

STUDY OF THE DYNAMIC VARIATION IN THE SECURITY LEVEL OF AN INFORMATION PROTECTION SYSTEM

Olha Saliieva, Yurii Yaremchuk

Vinnitsia National Technical University, Department of Management and Security of Information Systems, Vinnitsia, Ukraine

Abstract. The rapid informatization of public life has resulted in a sharp increase in the number and complexity of cyberattacks, which inflict substantial material and reputational losses on both individuals and large organizations. Cybercriminals are progressively sophisticating their attack methods, particularly through the application of emergent technologies like artificial intelligence and machine learning. This trend poses a heightened threat to the integrity of information systems and the safeguarding of sensitive data. Consequently, there is a critical need to promptly identify the influence of dominant factors on the security level of information protection systems. To effectively address this problem, the present study investigates the combined effects of key concepts on a fuzzy cognitive map by applying the framework of dynamic causal algebra. The process dynamics in this case are shaped by the introduction of a nominal time, which enables the determination of the process stabilization point and the analysis of the effects of controlling concepts on the target at specific moments. In addition to the adjacency matrix that defines the cognitive map under consideration, the model includes three essential vector parameters: a vertex state vector representing node activity; an input influence vector initiating the activation process; and a threshold vector that filters out minor effects and remains invariant over time. Based on all activated paths, the indirect impacts of conceptual elements on the system's information security level are computed. The analysis of the obtained results is intended to ensure the reliable and stable operation of the security system. Furthermore, it will contribute to developing an effective strategy for preventing cyberattacks.

Keywords: information security, threat, cyberattack, fuzzy cognitive map, dynamic causal algebra

BADANIE DYNAMICZNYCH ZMIAN POZIOMU BEZPIECZEŃSTWA SYSTEMU OCHRONY INFORMACJI

Streszczenie. Szybka informatyzacja życia publicznego spowodowała gwałtowny wzrost liczby i złożoności cyberataków, które powodują znaczne straty materialne i reputacyjne zarówno dla osób fizycznych, jak i dużych organizacji. Cyberprzestępcy stopniowo udoskonalają swoje metody ataku, zwłaszcza poprzez wykorzystanie nowych technologii, takich jak sztuczna inteligencja i uczenie maszynowe. Tendencja ta stanowi zwiększone zagrożenie dla integralności systemów informatycznych i bezpieczeństwa danych wrażliwych. W związku z tym istnieje pilna potrzeba szybkiej identyfikacji wpływu dominujących czynników na poziom bezpieczeństwa systemów ochrony informacji. Aby skutecznie rozwiązać ten problem, w niniejszym badaniu analizuje się łączny wpływ kluczowych pojęć na rozmytą mapę poznawczą poprzez zastosowanie ram dynamicznej algebry przyczynowej. Dynamika procesu w tym przypadku jest kształtowana przez wprowadzenie czasu nominalnego, co umożliwia określenie punktu stabilizacji procesu oraz analizę wpływu pojęć kontrolujących na cel w określonych momentach. Oprócz macierzy sąsiedztwa, która definiuje rozpatrywaną mapę poznawczą, model obejmuje trzy podstawowe parametry wektorowe: wektor stanu wierzchołka reprezentujący aktywność węzła; wektor wpływu wejściowego inicjujący proces aktywacji; oraz wektor progowy, który odfiltruje nieistotne efekty i pozostaje niezmienny w czasie. Na podstawie wszystkich aktywowanych ścieżek obliczane są pośrednie oddziaływania elementów koncepcyjnych na poziom bezpieczeństwa informacji systemu. Analiza uzyskanych wyników ma na celu zapewnienie niezawodnego i stabilnego działania systemu bezpieczeństwa. Ponadto przyczyni się ona do opracowania skutecznej strategii zapobiegania cyberatakowi.

