МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАУКОВІ ПРАЦІ ДОНЕЦЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ

Серія: «Обчислювальна техніка та автоматизація»

Всеукраїнський науковий збірник
Заснований у липні 1998 року
Виходить 2 рази на рік
Т4. № 6(38)'2026

Видавничий дім
«Гельветика»
2026

УДК 681.5:658.5:621.3

Друкується за рішенням Вченої ради Державного вищого навчального закладу «Донецький національний технічний університет» (протокол № 5 від 07.05.2026 р.).

У збірнику опубліковано статті науковців, аспірантів, магістрів та інженерів провідних підприємств і закладів вищої освіти України, у яких наведено результати наукових досліджень та розробок, виконаних у 2023–2024 рр. відповідно до напрямків: автоматизація технологічних процесів, інформаційна безпека, інформаційно-вимірювальні системи, електронні та мікропроцесорні прилади, інформаційні технології, кібербезпека та захист критичної інфраструктури, математичне та комп'ютерне моделювання, телекомунікаційні системи та мережі.

Матеріали збірника призначено для викладачів, наукових співробітників, інженерно-технічних працівників, аспірантів і студентів, які досліджують питання інформаційної безпеки, розробки та впровадження інформаційних систем та технологій, розробки й використання автоматичних, інформаційних та електронних систем.

Засновник – Донецький національний технічний університет.

Ідентифікатор медіа R30-02474 відповідно з додатком до Рішення НРУ з питань телебачення і радіомовлення №139 від 18.01.2024 р.

Суб'єкт у сфері друкованих медіа – Державний вищий навчальний заклад «Донецький національний технічний університет» (пл. Шибанкова, буд. 2, м. Покровськ Донецької обл., 85300, mail@donntu.edu.ua, +380 99 604-91-28).

Збірник включено до списку друкованих (електронних) періодичних наукових фахових видань України, у яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора й кандидата наук (спеціальності G6 Інформаційно-вимірювальні технології; G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка; F3 Комп'ютерні науки). Наказ МОН України № 886 (додаток № 4) від 2 липня 2020 року, Наказ МОН України № 349 (додаток № 5) від 24 лютого 2025 року (виправлено відповідно до Наказу МОН України № 641 (додаток № 8) від 28 квітня 2025 року).

ISSN 2075-4272 (Print),
ISSN 2786-9024 (Online)

ЗМІСТ

АВТОМАТИЗАЦІЯ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМИ, ЕЛЕКТРОННІ ТА МІКРОПРОЦЕСОРНІ ПРИЛАДИ

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ШТУЧНИЙ ІНТЕЛЕКТ

CONTENTS

PROCESS AUTOMATION

INFORMATION TECHNOLOGY

INFORMATION AND MEASUREMENT SYSTEMS, ELECTRONIC AND MICROPROCESSOR DEVICES

CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

ARTIFICIAL INTELLIGENCE

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

Автоматизація технологічних процесів

UDC 004.896:681.536.5]:004.415

HARDWARE-SOFTWARE MODULE FOR INTELLIGENT MICROCLIMATE CONTROL IN INDUSTRIAL FACILITIES

V.V. Yevsieiev, I.V. Holod
Department of Computer-Integrated Technologies, Automation and Robotics, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID https://orcid.org/0000-0002-2590-7085
ORCID https://orcid.org/0009-0005-1056-8614
E-mail: vladyslav.yevsieiev@nure.ua

ABSTRACT

The article addresses the problem of automated and intelligent microclimate control in industrial premises, where the stability of the temperature and humidity regime directly affects the efficiency of technological processes, energy efficiency, and equipment reliability. It is shown that traditional control systems based on simplified linear models do not provide the required accuracy under conditions of multifactor disturbances and dynamic changes in environmental parameters. The purpose of the study is to develop a hardware–software module capable of providing adaptive, stable, and energy-efficient control of microclimate parameters based on the coordinated operation of sensor, computational, and executive subsystems.

The research methodology involves the development of a structural architecture of the hardware–software module, integration of a sensor system, a controller with embedded HMI, and executive mechanisms, as well as the formation of algorithmic logic for regulating temperature, humidity, air exchange, and internal pressure. The study applies methods of analysis and synthesis, mathematical modeling, and experimental testing under real industrial conditions. The module operation was verified through continuous data acquisition, real-time parameter logging, and evaluation of the response of executive mechanisms to changes in external and internal factors.

