https://doi.org/10.31891/2219-9365-2026-86-10
UDC 004.056.5:004.056.53:621.39:519.8

KUCHMA Yurii
Limited Liability Company Private Higher Education Institution «University of Modern Technologies»
https://orcid.org/0009-0002-5498-4271
e-mail: krabatua@gmail.com
POLINOVSKYI Viacheslav
Limited Liability Company Private Higher Education Institution «University of Modern Technologies»
https://orcid.org/0009-0008-1271-5528
e-mail: v.v.polin@gmail.com
PLAKHTII Maksym
Limited Liability Company Private Higher Education Institution «University of Modern Technologies»
https://orcid.org/0000-0003-3805-0591
e-mail: mp@ukr.net

METHODS FOR DYNAMIC OPTIMIZATION OF POST-QUANTUM DIGITAL SIGNATURES IN AUTHENTICATION PROTOCOLS FOR 6G ULTRA-DENSE NETWORKS

The development of sixth-generation (6G) networks, focused on ultra-dense access scenarios, ultra-low latency, and massive connectivity of heterogeneous devices, significantly increases the requirements for authentication mechanisms and cybersecurity. An additional risk factor is the projected progress in quantum computing, which challenges the long-term security of classical cryptographic algorithms and necessitates the integration of post-quantum digital signatures into telecommunication protocols. At the same time, existing approaches to implementing post-quantum cryptography in mobile networks are primarily based on static schemes and do not account for the dynamic operating conditions of 6G ultra-dense networks.

This paper investigates the problem of constructing quantum-resistant and high-performance authentication protocols for 6G networks, considering fluctuating network parameters, device heterogeneity, and constraints on computational and energy resources. It is demonstrated that the static application of post-quantum digital signatures fails to provide the necessary balance between security levels and the efficiency of authentication procedures in ultra-dense access scenarios.

To overcome these limitations, a generalized methodology for the dynamic optimization of post-quantum digital signatures in 6G authentication protocols is proposed. This methodology is based on the adaptive selection of cryptographic algorithms and their parameters depending on the current network state and the resource characteristics of authenticated nodes. The developed model formalizes a mechanism for dynamic signature selection, accounting for latency, computational costs, energy consumption, and quantum resistance levels, which allows for the formulation of formal optimality criteria for 6G networks. The integration of the proposed methods into the authentication protocol forms an adaptive cryptographic architecture capable of scaling under high connection density without compromising security. Experimental simulation results for ultra-dense access scenarios confirm that dynamic optimization reduces authentication latency and energy consumption compared to static post-quantum variants, justifying the feasibility of using adaptive protocols in 6G networks.

Keywords: post-quantum cryptography; cybersecurity; cyber risks; digital signature; authentication protocols; 6G networks; ultra-dense networks; dynamic optimization.

КУЧМА Юрій, ПОЛІНОВСЬКИЙ Вячеслав, ПЛАХТІЙ Максим
ТОВ ПВНЗ «Університет сучасних технологій»

МЕТОДИ ДИНАМІЧНОЇ ОПТИМІЗАЦІЇ ПОСТКВАНТОВИХ ЦИФРОВИХ ПІДПИСІВ У ПРОТОКОЛАХ АВТЕНТИФІКАЦІЇ НАДЩІЛЬНИХ МЕРЕЖ 6G

Розвиток мереж шостого покоління (6G), орієнтованих на надщільні сценарії доступу, ультранизькі затримки та масове підключення гетерогенних пристроїв, суттєво підвищує вимоги до механізмів автентифікації та забезпечення кібербезпеки. Додатковим фактором ризику є прогнозований прогрес квантових обчислень, який ставить під сумнів довгострокову стійкість класичних криптографічних алгоритмів і зумовлює необхідність використання постквантових цифрових підписів у телекомунікаційних протоколах. Водночас наявні підходи до впровадження постквантової криптографії в мобільних мережах здебільшого ґрунтуються на статичних схемах і не враховують динамічні умови функціонування надщільних мереж 6G. У роботі досліджено проблему побудови квантово-стійких і продуктивних протоколів автентифікації для мереж 6G з урахуванням змінності мережевих параметрів, гетерогенності пристроїв та обмежень обчислювальних і енергетичних ресурсів. Показано, що статичне застосування постквантових цифрових підписів не забезпечує необхідного балансу між рівнем безпеки та ефективністю автентифікаційних процедур у надщільних сценаріях доступу.