Słowa kluczowe: bezpieczeństwo informacji, zagrożenie, cyberatak, rozmyta mapa poznawcza, dynamiczna algebra przyczynowa

Introduction

With the rapid expansion of digital services and electronic transactions, the volume of confidential information stored in digital form is increasing significantly. Consequently, ensuring robust data protection becomes more complex, which, in turn, elevates the probability of data compromise or modification as a result of cyberattacks. As a result, research in the field of information security is becoming increasingly important, serving as a key factor in ensuring the stability and safety of the digital environment. Researchers worldwide are striving to improve the reliability and resilience of information protection systems (IPS) by analysing their security levels. For instance, the authors of [12] proposed a novel structural model for analysing information security requirements, the fulfilment of which contributes to maintaining the confidentiality, integrity, and availability of information systems and their components. To enhance security, two modelling frameworks have been developed: one aimed at defining security requirements, and another designed to detect insider misuse through the auditing of access logs. Study [5] provides an analysis of various information security challenges encountered by organizations in the course of digital transformation. Emphasis is placed on the critical role of organizational and managerial measures in safeguarding information. In [6], a method for automated forecasting of information security vulnerabilities was proposed, based on a business process model. At the foundational modelling level, the process is represented as a sequence of tasks, and potential vulnerabilities are identified through the analysis of each task's type and label. Based on the TOE (Technology–Organization–Environment) framework, the authors of [8]

analysed the interrelationship between technical, organizational, and environmental aspects affecting the continuity of corporate information security management. In scientific study [4], a comprehensive review was conducted based on the PRISMA methodology to examine the current state of information security in the modern information society. Special emphasis was placed on common threats, mitigation strategies, and optimal approaches to the protection of digital data. Scientific work [15] introduced a comprehensive security architecture, identifying eight principal knowledge domains: intrusion detection, privacy preservation, secure machine learning, cryptographic systems, data transmission service security, malware analysis, decision-making, and security governance. The study [13] involves an analysis of impulse processes on a cognitive map that reflects the dynamics of changes in the security level of a computer network. However, it would be reasonable to expand the scope of the research beyond network security to encompass the overall IPS, which would also include organizational, technical, and software aspects. In academic study [14], a cognitive model was developed and thoroughly examined to assess the level of protection provided by an IPS. The most influential system concepts were identified, and scenario-based modelling was performed to evaluate their impact on the security level of the IPS. However, the scenario analysis did not enable the representation of temporal dynamics in the system's security level. In this context, the application of dynamic causal algebra [9, 16] appears promising, as it facilitates the forecasting of system behaviour at specific points in time. Consequently, studying the impact of the key factors identified by the cognitive approach on the dynamic variation in the security level of the protection system remains a relevant research task.



[illegible]

Table 4. Row-ordered transition matrix

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	$q^{(i)}$
K_6	1	1	1	1	0	0	1	1	0	0	0	5
K_5	1	1	1	1	0	0	0	1	0	0	0	4
K_7	1	1	1	1	0	0	0	1	0	0	0	4
K_{10}	1	0	0	1	0	0	0	1	0	0	0	2
K_4	0	0	0	0	0	0	0	1	0	0	1	1
K_1	0	0	0	0	0	0	0	0	0	0	1	0
K_2	0	0	0	0	0	0	0	0	0	0	1	0
K_3	0	0	0	0	0	0	0	0	0	0	1	0
K_8	0	0	0	0	0	0	0	0	0	0	1	0
K_9	0	0	0	0	0	1	0	0	0	0	0	0
K_{11}	0	0	0	0	0	0	0	0	0	0	0	-1

To determine the dimension of the simplices in the complex $K_X(Y; \lambda)$ the following formula is applied:

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

Subsequently, the i -th rows of the transition matrix are sorted according to the rule: $q_1^{(v_i)} > q_2^{(v_i)} > \dots > 0 > -1$.

After completing the above steps, the ordered transition matrix is obtained (Table 4).