The test results confirmed the module’s ability to maintain stable microclimate parameters within specified setpoints, ensuring smooth switching between heating, cooling, and ventilation modes. The recorded temperature dynamics demonstrate the absence of sharp fluctuations, effective operation of hysteresis mechanisms, and rapid system response to load changes. The practical applicability of the module is confirmed by its stable operation under daily variations in outdoor temperature, the presence of thermal disturbances, and variations in air exchange. The selected combination of equipment (KSP-08.L controller, data acquisition modules, and sensor devices) provided the required performance, accuracy, and flexibility.

Prospects for further research include expanding the functionality of the hardware–software module through the integration of predictive models, in particular neural network structures of the NNARX type, which will increase the accuracy of microclimate dynamics assessment and optimize control logic in complex industrial scenarios. The obtained results form a basis for improving intelligent control systems in industrial cyber-physical complexes and for their implementation in various industrial sectors.

Keywords: *intelligent control; microclimate; hardware-software module; cyber-physical systems; sensor subsystem; actuators; control algorithms; parameter forecasting.*

Task statement

Maintaining a stable microclimate in industrial premises determines the reliability of technological processes and the level of energy consumption; therefore, the accuracy of the control system operation directly affects product quality and equipment lifetime. Real-world operation is associated with nonlinear heat and moisture exchange processes, the presence of unpredictable disturbances, and changes in internal conditions, which complicate the performance of traditional controllers. Their response is delayed, and environmental parameters

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

change inertially, causing deviations from technologically permissible values.

The industrial environment requires a solution capable of continuously registering parameters, correctly interpreting changes in thermal load, and coordinating the operation of executive mechanisms under conditions of incomplete information and disturbances. The system must ensure the generation of control actions in real time and remain robust to noise and time delays that affect control accuracy.

Against this background, there is a need to develop a hardware–software module that integrates a sensor subsystem, data acquisition tools, a computational platform, and executive mechanisms into a unified control loop. Such a solution should demonstrate microclimate stabilization under real industrial disturbances and form a basis for further system development through the implementation of predictive models capable of increasing control accuracy and adaptability to changing technological scenarios.

Analysis of recent research and publications

In study [1], modern approaches to the use of artificial intelligence in climate research and energy systems are summarized, highlighting the growing role of intelligent methods in modeling and optimizing microclimate processes. Study [2] demonstrates the significance of digital twins and smart manufacturing in the context of sustainable development, emphasizing the close integration of sensor systems, communication tools, and real-time analytics. Paper [3] presents a comprehensive vision of the architecture and practices of cyber-physical systems for Industry 4.0, where computational resources, communications, and physical processes are integrated. Study [4] complements this approach by focusing on cybersecurity and resilience aspects of cyber-physical systems, which are crucial for the implementation of intelligent control modules in industrial environments.

The methodological foundations for the construction and formal description of cyber-physical production systems are considered in studies [5–7]. In [5], a method for synthesizing CPS operation algorithms oriented toward subsystem coordination and ensuring consistency of their operation is proposed, which is important for building an integrated microclimate control loop. In [6], a declarative modeling language for CPS is developed, enabling the formalization of the structure and behavior of production systems, which directly correlates with the tasks of designing hardware–software modules. Study [7] is devoted to the organization of secure access to HMI/SCADA systems over unsecured networks and emphasizes the importance of reliable user authentication in the context of distributed cyber-physical systems. Review [8] systematizes possible applications of edge computing in industry, demonstrating the feasibility of transferring part of data processing to the local device level, which corresponds to the concept of a hardware–software module with embedded intelligent functions.

A separate group of studies focuses on sensor systems and hardware. In [9], a sensor-based navigation system for a mobile robot using ultrasonic sensors is developed, highlighting the role of multichannel real-time data acquisition and its relevance for building a microclimate sensor subsystem. Report [10] analyzes modern sensors and control systems for commercial buildings, outlining barriers and drivers for the implementation of intelligent sensors and controllers in HVAC practice. Review [11] summarizes data-driven approaches to fault diagnosis in HVAC systems, indicating the importance of high-quality data acquisition and processing to ensure the reliability of microclimate control systems.