З метою подолання зазначених обмежень запропоновано узагальнену методологію динамічної оптимізації постквантових цифрових підписів у протоколах автентифікації 6G, яка базується на адаптивному виборі криптографічних алгоритмів і параметрів їх застосування залежно від поточного стану мережі та ресурсних характеристик автентифікованих вузлів. Розроблена модель формалізує механізм динамічного вибору цифрового підпису з урахуванням затримок, обчислювальних витрат, енергоспоживання та рівня квантової стійкості, що дозволяє сформувати формальні критерії оптимальності для 6G мереж. Інтеграція запропонованих методів у протокол автентифікації формує адаптивну криптографічну архітектуру, здатну масштабуватися в умовах високої щільності підключень без зниження рівня безпеки. Результати експериментального моделювання для надщільних сценаріїв доступу підтверджують, що динамічна оптимізація забезпечує зменшення затримок автентифікації та енергоспоживання порівняно зі статичними постквантовими варіантами, що обґрунтовує доцільність використання адаптивних протоколів у мережах 6G.

Ключові слова: постквантова криптографія, кібербезпека, кіберризики, цифровий підпис, протоколи автентифікації, мережі 6G, надщільні мережі, динамічна оптимізація.

Стаття надійшла до редакції / Received 18.03.2026
Прийнята до друку / Accepted 16.04.2026
Опубліковано / Published 31.05.2026

PROBLEM STATEMENT

Sixth-generation (6G) networks establish a new telecommunications paradigm supporting ultra-low latency, ultra-dense device connectivity, and heterogeneous services, which places increased demands on authentication mechanisms and cybersecurity. An additional risk factor is the potential emergence of quantum computers capable of undermining the security of traditional cryptographic algorithms underlying digital signatures and key exchange, such as RSA and ECC, due to the efficiency of Shor's algorithm for systems like RSA and ECDSA [1]. Consequently, the international IT community is actively working on Post-Quantum Cryptography (PQC) a set of algorithms resistant to attacks utilizing quantum computing [2].

Despite efforts to develop and standardize post-quantum digital signature algorithms, such as CRYSTALS-Dilithium, Falcon, and SPHINCS+ specified by NIST, existing approaches to their application in telecommunication protocols remain limited in practical scope and are predominantly based on static solutions without adaptation to fluctuating network operating conditions [3]. The static implementation of PQC schemes fails to account for key aspects such as dynamic traffic loads, node mobility, and the constrained resources of end-user devices factors typical of 6G ultra-dense networks that directly impact authentication efficiency and system scalability [4].

The scientific and applied problem lies in the fact that the absence of adaptive authentication protocols with PQC and models for dynamic digital signature selection limits the ability to balance quantum resistance and performance in 6G ultra-dense environments. This precludes the formalization of clear optimality criteria that could ensure coordinated management of collisions, energy consumption, and computational costs during authentication. Research in this field is also insufficiently supported by experimental results for ultra-dense access scenarios and lacks a generalized methodology for optimizing post-quantum digital signatures in telecommunication networks, complicating their integration into future standards.

Thus, addressing this problem is essential both from a theoretical perspective in the context of advancing post-quantum cryptography and from a practical standpoint due to the need to build efficient and secure authentication protocols for 6G architectures capable of withstanding high connection density without significant performance degradation.