Thus, the simplicial complex $K_X(Y; \lambda)$ will take the following form:

$$K_X(Y; \lambda) = \{ \sigma_q^{(v_i)} \} = \{ \sigma_5^{(6)}, \sigma_4^{(5)}, \sigma_4^{(7)}, \sigma_2^{(10)}, \sigma_1^{(4)}, \sigma_0^{(1)}, \sigma_0^{(2)}, \sigma_0^{(3)}, \sigma_0^{(8)}, \sigma_0^{(9)} \}$$

Since q – connectivity induces an equivalence relation on the simplices of the complex $K_X(Y; \lambda)$, the problem of analysing the connectivity structure of the complex reduces to the study of q -equivalence classes. Accordingly, for each value of the dimension $q = 0, 1, 2, \dots, \dim K$, the number of distinct equivalence classes Q_q is determined as follows:

$$\begin{aligned} q = 5, & \quad Q_5 = 1, \{K_6\} \\ q = 4, & \quad Q_4 = 1, \{K_6, K_5, K_7\} \\ q = 2, & \quad Q_2 = 1, \{K_6, K_5, K_7, K_{10}\} \\ q = 1, & \quad Q_1 = 2, \{K_6, K_5, K_7, K_{10}\}, \{K_4\} \\ q = 0, & \quad Q_0 = 1, \{ \text{all } K_i (i = 1, \dots, 11), \text{ except } K_{11} \} \end{aligned}$$

Therefore, the first structural vector, which reflects the global structure of the complex $K_X(Y; \lambda)$, is as follows:

$$Q_x = \{1 \ 1 \ 1 \ 2 \ 1\}$$

Analysing the concepts of the studied FCM reveals that at levels $q = 2$ and $q = 1$ the connected components $\{K_6, K_5, K_7, K_{10}\}$ emerged. This indicates that introducing a control influence on K_6 , is sufficient to elicit a response from K_5, K_7, K_{10} .

Accordingly, the concepts K_6 and K_4 , which correspond to the simplices of the highest dimensionality, may be selected as control elements for the entire IPS.

2. Analysis of the temporal dynamics of the IPS security level

To ensure the reliability and resilience of an IPS, a proactive approach is often employed, enabling the prediction of potential risks and vulnerabilities of the studied object. Specifically, employing dynamic analysis facilitates tracking changes in the system's security level over time, as well as identifying key trends and functional patterns. For this purpose, an analysis is conducted to determine how the most significant control concepts, identified through topological analysis, influence the subsequent development of the studied system. To represent the system's dynamics, the concept of conditional time is used, according to which the wave of influence propagates through the paths up to the moment t – the influence propagation time. In addition to the adjacency matrix W , the following vector parameters are considered: the state vector of vertices $\Psi(t) = (\Psi_1(t), \Psi_2(t), \dots, \Psi_n(t))$, where $\Psi_i(t)$ is the state

of vertex i (for $i = 1, \dots, n$) at time t ; the input influence vector $(\mu_1(t), \mu_2(t), \dots, \mu_n(t))$, where $\mu_i(t) = \sum_{k=1}^n w_{ki} \cdot \Psi_k(t)$; the threshold vector of vertices $Q = (q_1, \dots, q_n)$, which is time-independent. It should be noted that the threshold values of the vertices are set taking into account the structural analysis of the adjacency matrix and the functional purpose of concepts in the FCM, which allows filtering out zero and mutually compensated influences. In turn, the activity of a vertex is defined by its state, which can take only two values: 0 or 1. The input influence from vertex k is considered in the calculation for vertex i , only if vertex k is active, that is $\Psi_k(t) = 1$ [9, 16].