Considerable attention in contemporary research is given to control algorithms that use neural network and fuzzy approaches. In [12], the application of a nonlinear autoregressive NARX model for temperature prediction in a solar adsorption cooling system is demonstrated, confirming the effectiveness of autoregressive neural network structures for thermodynamic modeling tasks. Paper [13] examines guaranteed control in interval type-2 fuzzy systems, emphasizing operation under uncertainty, which is relevant for industrial facilities with variable environmental parameters. In [14], context-dependent HVAC control based on fuzzy logic is proposed, oriented toward adaptive mode changes depending on building state and external conditions. Study [15] demonstrates the capabilities of artificial neural networks for short-term indoor temperature forecasting, which directly relates to predictive microclimate control tasks. Review [16] systematizes neuro-fuzzy architectures in the context of interpretable AI, highlighting their potential for building transparent and adaptive control systems.

Issues of energy efficiency and comparison of classical and intelligent control methods are considered in studies [17–20]. In [17], a comparative modeling of HVAC control systems based on PID controllers and reinforcement learning methods is performed, demonstrating the advantages of intelligent approaches in tasks of simultaneous optimization of comfort and energy consumption. Paper [18] describes the integration of machine learning with model predictive control to improve the energy efficiency of HVAC systems, confirming the feasibility of combining predictive models with flexible control logic. Study [19] analyzes the potential of AI-oriented smart energy grids for reducing the carbon footprint, aligning with trends toward decarbonization of industrial processes. Review [20] systematizes the application of artificial intelligence to improve energy efficiency and indoor environmental quality in buildings, confirming

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

the general trend of transitioning from traditional controllers to hybrid, data-driven control systems.

In summary, the analyzed studies demonstrate the intensive development of cyber-physical systems, intelligent sensor and computational platforms, as well as hybrid control algorithms based on artificial neural networks and fuzzy logic. At the same time, existing works mainly address either general CPS concepts and energy-efficient control or individual aspects of software and algorithmic solutions for HVAC systems. The issue of creating an integrated hardware–software module for intelligent microclimate control in industrial premises–combining hardware platform selection, sensor infrastructure, executive mechanisms, and control logic, and validated through full-scale testing under real operating conditions–remains insufficiently explored, which determines the relevance of this study.

Separation of previously unresolved parts of the overall problem

Despite the active development of automated microclimate control systems, most existing solutions focus on partial aspects of their operation and do not provide full integration of hardware and software components into a unified industrial platform. Current studies present isolated descriptions of sensor devices, principles of executive mechanism operation, or control algorithms; however, a holistic architectural vision in which all these subsystems operate in a coordinated manner is lacking.

Issues related to the development of a modular computational structure capable of operating in an open software environment while simultaneously ensuring industrial reliability, resistance to external influences, and compliance with real-time requirements remain insufficiently explored. The literature lacks descriptions of solutions capable of maintaining parameter stability under variable industrial conditions, where the system must respond to dynamic thermal loads, spatial heterogeneity of the environment, and significant fluctuations in airflow.

Another unresolved problem is the lack of practical studies in which the hardware platform is combined with the possibility of further implementation of predictive data analysis methods. Scientific works predominantly address simulation-based or laboratory models, whereas real industrial scenarios are scarcely described. This complicates the assessment of how theoretically proposed approaches can operate in the complex environment of industrial premises.

Thus, the problem of creating an integrated hardware–software module that unifies sensor infrastructure, data acquisition tools, a computational platform, and an executive subsystem into a single solution–validated under real operating conditions and prepared for expansion through intelligent and predictive algorithms–remains unresolved. This gap defines both the direction and the necessity of the present study.

Purpose of the study

The purpose of the study is to improve the efficiency of microclimate control and the stability of technological processes in industrial premises by developing and experimentally validating a hardware–software module for intelligent control that ensures coordinated interaction of sensor, computational, and executive subsystems within a unified cyber-physical loop. The implementation of the module is aimed at minimizing the impact of industrial disturbances, reducing the system response time to parameter deviations, and creating a basis for the integration of predictive neural network models.

Methods, object, subject and methods of research

Methods. Observation, analysis and synthesis, mathematical modeling, artificial neural network and fuzzy logic methods, and experimental modeling in the Python environment using the Keras library.