ANALYSIS OF THE LATEST RESEARCH

The emergence of post-quantum cryptography as an integral part of securing global cyberspace is driven by significant consolidated efforts from the international scientific community and key standardization bodies.

A leading role in this process is played by the U.S. National Institute of Standards and Technology (NIST). As early as 2016, NIST initiated a large-scale international program for PQC standardization. The primary goal of this program is to develop and implement cryptographic algorithms capable of effectively resisting potential threats arising from the rapid advancement of quantum computing technologies [5].

In August 2024, NIST published the first official standards FIPS 203, FIPS 204, and FIPS 205 which define cryptographic protection algorithms, including post-quantum digital signature schemes based on CRYSTALS-Dilithium (ML-DSA) and SPHINCS+ (SLH-DSA) [6]. This establishes a foundation for the further implementation of quantum-resistant authentication mechanisms in critical electronic communication systems.

Beyond official standardization, numerous academic studies analyze the efficiency and performance of new PQC algorithms, including measurements of latency, energy consumption, and computational overhead on real-world platforms, specifically mobile and IoT environments [7]. Such works are crucial for understanding the practical limitations of post-quantum digital signatures; however, they predominantly focus on individual algorithms and their implementations rather than on systemic authentication protocols or their adaptation to ultra-dense telecommunication network conditions.

Ukrainian scientists are also actively contributing to the global development of post-quantum cryptography. A number of domestic scientific papers have performed deep analyses of modern digital signature algorithms. In particular, comparisons of promising post-quantum architectures have been conducted, considering their cryptographic properties and computational complexity. These studies have justified the feasibility of their further adaptation to practical cybersecurity tasks [3, 7, 8, 9]. Furthermore, review studies by Ukrainian authors emphasize mathematical models, computational features, and the structure of post-quantum cryptographic systems. This highlights the necessity of developing effective optimization methods that account for resource constraints and the stringent requirements of modern electronic communication systems [10].

Overall, despite significant progress in the standardization and analytical evaluation of individual post-quantum cryptographic algorithms, several fundamental scientific gaps remain. Specifically, current research does not address adaptive authentication protocols capable of accounting for real-time network dynamics and the operational

characteristics of post-quantum digital signatures. There is also a lack of formalized models for the dynamic selection of digital signature architectural solutions and their optimality criteria in ultra-dense access scenarios typical of sixth-generation networks.

A separate unresolved issue is the lack of a generalized methodology for optimizing post-quantum digital signatures for 6G telecommunication networks, which complicates the assessment of adaptive architecture behavior in large-scale and highly dynamic networks due to the limited availability of experimental results.

Consequently, the combination of these factors justifies the scientific novelty and relevance of this research.

FORMULATION OF THE GOALS OF THE ARTICLE

The objective of the article is the development and substantiation of methods for the dynamic optimization of post-quantum digital signatures in authentication protocols for ultra-dense 6G networks, aimed at increasing authentication efficiency under conditions of variable network parameters, limited node resources, and strict requirements for latency and energy consumption while maintaining a specified level of quantum resistance.

PRESENTING THE MAIN MATERIAL

Ensuring quantum-resistant authentication in sixth-generation ultra-dense networks should be addressed as a system-level problem. In this context, cryptographic robustness, exchange timing characteristics, and node resource constraints form an interconnected multidimensional space of design decisions. Given the exponential growth in the number of connected devices, traffic unevenness, and the prospect of practical quantum attacks, the use of a single fixed digital signature algorithm leads either to excessive resource overhead or to unacceptable authentication latencies [11]. Therefore, from an engineering perspective, a post-quantum digital signature should be treated not as a static protocol element, but as a controllable optimization variable, the selection of which is performed contextually and dynamically according to the current network state.

