Scenario 3.*

The risk of data modification $C_3$ and data theft and falsification $C_2$ will reach near-maximum levels if the risk associated with vulnerabilities such as weak passwords for data access increases by 0.02 (Fig. 8).



Scenario

Sigmoid

State Prediction:

| | Component | +/- | Preferred State | Actual State |
|---|---|---|---|---|
| ☑ | C 6 | | | |
| ☑ | C 1 | | | |
| | C 2 | 0.99 | | |
| | C 3 | 0.94 | | |
| ☑ | C 4 | | | |
| ☑ | C 5 | | | |
| ☑ | C 7 | | | |
| ☑ | C 8 | | | Increase |
| ☑ | C 9 | | | |

**Figure 8:** Simulated Scenario with Changes in $C_3$ and $C_2$

Thus, the use of fuzzy cognitive maps allows for the identification of key concepts that influence system behavior. Through cognitive modeling, it is possible to explore how changes in the values of these factors will affect other system elements. This enables the development of various event scenarios and the evaluation of their consequences. However, one limitation is that cognitive maps are tools for visualizing and structuring expert knowledge but do not replace objective data. They reflect the subjective understanding of experts about the system and can serve as a basis for further analysis. Nevertheless, for effective use of cognitive maps, it is necessary to apply more specialized software that includes a threat library, their sources, a set of asset vulnerabilities, and other tools that allow automating routine operations and providing a more accurate information security risk analysis.

## 4. Conclusions

The proposed methodological approach to information and cyber security risk management through scenario analysis, represented by fuzzy cognitive mapping, enables the identification of key indicators that determine system behavior, the influence of various factors and concepts on the system as a whole, and the identification of the highest risks and priorities for developing measures to ensure confidentiality, integrity, and availability of information.

This approach provides the ability to construct event development scenarios, which supports informed managerial decision-making.

The research results will be useful for information security professionals, managers responsible for data protection, as well as students studying disciplines related to risk management in the field of security.

## References

[1] S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.

[2] A. Gusmão, et al., Cybersecurity Risk Analysis Model Using Fault Tree Analysis and Fuzzy Decision Theory, Int. J. Inf. Manag. 43 (2018). doi: 10.1016/j.ijinfomgt.2018.08.008.

[3] O. Saliyeva, Yu. Yaremchuk, Cognitive Model for Researching the Level of Security of a Critical Infrastructure Object, Security of Information, 26(2) (2020) 64–73.

[4] V. Kononovich, et al., Influence of Delays Decision Action for Information Protection on Information Security Risks, Ukrainian Sci. J. Inf. Secur. 20(1) (2014) 83–91.

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

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

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

[8] X. Ban, X. Tong, A Scenario-based Information Security Risk Evaluation Method, Int. J. Secur. Appl. 8 (2014) 21–30. doi: 10.14257/ijsia.2014.8.5.03.

[9] S. Shevchenko, et al., Information Security Risk Management using Cognitive Modeling, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 297–305.

[10] S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 318–328.

[11] D. Berestov, et al., Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II-2, vol. 3188 (2021) 135–148.

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

[13] S. A. Gray, et al., Using Fuzzy Cognitive Mapping as a Participatory Approach to Analyze Change, Preferred States, and Perceived Resilience of Social-Ecological Systems, Ecology and Society, 20(2) (2015).