Object of the study. Microclimate control processes in industrial premises under conditions of variable external and internal factors.

Subject of the study. The structure, principles of design, and operation of a hardware–software module for intelligent microclimate control in industrial premises, which ensures coordinated operation of sensor, computational, and executive subsystems.

The main material

The stability of the microclimate in industrial premises is a key condition for the efficiency of technological processes, energy efficiency, and reliable equipment operation, since the temperature and humidity regime directly affects product quality and equipment durability. Traditional threshold-based control systems that use a limited set of sensors do not provide the required accuracy or timely response to changes in external conditions, which leads to fluctuations in environmental parameters and increased energy consumption.

The development of modern automation systems creates opportunities for more accurate and adaptive operation through coordinated interaction of sensor devices, executive mechanisms, and controllers capable of processing data in real time. In this context, the development of a hardware–software module that provides integrated microclimate control with scalability and potential for further development is particularly relevant.

This study presents a hardware–software module for intelligent microclimate control, the operability of which has been confirmed through full-scale testing under real industrial conditions, making it possible to ensure stable

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

environmental parameters and improve the efficiency of technological processes.

Structure of the hardware–software module. The architecture of the hardware–software module forms an integrated system for collecting, processing, and utilizing technological information to stabilize the microclimate in industrial premises. The module integrates a sensor subsystem, primary data processing tools, a controller with embedded HMI, and a set of executive mechanisms that provide regulation of temperature, humidity, air exchange, and pressure. All components operate in real time, enabling prompt response to external and internal disturbances.

The structural diagram (Fig. 1) illustrates the interaction between sensor channels, the data acquisition module, the central controller, communication interfaces, and executive mechanisms. The sensor subsystem provides measurements of temperature, humidity, air gas composition, and internal pressure, with the possibility of adapting sensor types to the requirements of a specific facility. Primary data undergo filtering, linearization, and normalization within the data acquisition module.

Communication interfaces, including RS-485 and Ethernet, enable data exchange between subsystems, ensuring module scalability and resistance to electromagnetic interference, which is critical for industrial environments. The controller with embedded HMI performs microclimate parameter analysis and generates control actions, supporting coordinated operation of heaters, fans, and valves. The operator is able to monitor the system status and adjust settings in real time.

Actuators implement physical effects on the environment through smooth or discrete regulation of heating and ventilation. The coordination of their operation is based on feedback principles, which ensures microclimate stabilization under dynamic external factors. Measurement and control signal flows form a closed loop that determines control accuracy and system reliability.

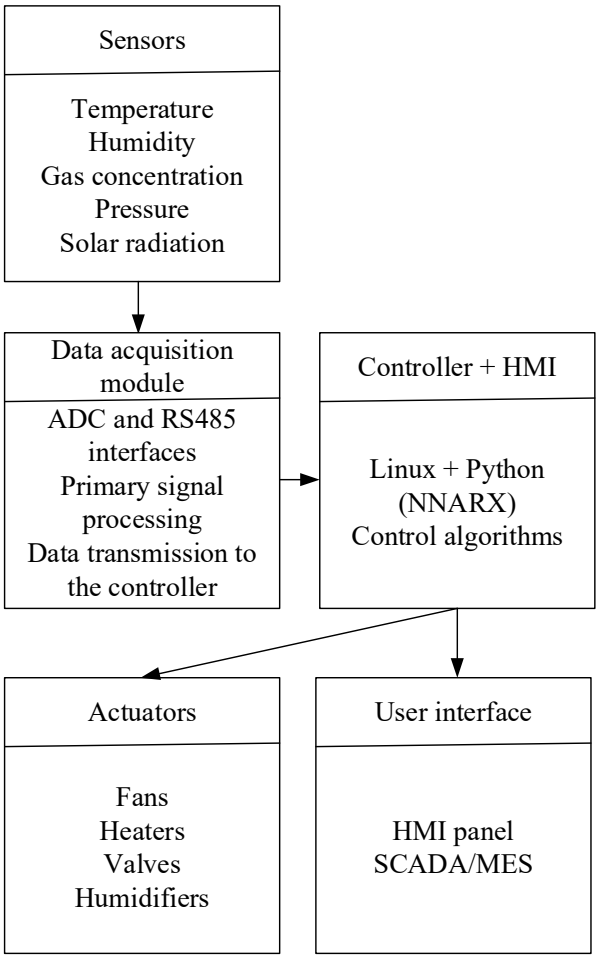

Fig. 1. Structural diagram of the hardware–software module

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

Selection of hardware components

The development of a hardware–software module for intelligent microclimate control requires the selection of a computational platform that provides sufficient performance, support for modern algorithms, and a user-friendly operator interface. In this context, a key component is a controller with an embedded HMI that combines data acquisition, control logic, and local visualization functions.