Such an approach requires a formal mathematical formulation that allows for the simultaneous consideration of several conflicting performance criteria. Let us define a set of available post-quantum digital signature schemes:

$$\boldsymbol{S} = \{s_1, s_2, \ldots, s_{\mathrm{n}}\}. \tag{1}$$

Each scheme s_i is mapped to a vector of technical and operational characteristics:

$$\mathbf{P}_i = (D_i, C_i, E_i, Q_i), \tag{2}$$

where D_i characterizes the time overhead for executing the digital signature generation and verification procedures, C_i reflects the computational complexity of the algorithm, while E_i determines the energy consumption level and Q_i corresponds to the quantum resistance level of the scheme according to current cryptographic assessments and standardization results.

In this case, the primary security requirement is formalized as the constraint $Q_i \geq Q_{\min}$, after which the selection task is reduced to minimizing the total resource costs. However, given the mutually conflicting nature of the indicators D_i, C_i, E_i, Q_i, scalar optimization does not provide a universal solution. Therefore, it is appropriate to transition to a multi-objective formulation based on Pareto optimality.

Let us introduce the cost vector

$$\boldsymbol{z}_i = \left(D_i, C_i, E_i, -Q_i\right), \tag{3}$$

where the minus sign reflects the maximization nature of the security indicator. A scheme s_a dominates scheme s_b if $\boldsymbol{z}_a \leq \boldsymbol{z}_b$ component-wise, and the inequality is strict for at least one component. The set of non-dominated alternatives

$$P = \{s \in S \mid \text{y}\, s' \in S : \boldsymbol{z}(s') \prec \quad s \tag{4}$$

forms the Pareto frontier, which geometrically describes the boundary surface of acceptable trade-offs between latency, computational costs, energy, and cryptographic robustness. Thus, instead of a single "best" algorithm, a region of rational solutions is obtained, within which the subsequent selection is determined by the application context.

Since 6G network parameters fluctuate significantly over time, the effectiveness of each scheme becomes dependent on the current operating mode. To formalize this dependency, we introduce the network state vector:

$$N(t) = \left[\rho(t), \lambda(t), \tau(t), \tau(t)\right], \tag{5}$$

where $\rho(t)$ is the active connection density, $\lambda(t)$ is the authentication request intensity, $\tau(t)$ represents the average signaling latencies, and $\tau(t)$ denotes the available energy resources of the nodes. Consequently, the

characteristics D_i, C_i, E_i and even the practical efficiency Q_i are interpreted as functions of the network state, while the Pareto frontier acquires a time dependency $P(t)$.

To obtain a specific solution within the frontier, a context-dependent scalarization of criteria is used in the form of a generalized objective function

$$J_i(t) = \alpha(t)D_i + \beta(t)C_i + \gamma(t)E_i - \delta(t)Q_i, \tag{6}$$

where the weighting coefficients reflect the current optimization priorities. The optimal scheme for a given point in time is determined as:

$$s^*(t) = \arg \min_{s_i \in P(t)} J_i(t). \tag{7}$$

Thus, an adaptive control module is formed. Before each authentication session, this module selects a cryptographic algorithm without altering the structure of the message exchange protocol itself and determines the optimal post-quantum digital signature scheme based on the current network state.

Further generalization is achieved through stochastic modeling of the network state evolution. It is assumed that the process $N(t)$ satisfies the Markov property

$$\Pr\{N(t+1) | \ N(t), N(t-1), \ldots\} = \Pr\{N(t+1) | \ N(t)\}, \tag{8}$$

that is, the future dynamics are determined solely by the current parameters. After the state space discretization, we obtain the set Ω and the transition probability matrix $P_{n\,n'}$, which defines the probabilistic load dynamics.