Thus, the vector of input influences along all activated paths through all active vertices is determined by the following convolution expression:

$$(\mu_1, \dots, \mu_n) = \Psi(t) \times W \quad (1)$$

Considering equation (1) the state vector at time $t + 1$ can be calculated as:

$$\Psi(t + 1) = f_Q(\Psi(t) \times W) = (f_{q_1}(\mu_1), \dots, f_{q_n}(\mu_n)) \quad (2)$$

where $f_{qi}(\mu_i)$ is the threshold function at vertex i , which filters out insignificant influences:

$$f_{qi}(\mu_i) = \begin{cases} 1, & \text{if } |\mu_i| \geq q_i \\ 0, & \text{if } |\mu_i| < q_i \end{cases} \quad (3)$$

At time t the indirect influence along the path P from vertex i to vertex j is determined by the formula:

$$I_p(t) = \prod_{(k,l) \in E(P)} \Psi_k(t) \times w_{kl} \quad (4)$$

where $E(P)$ is the set of edges of path P , $\Psi_k(t)$ is the state of vertex k at time t , and w_{kl} is the weight of edge (k, l) .

Taking into account the impact of all possible pathways from vertex i to vertex j , the total influence $T_{(i,j)}$ is defined as:

$$T_{(i,j)}(t) = \sum_{k \in N^-(j)} \max_{P \in P(i,k,j)} I_p(t) \quad (5)$$

where $N^-(j) = \{k | (k, j) \in E\}$ is the set of vertices directly connected to vertex j , and $P(i, k, j)$ is the set of paths from vertex i to vertex j through vertex k .

Thus, the influence computation consists of two parallel «waves»: the μ – waves, which activates the necessary paths, and the $I - T$ wave, which determines the influence along the activated paths.

Analysis of the adjacency matrix shown in Table 1 shows that for most concepts, the algebraic sum of the input weights is less than one in magnitude, resulting in corresponding threshold values equal to zero. At the same time, for vertex K_{11} , the total input influence exceeds one, which leads to the establishment of an increased threshold value $q_n = 2$. Thus, the vector of vertex thresholds will look like this: $Q = (0; 0; 0; 0; 0; 0; 0; 0; 0; 0; 2)$.

At the initial step of the influence analysis, vertex K_6 – representing the organizational support of information protection – exerts an external influence on K_{11} , the security of the IPS. It is assumed that vertex K_6 is externally activated and remains active throughout the process, i.e., $\Psi_6(t) = 1$ for any time t . Accordingly, the initial state vector of the vertices is given by:

$$\Psi_\Omega(0) = (0; 0; 0; 0; 0; 1; 0; 0; 0; 0; 0; 0)$$

Using equations (1)–(3), we compute the μ -wave, which initiates the activation process of the vertices and corresponding paths:

$$\Psi_{\Omega}(0) \times W_{\Omega} = (0.7; 0.65; -0.9; 0.8; 0; 0; -0.3; 0.7; 0; 0; 0)$$

$$\Psi_{\Omega}(1) = f_T(\Psi_{\Omega}(0) \times W_{\Omega}) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 0)$$

$$\Psi_{\Omega}(1) \times W_{\Omega} = (-0.65; -0.1; 0.5; -0.87; 0; 0.55; -0.3; -0.72; 0; 0; 2.25)$$

$$\Psi_{\Omega}(2) = f_T(\Psi_{\Omega}(1) \times W_{\Omega}) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$$

$$\Psi_{\Omega}(2) \times W_{\Omega} = (-0.65; -0.1; 0.5; -0.87; 0; 0.55; -0.3; -0.72; 0; 0; 2.25)$$

$$\Psi_{\Omega}(3) = f_T(\Psi_{\Omega}(2) \times W_{\Omega}) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$$

Thus, at time $t = 2$, the process stabilizes, because at this step all vertices of the cognitive map become active, as a result of which further multiplication of the state vector by the adjacency matrix does not change the total weighted influences. In addition, applying the activation threshold function to the resulting vector reproduces the same state vector that corresponds to the fixed point of the iterative process. Thus, at $t = 2$, the system reaches a stable equilibrium state, and further iterations do not lead to a change in the structure of active vertices.