The presented comparison covers the key parameters that determine the suitability of controllers for operation in intelligent microclimate control systems. Closed platforms with fixed functionality limit flexibility and complicate the integration of modern data processing methods, whereas open systems based on Linux create conditions for scalability, network interaction, and the implementation of complex algorithms.

In this context, the KSP-08.L controller is distinguished by its open architecture, Python support, and the ability to implement web-oriented and SCADA solutions without additional hardware modules. The availability of Ethernet and RS-485 interfaces simplifies integration into industrial infrastructure and ensures interaction with data acquisition modules, sensors, and executive mechanisms. The embedded HMI enables local monitoring, parameter configuration, and real-time observation of system response.

Considering the combination of functionality, openness of the software platform, and cost, the KSP-08.L is an optimal basis for implementing a hardware–software module for intelligent microclimate control under industrial conditions.

Data acquisition tools are a key element of the hardware–software module, as they determine measurement accuracy, system response speed, and data quality for control algorithms. For comparison, several typical data acquisition modules from different manufacturers were selected.

The comparison shows that commercial modules are often characterized either by excessive orientation toward discrete channels with limited analog capabilities or, conversely, by support for several analog inputs with a lack of discrete signals. This complicates the connection of temperature, humidity, pressure, and gas composition sensors, which require the simultaneous operation of different types of channels. In addition, many modules provide only basic filtering functions, which creates an additional load on the controller and affects system performance.

The MP100-24.02.2 module is distinguished by a balanced configuration that includes integrated discrete and analog inputs and outputs with support for standard signal ranges. The presence of built-in digital filtering mechanisms ensures measurement stability under electromagnetic interference conditions. Support for industrial interfaces enables synchronized data exchange with the controller and minimizes information transmission delays, which is critical for real-time systems.

Due to the combination of functionality, performance, and the possibility of direct integration with sensor and executive devices, the MP100-24.02.2 module is an effective solution for intelligent microclimate control systems in industrial environments.

The sensor subsystem provides measurement of the main microclimate parameters and forms streams of primary data for further processing. Its quality determines the system’s ability to respond promptly to disturbances, maintain a stable operating mode, and ensure correct operation of control algorithms. The subsystem is based on sensors of temperature, humidity, gas composition,

Table 1. Comparison of technical characteristics of controllers with HMI

Characteristics	AKYTEC KSP-08.L	Siemens KP700 Comfort	Schneider HMIGTO4310
Display	8", 1024×768	7", 800×480	7.5", 640×480
Processor	up to 1.8 GHz	500 MHz	333 MHz
Memory	2-4GB RAM, 64GB SSD	12 MB, SD card	96MB Flash, SD 4GB
OS / Software	Linux (Python, SCADA)	WinCC	Vijeo Designer
Interfaces	Ethernet, RS-485, USB	PROFINET, Ethernet	Ethernet, Modbus
Price (UAH)	28 300	48 900	49 749

Table 2. Comparison of data acquisition modules from different manufacturers

Signal type / Modules	AKYTEC MP100-24.02.2	Siemens SM modules	Schneider TM3
Discrete inputs	built-in	SM1223 (8DI+8DO)	TM3DI
Discrete outputs	built-in	–	TM3DQ
Analog inputs	built-in	SM1231	TM3AI
Analog outputs	built-in	SM1234	TM3AQ
Rated price	12 960 UAH	high range	medium range

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

and pressure, which must provide high accuracy, fast response, and resistance to industrial conditions, including vibration, dust, and humidity fluctuations.