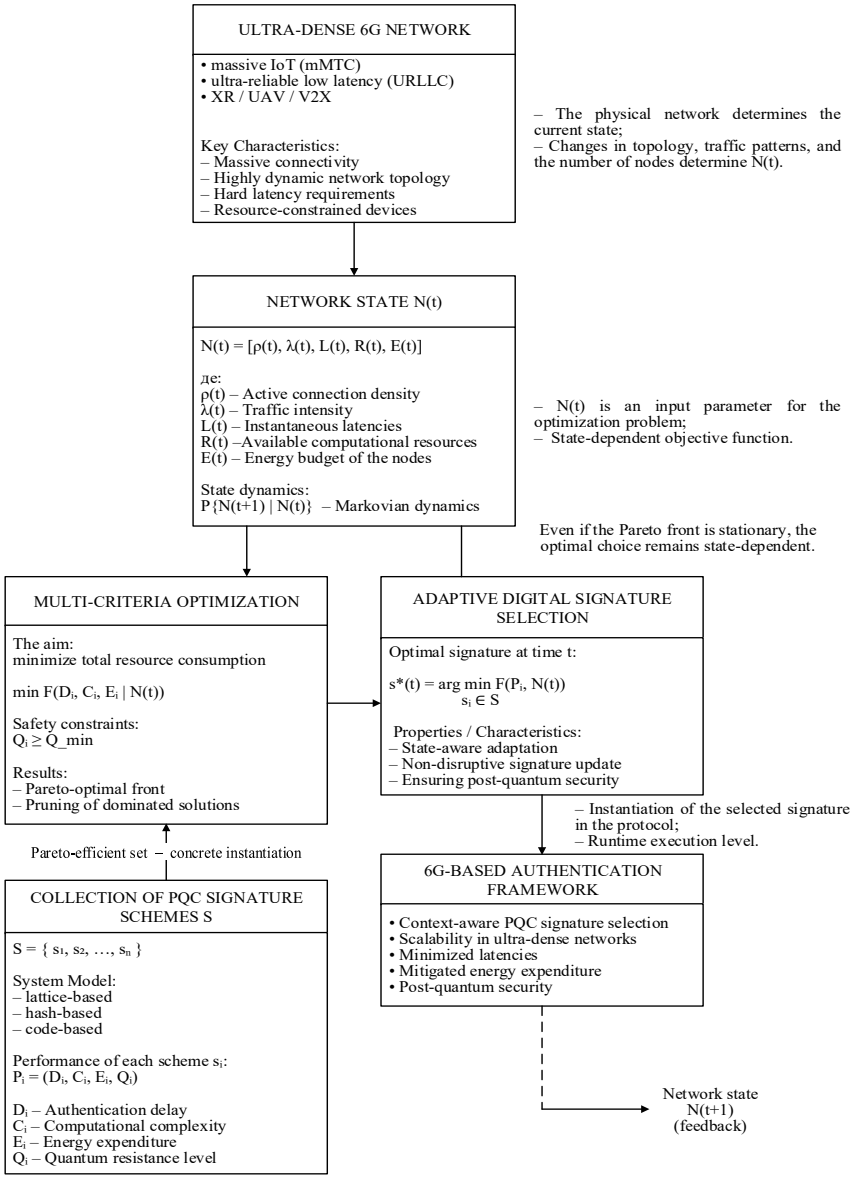

Fig. 1. Generalized structural and functional diagram of adaptive post-quantum digital signature selection in the 6G authentication protocol

In this formulation, the signature selection is interpreted as a Markov Decision Process (MDP) with a policy

$$\pi : \Omega \to \mathrm{S}, \tag{9}$$

which maps each network state to a specific cryptographic scheme. The optimal policy minimizes the expected long-term costs, as described by the Bellman equation:

$$V(n) = \min_{s \in S} \left[J(n,s) + \sum_{n' \in \Omega} \mathrm{P}_{nn'}(s) V(n') \right], \tag{10}$$

where $J(n,s)$ is the instantaneous cost of authentication in state n when using scheme s, while the transition term accounts for the impact of the current choice on future network operating modes. Consequently, the decision becomes proactive: not only current costs but also expected future costs are minimized.

