http://doi.org/10.35784/iapgos.6719

received: 16.10.2024 | revised: 15.11.2024 | accepted: 09.12.2024 | available online: 21.12.2024

INVESTIGATION OF CHANGES IN THE LEVEL OF NETWORK SECURITY BASED ON A COGNITIVE APPROACH

Olha Saliieva, Yurii Yaremchuk
Vinnytsia National Technical University, Department of Management and Security of Information Systems, Vinnytsia, Ukraine

Abstract. *A study was conducted on the impact of the most significant threats on the level of network security based on the examination of impulse processes on a fuzzy cognitive map. A topological analysis of the structure of the cognitive map was performed, simplicial complexes were constructed, and their structural vectors were determined. Based on the obtained data, a set of control and target concepts of the fuzzy cognitive map was formed, and the relationships between these concepts within the simplicial complexes were established. Taking this information into account, a study was conducted on the change in the level of computer network security using the propagation of impulses introduced into the control concepts of the fuzzy cognitive map. The results obtained enable an increase in the level of network security by considering the impact of the most significant threats through timely managerial decisions and the implementation of necessary software and technical measures.*

Keywords: threats, network security, computer network, cognitive model, simplicial analysis, impulse process

BADANIE ZMIAN POZIOMU BEZPIECZEŃSTWA SIECI W OPARCIU O PODEJŚCIE KOGNITYWNE

Streszczenie*. Przeprowadzono badanie wpływu najważniejszych zagrożeń na poziom bezpieczeństwa sieci w oparciu o badanie procesów impulsowych na rozmytej mapie kognitywnej. Przeprowadzono analizę topologiczną struktury mapy kognitywnej, skonstruowano układy proste i określono ich wektory strukturalne. Na podstawie uzyskanych danych utworzono zestaw pojęć kontrolnych i docelowych rozmytej mapy kognitywnej oraz ustalono relacje między tymi pojęciami w ramach układów prostych. Biorąc pod uwagę te informacje, przeprowadzono badanie zmiany poziomu bezpieczeństwa sieci komputerowej za pomocą propagacji impulsów wprowadzonych do koncepcji sterowania rozmytej mapy kognitywnej. Uzyskane wyniki umożliwiają zwiększenie poziomu bezpieczeństwa sieci poprzez uwzględnienie wpływu najważniejszych zagrożeń poprzez podejmowanie w odpowiednim czasie decyzji menedżerskich oraz wdrażanie niezbędnego oprogramowania i środków technicznych.*

Słowa kluczowe: zagrożenia, bezpieczeństwo sieci, sieć komputerowa, model kognitywny, analiza uproszczona, proces impulsowy

Introduction

In the modern world, computer networks represent the main driving force of technological progress and facilitate the rapid exchange of information. At the same time, the increasing number of cyber threats and network attacks necessitates effective measures to protect the confidentiality, integrity, and availability of data circulating within information and communication systems. Therefore, the issues related to ensuring the reliable and secure operation of computer networks and enhancing their level of protection are of significant importance.

Modern scientists pay considerable attention to the study of network security. For example, the authors of work [4] analyzed methods and means of protecting computer systems from unauthorized access and information leakage transmitted over communication channels. Work [1] reflects the improvement of the information security model of the computer network through the use of weight coefficients for various types of internal and external network attacks. In [11], an innovative model of ATP attacks based on semi-supervised learning and complex network characteristics is proposed. Article [9] is dedicated to the integration of heterogeneous threat data collected from security and event management systems to reconstruct multi-stage attack scenarios. The authors of work [10] presented a study on the applicability of an improved V-detector algorithm for detecting network intrusions. Work [3] demonstrates a taxonomy of network threats and associated tools for carrying out attacks, and analyzes the impact of current datasets on intrusion detection systems. Based on a deep learning approach, a hierarchical network for detecting malicious traffic at the packet level is proposed in [8]. In work [7], a cognitive model is developed to determine changes in the level of network security, which is based on a constructed fuzzy cognitive map (FCM). A structural analysis of the studied FCM was conducted, which allowed for the identification of the most significant network threats; however, it did not enable the determination of the connectivity between them or the distinction of the main control and target concepts of the FCM. To address these issues, it is advisable to conduct a simplicial analysis of the studied FCM, and based on the obtained results, perform impulse modeling, which will contribute to determining the changes in the level of network security and other target concepts when disturbances are introduced into the most significant control concepts of the FCM.