According to formulas (4) and (5), the influence along the activated paths is computed. Since there are six paths from K_6 to K_{11} : one path through K_2 , one through K_4 , four through K_8 and two paths each through K_1 and K_3 , the set N^- is defined as:

$$N^- = \{K_1, K_2, K_3, K_4, K_8\}$$

The indirect influences along specific paths at various time moments are calculated, and the results are presented in Table 5.

Table 5. Indirect influence values of vertex K_6 on vertex K_{11}

$P(K_6, K_{11})$	$I_p(0)$	$I_p(1)$	$I_p(2)$
(K_6, K_1, K_{11})	0	0.630	0.630
(K_6, K_7, K_1, K_{11})	0	0.122	0.122
(K_6, K_2, K_{11})	0	0.553	0.553
(K_6, K_7, K_2, K_{11})	0	0.077	0.077
(K_6, K_8, K_2, K_{11})	0	0.149	0.149
$(K_6, K_7, K_8, K_2, K_{11})$	0	0.035	0.035
$(K_6, K_4, K_8, K_2, K_{11})$	0	0.085	0.085
$(K_6, K_7, K_4, K_8, K_2, K_{11})$	0	0.013	0.013
(K_6, K_3, K_{11})	0	0.675	0.675
(K_6, K_7, K_3, K_{11})	0	0.131	0.131
(K_6, K_7, K_4, K_{11})	0	0.088	0.088
(K_6, K_8, K_{11})	0	0.385	0.385
(K_6, K_4, K_8, K_{11})	0	0.220	0.220
(K_6, K_7, K_8, K_{11})	0	0.091	0.091
$(K_6, K_7, K_4, K_8, K_{11})$	0	0.035	0.035

From Table 5, for time moments $t = 1, 2$ the following results are obtained:

$$\max_{P \in P(K_6, K_1, K_{11})} I_p(t) = (0; 0.630; 0.630)$$

$$\max_{P \in P(K_6, K_2, K_{11})} I_p(t) = (0; 0.553; 0.553)$$

$$\max_{P \in P(K_6, K_3, K_{11})} I_p(t) = (0; 0.675; 0.675)$$

$$\max_{P \in P(K_6, K_4, K_{11})} I_p(t) = (0; 0.088; 0.088)$$

$$\max_{P \in P(K_6, K_8, K_{11})} I_p(t) = (0; 0.385; 0.385)$$

Thus, taking into account the influences along all paths, the total indirect influence of vertex K_6 on vertex K_{11} is determined as:

$$\begin{aligned} T_{(K_6, K_{11})} &= \max_{P \in P(K_6, K_1, K_{11})} I_p(t) + \max_{P \in P(K_6, K_2, K_{11})} I_p(t) + \\ &+ \max_{P \in P(K_6, K_3, K_{11})} I_p(t) + \max_{P \in P(K_6, K_4, K_{11})} I_p(t) + \max_{P \in P(K_6, K_8, K_{11})} I_p(t) = \\ &= (0; 2.331; 2.331) \end{aligned}$$

Similarly, the influence of concept K_4 – physical security – affects the target concept K_{11} , representing the security of the IPS. The initial state vector is set by assuming vertex K_4 remains active throughout the process, i.e., $\Psi_4(t) = 1$ for any t . Thus, the initial vector is:

$$\Psi_{\Omega}(0) = (0; 0; 0; 1; 0; 0; 0; 0; 0; 0; 0)$$

According to formulas (1)–(3), the resulting process is:

$$\Psi_{\Omega}(0) \times W_{\Omega} = (0; 0; 0; 0; 0; 0; 0; 0.5; 0; 0; 0.7)$$

$$\Psi_{\Omega}(1) = f_T(\Psi_{\Omega}(0) \times W_{\Omega}) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 0)$$

$$\Psi_{\Omega}(1) \times W_{\Omega} = (-0.65; -0.1; 0.5; -0.87; 0; 0.55; -0.3; -0.72; 0; 0; 2.25)$$

$$\Psi_{\Omega}(2) = f_T(\Psi_{\Omega}(1) \times W_{\Omega}) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$$

$$\Psi_{\Omega}(2) \times W_{\Omega} = (-0.65; -0.1; 0.5; -0.87; 0; 0.55; -0.3; -0.72; 0; 0; 2.25)$$

$$\Psi_{\Omega}(3) = f_T(\Psi_{\Omega}(2) \times W_{\Omega}) = (1; 1; 1; 1; 1; 1; 1; 1; 1; 1; 1)$$

Thus, the process stabilizes at $t = 2$.