To align the model with the service heterogeneity of 6G, the weighting coefficients are defined as functions of the network state:

$$\alpha = f_\alpha(N), \quad \beta = f_\beta(N), \quad \gamma = f_\gamma(N), \quad \delta = f_\delta(N), \tag{11}$$

which ensures an automatic reconfiguration of priorities. In particular, for URLLC scenarios, the following holds

$$\alpha \square \qquad \square ,$$

which forcibly minimizes authentication latency, whereas for mMTC, it is appropriate to

$$\gamma \square \qquad \approx \gamma ,$$

which orients the selection towards energy-efficient and computationally moderate schemes during massive connection events.

This can be generalized as a priority matrix (Table 1).

Table 1

Service Type	Latency (D)	Computation (C)	Energy (E)	Security (Q)
URLLC	High	Medium	Low	High
mMTC	Low	Medium	High	Medium

Thus, the service type defines the baseline profile of the objective function's weighting coefficients, reflecting the regulatory requirements for latency, reliability, energy consumption, and security level for the respective traffic class.

The current network state acts as a contextual regulator, performing continuous operational adjustment of these weights through the mapping of the network state function. As a result, the optimization process occurs simultaneously in two interconnected dimensions: policy-driven and state-driven. This ensures both compliance with the SLA of a specific service and adaptation to current resource and traffic conditions.

Under this problem formulation, the criteria system transitions from a static configuration to a dynamic controllable model, where the selection of a cryptographic primitive is a function of the network state. This establishes a formalized, scalable mechanism for the real-time adaptation of post-quantum authentication protocols to diverse 6G scenarios. Accordingly, the proposed multi-level optimization model forms a closed-loop decision-making framework, within which the current network state, service characteristics, and cryptographic algorithm parameters are integrated into a unified adaptive management mechanism [12].

Practical integration of the proposed approach is implemented in the form of a closed control loop at the core or edge-node level: estimation of the current state $N(t)$; formation of the dynamic Pareto frontier $P(t)$; calculation of objective functions with adaptive weights; selection of $s^*(t)$ and transmission of parameters to the protocol parties; execution of the standard authentication procedure; updating of statistical estimates to refine transition and cost models.

Decentralized implementation of this cycle at the edge level ensures linear scalability relative to the number of concurrent sessions and eliminates centralized processing bottlenecks, which is critical for 6G ultra-dense deployments.

Summarizing the above, it is appropriate to state that the proposed approach forms a mathematical synergistic basis of multi-objective Pareto optimization, contextual scalarization, and stochastic control based on Markov processes, establishing a holistic theoretical and applied framework for the adaptive orchestration of authentication services.

Furthermore, it should be emphasized that within the proposed approach, the post-quantum digital signature is determined not as a fixed parameter, but as a dynamically controlled variable of the optimization objective function. Therefore, such a methodological approach allows for achieving a trade-off between ensuring quantum-resistant protection and adhering to stringent criteria regarding latency, throughput, and energy autonomy in the context of heterogeneous and resource-constrained 6G telecommunication ecosystems.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

This scientific paper investigates the problem of constructing quantum-resistant and high-performance authentication protocols for sixth-generation networks. The problem is formalized as a multi-objective optimization task, allowing for a comprehensive integration of requirements for quantum cryptographic robustness, computational efficiency, authentication latency, and scalability in ultra-dense network environments.

The study employs a Pareto-oriented optimization approach, which enables the identification of a set of non-dominated solutions representing the trade-offs between time delays, computational overhead, and the quantum resistance level of authentication protocols.

A generalized methodology for the dynamic optimization of post-quantum digital signatures in 6G authentication protocols is proposed. This methodology is based on the adaptive selection of cryptographic algorithms and their application parameters depending on the current network state and the resource characteristics of the authenticated nodes.

Simulation results confirm that the dynamic selection of digital signature mechanisms provides a significant increase in time and energy efficiency compared to static scenarios. Ultimately, a mechanism suitable for practical implementation has been developed, where the post-quantum digital signature is treated as an optimization variable, enabling the real-time alignment of security requirements and resource efficiency.