1. Study of the structure of the FCM based on simplicial analysis

In the process of conducting simplicial analysis, the cognitive map is considered as a relation between the elements of a set of vertices and a given family of non-empty subsets of these vertices – simplices. A simplex $\sigma_q^{v_i}$ is defined as a set of elements that corresponds to a specific element v_i in relation λ of dimension ρ, and their collection forms a simplicial complex $K_x(Y;\lambda)$: by rows (vertices are encoded as X) or $K_y(X;\lambda^*)$: by columns (vertices are encoded as Y) of the matrix λ. Thus, the sets of vertices and their corresponding simplices form simplicial complexes K. In this case, the problem of studying the connectivity structure of the complex K is reduced to constructing q-equivalence. For this purpose, for each value of dimension $q = 0,1,2,\dots,dimK$ ($dimK$ – the maximum dimension of the complex) it is possible to determine the number of different equivalence classes Q_q. This operation is called the q-analysis of the simplicial complex K, and the vector $\mathrm{Q} = \{\mathrm{Q}_{\mathrm{dimK}},\dots,\mathrm{Q}_1,\mathrm{Q}_0\}$ is the first structural vector of the complex, which allows for establishing the connectivity of the complexes at all levels q [2].

To conduct the simplicial analysis, the FCM [7] will be used, as shown in Figure 1, along with the corresponding adjacency matrix (Table 1).

The values of relationships between the concepts of the studied FCM will be structured by converting the fuzzy values of the elements of the adjacency matrix to the values of "-1", "0", and "1", according to the conditions outlined in Table 2.

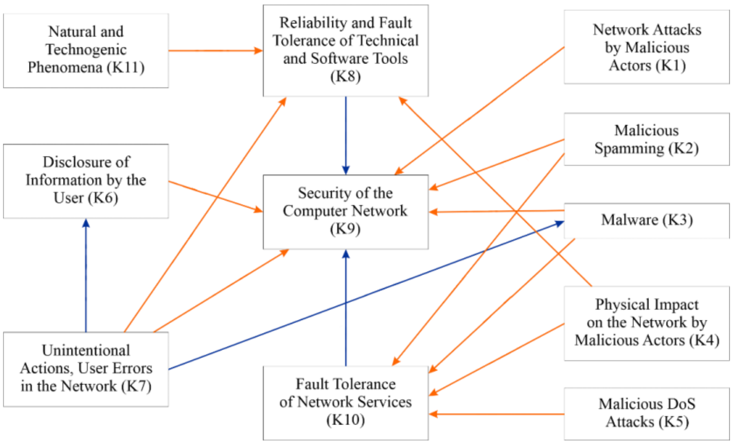

Natural and Technogenic Phenomena (K11)
Reliability and Fault Tolerance of Technical and Software Tools (K8)
Network Attacks by Malicious Actors (K1)
Malicious Spamming (K2)
Disclosure of Information by the User (K6)
Security of the Computer Network (K9)
Malware (K3)
Physical Impact on the Network by Malicious Actors (K4)
Unintentional Actions, User Errors in the Network (K7)
Fault Tolerance of Network Services (K10)
Malicious DoS Attacks (K5)

Fig. 1. FCM of the Study of Changes in the Level of Network Security

Table 1. Adjacency Matrix of the Studied Cognitive Map

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K_1	0	0	0	0	0	0	0	0	-0.85	0	0
K_2	0	0	0	0	0	0	0	0	-0.15	-0.5	0
K_3	0	0	0	0	0	0	0	0	-0.9	-0.61	0
K_4	0	0	0	0	0	0	0	-0.38	0	-0.75	0
K_5	0	0	0	0	0	0	0	0	0	-0.98	0
K_6	0	0	0	0	0	0	0	0	-0.75	0	0
K_7	0	0	0.5	0	0	0.58	0	-0.55	-0.65	0	0
K_8	0	0	0	0	0	0	0	0	0.55	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0
K_{10}	0	0	0	0	0	0	0	0	0.55	0	0
K_{11}	0	0	0	0	0	0	0	0	-0.82	0	0