Using formulas (4)–(5), the influence of concept K_4 on K_{11} through all indirectly activated paths is computed.

It is assumed that from K_4 to K_{11} there exists one indirect path through each of K_2 and K_8 , i.e., $N^- = \{K_2, K_8\}$.

The values of indirect influences through activated paths at different time moments are presented in Table 6.

Table 6. Indirect influence values of vertex K_4 on vertex K_{11}

$P(K_4, K_{11})$	$I_p(0)$	$I_p(1)$	$I_p(2)$
(K_4, K_8, K_{11})	0	0.275	0.275
(K_4, K_8, K_2, K_{11})	0	0.106	0.106

Based on the data presented in Table 6, the total indirect influence of vertex K_4 on K_{11} is determined as:

$$\begin{aligned} T_{(K_4, K_{11})} &= \\ &= \max_{P \in P(K_4, K_2, K_{11})} I_p(t) + \max_{P \in P(K_4, K_8, K_{11})} I_p(t) = (0; 0.381; 0.381) \end{aligned}$$

The results of the conducted study clearly demonstrate how the security level of the IPS evolves over time under the influence of the most critical concepts, such as: K_6 – organizational support for information protection, and K_4 – physical security. It was found that in both cases, the process stabilizes at time $t = 2$. Moreover, the total influence of concept K_6 on K_{11} exceeds that of K_4 indicating a stronger contribution to overall system security. Therefore, it is recommended to strengthen organizational information protection measures by developing clear security policies, defining responsibility zones, implementing access control procedures, and conducting regular audits and training sessions on information security.

3. Conclusions

This study is devoted to examining the dynamics of changes in the security level of an IPS under the influence of key governing concepts derived from a topological analysis of the developed cognitive map structure. For this purpose, a simplicial complex was constructed, representing a sequence of simplices ordered by decreasing dimensionality. The first structural vector of the complex was determined, which enabled the identification of controlling and connected concepts within the fuzzy cognitive model.

Additionally, conditional time and vector parameters were introduced, including vertex state, input influence, and threshold vectors. It was established that the process stabilizes at time $t = 2$. All possible activation paths from the key concepts K_6 – organizational support for information protection, an K_4 – physical security, to the target concept K_{11} – system security, were analyzed. The indirect influence values of these concepts on system security were calculated. Based on the obtained results, it was found that the total influences from K_6 and K_4 to K_{11} at time moments $t = 0, 1, 2$ are: $T_{(K_6, K_{11})} = (0; 2.331; 2.331)$, $T_{(K_4, K_{11})} = (0; 0.381; 0.381)$.

In other words, beginning from $t = 1$, both processes reach a stable state; however, the influence of K_6 on system security remains approximately six times greater than that of K_4 . This highlights the critical role of organizational measures in shaping an effective IPS and underscores the importance of focusing efforts on improving managerial and regulatory mechanisms of cybersecurity.