Promising directions for further research include expanding the set of optimization metrics to account for channel reliability, latency jitter, and packet loss intensity, as well as implementing online learning methods for the dynamic adaptation of weight profiles based on real network traffic analysis. Particular attention should be paid to investigating the resistance of the proposed schemes to physical implementation attacks, specifically side-channel attacks and fault injections. Furthermore, the development of cooperative interaction protocols between Edge nodes for sharing aggregated telemetry and the hardware acceleration of post-quantum cryptographic primitives based on FPGA/ASIC, followed by field validation in 6G network infrastructure, remain highly relevant.

References

1. SSL.org.ua. (n.d.). *Post-quantum cryptography – preparing for a quantum-secure future*. Retrieved January 28, 2026, URL: https://ssl.org.ua
2. Novikov, D., & Poltorak, V. Technologies of post-quantum cryptography. *Adaptive automatic control systems.* 2023. Vol. 1(42), P. 171–183. DOI: https://doi.org/10.20535/1560-8956.42.2023.279169.
3. Lavryk I. RESEARCH OF POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS. *Herald of Khmelnytskyi National University. Technical Sciences*. 2024. Vol. 333(2), P. 361–369. DOI: https://doi.org/10.31891/2307-5732-2024-333-2-56
4. Karthik Kumar Vaigandla Quantum-Secure IoT Networks for the 6G Era: Post-Quantum Cryptography, Blockchain Integration, and Trust Architectures - A Comprehensive Review. *Journal of Sensors, IoT & Health Sciences (JSIHS,ISSN: 2584-2560)*. 2025. Vol. 3, №3. P. 44–75. DOI: https://doi.org/10.69996/jsihs.2025014
5. Zhyvylo, Y., & Kuchma, Y. DEEP LEARNING MODEL FOR PREDICTING COMPROMISED ACCOUNTS IN SECURITY EVENT MANAGEMENT SYSTEMS. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 2025. Vol. 3(31), P. 589–601. DOI: https://doi.org/10.28925/2663-4023.2025.31.1050
6. Zhyvylo, Ye. O., Kuchma, Yu. V., & Fesenko, T. M. Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures [Monograph]. *C91 Moderní aspekty vědy: LXII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o*., 2025. pp. 407–456. URL: http://perspectives.pp.ua/public/site/mono/mono-62.pdf
7. Zhyvylo, Y., & Kuchma, Y. Mathematical modeling of intellectual and cryptographic protection of authentication keys. *Collection "Information Technology and Security"*. 2025. Vol. 13(2), P. 162–177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591
8. Correction Codes in the System of Residual Classes / V. Krasnobayev et al. *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 8–11 October 2019. 2019. DOI: https://doi.org/10.1109/picst47496.2019.9061253.
9. Zhyvylo, Y., & Kuchma, Y. Practical application and vulnerabilities of the Hill Cipher in a modern context. *Systems of Control, Navigation and Communication*. 2025. Vol. 4(78), P. 66–69. DOI: https://doi.org/10.26906/SUNZ.2025.4.066
10. Shyshatskyi, A. (Ed.). The development of management methods based on bio-inspired algorithms Information and control systems: modelling and optimizations: collective monograph. – Kharkiv: *TECHNOLOGY CENTER PC*. 2024. – 35-69p. DOI: http://doi.org/10.15587/978-617-8360-04-7
11. Fesenko, T., & Kalashnicova, Y. FEDERATIVE GNN-XAI MODEL FORPREDICTING COMPROMISE OF ACCOUNT RECORDS IN ZERO TRUST ENVIRONMENT. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 2025. Vol. 3(31), P. 602–619. DOI: https://doi.org/10.28925/2663-4023.2025.31.1049
12. Fesenko, T., & Kalashnikova Y. Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection. *Collection "Information Technology and Security"*. 2025. Vol. 13(2), P. 178–191. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344592.