Table 2. Conditions for Transition from Fuzzy Values of Adjacency Matrix Elements to Values of "-1", "0", "1"

Interval corresponding to the strength of connection between concepts of the adjacency matrix	Assigned new value
[-1; 0)	-1
[0; 0.5)	0
[0.5; 1]	1

Table 3. Ordered Transition Matrix

	y_9	y_{10}	y_8	y_6	y_{11}	y_1	y_2	y_3	y_4	y_5	y_7	$\boldsymbol{q^{(i)}}$
x_7	1	0	1	1	0	0	0	0	0	0	0	**2**
x_2	1	1	0	0	0	0	0	0	0	0	0	**1**
x_3	1	1	0	0	0	0	0	0	0	0	0	**1**
x_4	0	1	1	0	0	0	0	0	0	0	0	**1**
x_1	1	0	0	0	0	0	0	0	0	0	0	**0**
x_5	0	1	0	0	0	0	0	0	0	0	0	**0**
x_6	1	0	0	0	0	0	0	0	0	0	0	**0**
x_8	1	0	0	0	0	0	0	0	0	0	0	**0**
x_{10}	1	0	0	0	0	0	0	0	0	0	0	**0**
x_{11}	0	0	1	0	0	0	0	0	0	0	0	**0**
x_9	0	0	0	0	0	0	0	0	0	0	0	**-1**
$\boldsymbol{q^{(j)}}$	**6**	**3**	**2**	**0**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	

Using the obtained transition matrix, the dimensions of the simplices of the complexes $K_x(Y; \lambda)$ and $K_y(X; \lambda^*)$ will be determined:

$$q = \sum_{i,j=1}^{m} \lambda_{ij} - 1 \qquad (1)$$

According to the rule: $q_1^{(\nu_i)} > q_2^{(\nu_i)} > \cdots > 0 > -1$ the i-*th* rows will be ordered from top to bottom, and the j-*th* columns from left to right.

After completing all the aforementioned actions, an ordered transition matrix will be obtained (Table 3).

The simplicial complexes $K_x(Y, \lambda) = \{\sigma_q^{\nu_i}\}$ and $K_y(X, \lambda^*) = \{\sigma_q^{\nu_j}\}$, are constructed from simplices arranged in descending order of their dimension:

$$K_x(Y, \lambda) = \left\{\sigma_2^{(7)}, \sigma_1^{(2)}, \sigma_1^{(3)}, \sigma_1^{(4)}, \sigma_0^{(1)}, \sigma_0^{(5)}, \sigma_0^{(6)}, \sigma_0^{(8)}, \sigma_0^{(10)}, \sigma_0^{(11)}, \sigma_{-1}^{(9)}\right\},$$

$$K_y(X, \lambda^*) = \left\{\sigma_6^{(9)}, \sigma_3^{(10)}, \sigma_2^{(8)}, \sigma_0^{(6)}, \sigma_{-1}^{(11)}, \sigma_{-1}^{(1)}, \sigma_{-1}^{(2)}, \sigma_{-1}^{(3)}, \sigma_{-1}^{(4)}, \sigma_{-1}^{(5)}, \sigma_{-1}^{(9)}\right\}.$$

Analyzing the ordered transition matrix, structural vectors: $Q_x = \{Q_{dimK}, \dots, Q_q, \dots, Q_1, Q_0\}$ for the complex $K_x(Y, \lambda)$ and $Q_y = \{Q_{dimK}, \dots, Q_q, \dots, Q_1, Q_0\}$ for the complex $K_y(X, \lambda^*)$, will be formed, considering that a simplex constitutes a separate equivalence class if it contains at least one vertex that is not a vertex of any other simplex of higher dimension.

As a result, the following connectivity values are obtained:

1. For $K_x(Y, \lambda)$:
   $q = 2, Q_2 = 1, \{x_7\};$
   $q = 1, Q_1 = 4, \{x_7\}, \{x_2\}, \{x_3\}, \{x_4\};$
   $q = 0, Q_0 = 1, \{all\ except\ x_9\}.$
2. For $K_y(X, \lambda^*)$:
   $q = 6, Q_6 = 1, \{x_9\};$
   $q = 3, Q_3 = 2, \{x_9\}, \{x_{10}\};$
   $q = 2, Q_2 = 3, \{x_9\}, \{x_{10}\}, \{x_8\};$
   $q = 0, Q_0 = 1, \{all\ except\ x_1, x_2, x_3, x_4, x_5, x_7, x_{11}\}.$

Thus, the structural vectors of complexes $K_x(Y, \lambda)$ and $K_y(X, \lambda^*)$ can be represented as: $Q_x = \{1\ 4\ 1\}$ and $Q_y = \{1\ 2\ 3\ 1\}$, respectively.