References

- [1] Atkin, R. (1974). *Mathematical structure in human affairs*. Heinemann.
- [2] Atkin, R. H. (1977). Combinatorial Connectivities in Social Systems: An Application of Simplicial Complex Structures to the Study of Large Organizations. Birkhäuser Basel. <https://doi.org/10.1007/978-3-0348-5750-5>
- [3] Barcelo, H., Kramer, X., Laubenbacher, R., & Weaver, C. (2001). Foundations of a Connectivity Theory for Simplicial Complexes. *Advances in Applied Mathematics*, 26(2), 97–128. <https://doi.org/10.1006/aama.2000.0710>
- [4] Bhuiyan, M. R. I., Ullah, M. W., Ahmed, S., Bhuyan, M. K., Sultana, T., & Amin, A. (2024). Information Security for An Information Society for Accessing Secured Information: A PRISMA Based Systematic Review. *International Journal of Religion*, 5(11), 932–946. <https://doi.org/10.61707/irfrmr583>
- [5] Gebremeskel, B. K., Jonathan, G. M., & Yalew, S. D. (2023). Information Security Challenges During Digital Transformation. *Procedia Computer Science*, 219, 44–51. <https://doi.org/10.1016/j.procs.2023.01.262>
- [6] Hariyanti, E., Djunaidy, A., & Siahaan, D. (2021). Information security vulnerability prediction based on business process model using machine learning approach. *Computers & Security*, 110, 102422. <https://doi.org/10.1016/j.cose.2021.102422>
- [7] Jian Ying Zhang, Zhi-Qiang Liu, & Sanming Zhou. (2003). Quotient FCMs—A decomposition theory for fuzzy cognitive maps. *IEEE Transactions on Fuzzy Systems*, 11(5), 593–604. <https://doi.org/10.1109/TFUZZ.2003.817836>
- [8] Jiang, B., & Omer, I. (2007). Spatial Topology and its Structural Analysis based on the Concept of Simplicial Complex. *Transactions in GIS*, 11(6), 943–960. <https://doi.org/10.1111/j.1467-9671.2007.01073.x>
- [9] Kim, Y., & Kim, B. (2021). The Effective Factors on Continuity of Corporate Information Security Management: Based on TOE Framework. *Information*, 12(11), 446. <https://doi.org/10.3390/info12110446>
- [10] Liu, Z.-Q., & Zhang, J. Y. (2003). Interrogating the structure of fuzzy cognitive maps. *Soft Computing - A Fusion of Foundations, Methodologies and Applications*, 7(3), 148–153. <https://doi.org/10.1007/s00500-002-0202-x>
- [11] Raj, U., Banerjee, A., Ray, S., & Bhattacharya, S. (2024). Structure of higher-order interactions in social-ecological networks through Q-analysis of their neighbourhood and clique complex. *PLOS ONE*, 19(8), e0306409. <https://doi.org/10.1371/journal.pone.0306409>
- [12] Riihimäki, H. (2023). Simplicial q-connectivity of directed graphs with applications to network analysis. *SIAM Journal on Mathematics of Data Science*, 5(3), 800–828. <https://doi.org/10.1137/22M1480021>
- [13] Salagrama, S. (2021). An Effective Design of Model for Information Security Requirement Assessment. *International Journal of Advanced Computer Science and Applications*, 12(10). <https://doi.org/10.14569/IJACSA.2021.0121001>
- [14] Saliieva, O., & Yaremchuk, Y. (2024). Investigation of changes in the level of network security based on a cognitive approach. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, 14(4), 82–85. <https://doi.org/10.35784/iapgos.6719>
- [15] Saliieva, O., & Yaremchuk, Y. (2020). Determining the level of security of the information security system based on cognitive modeling. *Ukrainian Scientific Journal of Information Security*, 26(1), 42–49. <https://doi.org/10.18372/2225-5036.26.14669>
- [16] Shiao, W.-L., Wang, X., & Zheng, F. (2023). What are the trend and core knowledge of information security? A citation and co-citation analysis. *Information & Management*, 60(3), 103774. <https://doi.org/10.1016/j.im.2023.103774>

Ph.D. Olha V. Saliieva

e-mail: salieva8257@vntu.edu.ua

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 70 publications, including 27 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 modelling.

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



D.Sc. Eng. Yurii Ye. Yaremchuk

e-mail: yurevyar@vntu.edu.ua

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 360 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>