It should be noted that the studied cognitive map does not have connected concepts. As a result, the simplices of the highest dimension are formed by concepts such as K_7, K_2, K_3 and K_4. Considering the obtained results and the most significant threats to network security identified based on the cognitive approach [7], the validity of which has been confirmed using multiple regression analysis [6], it is advisable to select K_7, K_3 and K_4. Regarding the target concepts, they may include K_9, K_{10} and K_8.

2. Analysis of impulse processes on cognitive map

Utilize the obtained results of the topological analysis of the studied cognitive model to examine a situation that demonstrates how changes in the activation level of the most significant controlling concepts affect the target concepts of the cognitive map in determining the level of security of the computer network. The impulse method of quantitative analysis of the cognitive map (CM) will be applied. This method involves analyzing the system's dynamics due to the propagation of an initial disturbance – an impulse introduced into one or several controlling concepts of the CM. During modeling, the impulse sequentially moves along the arcs of the CM, each of which has a weight that determines the change in the impulse's magnitude as it passes through. Thus, it is necessary to model the impulse propagation processes of disturbances introduced into one or several controlling concepts. This problem will be solved by calculating the transitive closure matrix M [5]:

$$M = E + W + W^2 + \cdots + W^n \qquad (2)$$

where E – unit matrix W – adjacency matrix of the FCM; n – order of matrix W (in our case $n = 11$).

After performing all the necessary calculations for the studied FCM, the transitive closure matrix is obtained (Table 4).

By analyzing the elements of the transitive closure matrix, conclusions can be drawn about the presence of simple impulse effects that define the system's initial state when an external influence impacts one of the elements corresponding to the *i-th* concept of the FCM.

For a simple impulse process with the initial vertex K_i the impulse is calculated as follows:

$$p_j = \{an\ element\ i, j\ of\ the\ matrix\ W^n\} \qquad (3)$$

The value of vertex K_j at discrete time points $t = 0, 1, 2, \ldots, m$ is determined by the formula [5]:

$$V_j(t) = V_j(0) + \{element\ i, j\ of\ the\ matrix\ M\} \qquad (4)$$

Considering the above formula, it can be concluded that a simple impulse process with the input vertex K_1 (network attacks by malicious actors) leads to a reduction in the value of the target concept K_9 (security of the computer network) to 0.85 (under zero initial conditions).

If, under the same initial conditions, vertex K_6 (disclosure of information by the user), is selected as the input vertex, a decrease in network security to 0.75.

It is worth noting that impulse modeling serves as a powerful tool for visualizing the dynamics of the cognitive map and its resilience to external influences. By introducing perturbations into specific vertices of the cognitive network, the evolution of the system over time can be analyzed, observing transitions from one state to another.

At the same time, each impulse reflects the degree of activity or importance of the concepts within the system. Based on the data obtained from the transitive closure matrix, it can be concluded that when an impulse is introduced into the concept K_7 (unintentional actions, user errors in the network), the security of the computer network will decrease to a maximum value (2.01). This indicates that the concept K_7 is key among all the controlling concepts of the studied cognitive model, and thus it requires special attention, as its activation may lead to leaks of confidential information, disruption of network operations, loss of access to information resources, and other negative consequences.

Table 4. The Transitive Closure Matrix of the FCM for determining changes in network security levels

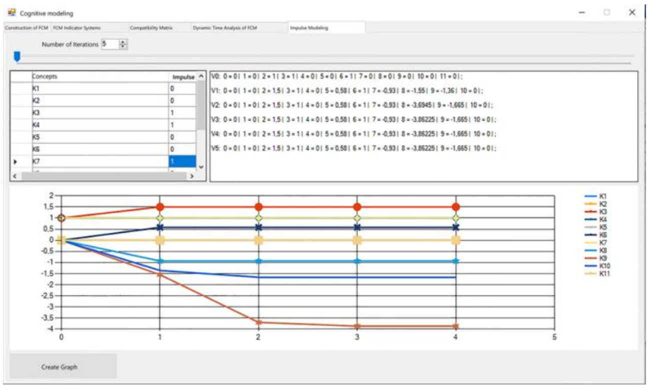
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
K_1	1	0	0	0	0	0	0	0	-0.85	0	0
K_2	0	1	0	0	0	0	0	0	-0.43	-0.5	0
K_3	0	0	1	0	0	0	0	0	-1.24	-0.61	0
K_4	0	0	0	1	0	0	0	-0.38	-0.62	-0.75	0
K_5	0	0	0	0	1	0	0	0	-0.54	-0.98	0
K_6	0	0	0	0	0	1	0	0	-0.75	0	0
K_7	0	0	0.5	0	0	0.58	1	-0.55	-2.01	-0.31	0
K_8	0	0	0	0	0	0	0	1	0.55	0	0
K_9	0	0	0	0	0	0	0	0	1	0	0
K_{10}	0	0	0	0	0	0	0	0	0.55	1	0
K_{11}	0	0	0	0	0	0	0	-0.82	-0.45	0	1

2. Experimental study of the evolutionary development of the system

Particular interest lies in the simultaneous activation of the most significant controlling concepts of the cognitive model for network security identification, as in this case, the security of the computer network is maximally weakened (to 3.86). At the same time, a significant decrease in other target concepts is observed, namely K_8(reliability and fault tolerance of technical and software tools) (to 0.93) and K_{10} (fault tolerance of network services) (to 1.67) (Fig. 2).

Figure 2 primarily reflects the quantitative trends in changes to network security under the influence of the most significant threats. This, in turn, serves to optimize timely comprehensive decision-making, including management, technical, and software aspects, with the aim of enhancing the level of network security.

Thus, the results obtained from the simplicial and impulse analysis of the cognitive model investigating the impact of threats to computer network security will contribute to improving the quality of forecasting and management of network security. They provide an opportunity to make timely decisions to enhance network protection and implement necessary mechanisms for prevention, protection, and access control at appropriate levels of the network infrastructure.



Number of Iterations 5

Concepts	Impulse
K1	0
K2	0
K3	1
K4	1
K5	0
K6	0
K7	1

```
V0: 0 = 0| 1 = 0| 2 = 1| 3 = 1| 4 = 0| 5 = 0| 6 = 1| 7 = 0| 8 = 0| 9 = 0| 10 = 0| 11 = 0|;
V1: 0 = 0| 1 = 0| 2 = 1,5| 3 = 1| 4 = 0| 5 = 0,58| 6 = 1| 7 = -0,93| 8 = -1,55| 9 = -1,36| 10 = 0|;
V2: 0 = 0| 1 = 0| 2 = 1,5| 3 = 1| 4 = 0| 5 = 0,58| 6 = 1| 7 = -0,93| 8 = -3,6945| 9 = -1,665| 10 = 0|;
V3: 0 = 0| 1 = 0| 2 = 1,5| 3 = 1| 4 = 0| 5 = 0,58| 6 = 1| 7 = -0,93| 8 = -3,86225| 9 = -1,665| 10 = 0|;
V4: 0 = 0| 1 = 0| 2 = 1,5| 3 = 1| 4 = 0| 5 = 0,58| 6 = 1| 7 = -0,93| 8 = -3,86225| 9 = -1,665| 10 = 0|;
V5: 0 = 0| 1 = 0| 2 = 1,5| 3 = 1| 4 = 0| 5 = 0,58| 6 = 1| 7 = -0,93| 8 = -3,86225| 9 = -1,665| 10 = 0|;
```

Fig. 2. Evolutionary development of the studied cognitive model upon the introduction of impulses into the most significant concepts

3. Conclusions

This work investigates the impact of threats on the security levels of computer networks. To identify the most significant controlling and target concepts of this cognitive model, a simplicial analysis of its structure was conducted. Specifically, complexes were constructed that include a sequence of simplices ordered by decreasing dimensionality. Structural vectors were determined, which allowed for the identification of absent connected concepts within the studied system and the formation of a set of the most significant controlling concepts: K_7 (unintentional actions, user errors in the network), K_3 (malicious software), K_4 (physical influence on the network from an attacker), as well as a set of target concepts: K_9 (security of the computer network), K_{10} (fault tolerance of network operation), and K_8 (reliability and fault tolerance of technical and software tools).

In addition, the analysis of the constructed transitive closure matrix of the subject area cognitive map allowed us to establish that when an impulse is introduced into the concept K_7 (unintentional actions, user errors in the network), the security of the computer network will decrease to a maximum value (2.01). The evolutionary development of the studied cognitive map when impulses are introduced into the most significant concepts has been visually demonstrated.

The obtained results will contribute to assessing the resilience of the computer network against various threats, developing priorities for responding to network threats, identifying potential vulnerabilities in the network, forecasting information security risks, and, as a result, formulating recommendations and strategies to enhance the security level of the computer network.

References

[1] Apenko N. et al.: Information security of the computer system and network from internal and external attacks. 17th International scientific and practical conference "System analysis and intelligent systems for management". Turkey, Ankara, 2023, 431–434.

[2] Atkin R. H.: Combinatorial Connectivies in Social Systems: An Application of Simplicial Complex Structures to the Study of Large Organisations. Birkhäuser, Basel 1977.

[3] Hindy H. et al.: A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access 8, 2020, 104650–104675 [https://doi.org/10.1109/ACCESS.2020.3000179].

[4] Nahornyi O. V., Zhyrova T. O., Nahornyi V. V.: Problems of information security in computer systems and means and methods of their solution. II International Scientific and Practical Conference. USA, Chicago, 2023, 171–180.

[5] Roberts F. S.: Discrete Mathematical Models with Applications to Social, Biological, and Environmental Problems. Rutgers University, Prentice-Hall Inc., New Jersey 1976.

[6] Saliieva O. V., Yaremchuk Yu. Ye.: Investigation of the reliability of the impact of threats on the level of security of a computer network, determined by scenario modeling based on a cognitive approach. Visnyk of Vinnytsia Politechnical Institute 4, 2020, 98–104 [https://doi.org/10.31649/1997-9266-2020-151-4-98-104].

[7] Saliieva O. V., Yaremchuk Yu. Ye.: Development of a cognitive model for analyzing the impact of threats on the level of security of a computer network. Data Recording, Storage & Processing 21(4), 2019, 28–39 [https://doi.org/10.35681/1560-9189.2019.21.4.199268].

[8] Wang B. et al.: A deep hierarchical network for packet-level malicious traffic detection. IEEE Access 8, 2020, 201728–201740 [https://doi.org/10.1109/ACCESS.2020.3035967].

[9] Zang X. et al.: Attack scenario reconstruction via fusing heterogeneous threat intelligence. Computers & Security 133(20), 2023 [https://doi.org/10.1016/j.cose.2023.103420].

[10] Zhong Y., Chen L.: Research on the application of improved V-detector algorithm in network intrusion detection. Applied Mathematics and Nonlinear Sciences 9(1), 2024, 1–14 [https://doi.org/10.2478/amns.2023.2.00526].

[11] Zimba A. et al.: Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. Future Generation Computer Systems 106, 2020, 501–517 [https://doi.org/10.1016/j.future.2020.01.032].

Ph.D. Olha V. Saliieva
e-mail: salieva8257@gmail.com

Ph.D., associate professor of the Department of Management and Security of Information Systems. Vinnytsia National Technical University.
She is the author of more than 50 publications, including 24 articles in scientific specialized publications, 14 certificates of copyright registration for work, and materials and abstracts of reports at academic conferences. The author's scientific interests are in computer network security, information systems security and cognitive modeling.

https://orcid.org/0000-0003-2388-7321

D.Sc. Eng. Yurii Ye. Yaremchuk
e-mail: yurevyar@vntu.edu.ua

The Doctor of Science in Engineering and the Professor, Head of the Center of IT and Information Security, professor of the Department of Management and Security of Information Systems of Vinnytsia National Technical University.
He is the author of more than 350 publications. The author's scientific interests are in cryptographic and steganographic protection of information, technical protection of information and security of information systems.

https://orcid.org/0000-0002-6303-7703