Temperature sensors must ensure a linear characteristic and stability over a wide operating range, while combined temperature and humidity sensors should have minimal response time and protection against contamination. Gas composition sensors impose increased requirements on calibration stability and resistance to electromagnetic interference, which is critical for systems in which air exchange is regulated according to air quality characteristics. Pressure sensors provide differential pressure control and enable stabilization of airflow.

For compatibility with the data acquisition module, sensors must operate within standardized ranges of 4–20 mA or 0–10 V, and their design must meet IP protection requirements. In the case of digital sensors, response speed and compliance with data exchange protocols are important. The combination of these characteristics defines the requirements for the sensor subsystem, which must ensure accurate and reliable measurements under dynamic industrial conditions.

The executive subsystem forms the physical level of influence on environmental parameters and ensures the implementation of control actions generated by the controller. It includes fans, air damper actuators, and heating elements, each of which has its own dynamic characteristics and requirements for control algorithms.

Supply air dampers are equipped with servo actuators that provide precise damper positioning and stable air exchange. They can operate in discrete or continuous modes, allowing adaptation to rapidly changing conditions. Ventilation equipment is represented by fans with discrete switching and units with smooth speed control driven by variable frequency drives. Smooth regulation of fan performance ensures stable airflow, reduces microclimate parameter fluctuations, and improves energy efficiency.

Heating elements ensure temperature maintenance under heat loss conditions or seasonal variations of the external environment. They can operate in discrete or proportional modes, which helps prevent overheating and reduces energy consumption.

Coordinated interaction of all executive mechanisms, supported by feedback, forms a closed control loop that ensures microclimate stability and creates a foundation for further implementation of intelligent algorithms.

Algorithmic logic of module operation. The algorithmic part of the hardware–software module ensures the generation of control actions in accordance with the current microclimate parameters and specified technological requirements. The system is based on feedback principles, through which the controller evaluates deviations of parameters from setpoints and initiates appropriate actions of the executive mechanisms. The control logic is aimed at smooth regulation, avoidance of excessive cycling, and reduction of energy consumption while maintaining stable conditions in the industrial premises.

The central element of the system is the temperature control loop. Heating control is performed based on the temperature error: when the temperature falls below the allowable range, heating elements are activated to provide a gradual increase in temperature. A hysteresis mechanism defines the range between heater switching on and off points, preventing frequent switching and reducing equipment wear. After reaching the upper setpoint limit, the system switches off heating and enters a standby mode, minimizing intervention under stable conditions.

The cooling logic is based on a comprehensive assessment of temperature, humidity, and the influence of the external environment. When the temperature exceeds the set threshold, the system activates ventilation or other cooling mechanisms, gradually reducing the temperature to the operating range. Consideration of humidity helps avoid undesirable fluctuations of this parameter, while responsiveness to outdoor temperature ensures adaptation to changing environmental conditions. In cases of simultaneous increases in temperature and humidity, the system transitions to a more intensive air exchange mode.

The operation of the ventilation subsystem is based on a combination of temperature, humidity, and pressure criteria. The system can employ both discrete fan on/off control and smooth speed regulation using variable frequency drives. Smooth regulation enables more precise adaptation of air exchange intensity to changing conditions, reduces microclimate parameter fluctuations, and improves energy efficiency.

The control logic for supply air dampers is based on evaluating the pressure difference between the indoor and outdoor environments. When internal pressure increases, the dampers open to provide air inflow, whereas when it decreases, they partially close. Control can be implemented in either discrete or continuous modes, allowing precise dosing of the supply air volume and maintaining coordinated operation with the ventilation equipment.

The system includes emergency state control mechanisms that ensure timely detection of critical deviations and faults. In the event of a sharp temperature rise, pressure drop, loss of sensor signals, or failure of executive mechanisms, the system transitions to a safe operating mode, generates an alarm signal, and limits the action of regulating elements. This prevents equipment overload, overheating, and undesirable pressure differentials, thereby ensuring the stability of the technological process.

The coordinated interaction of all control loops – heating, cooling, ventilation, and pressure control–forms

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

a closed regulation cycle that ensures microclimate stability and creates prerequisites for the further implementation of intelligent control algorithms.

FULL-SCALE TESTING OF THE HARDWARE–SOFTWARE MODULE. Full-scale testing was conducted to evaluate the practical effectiveness of the hardware–software module and to determine its ability to maintain stable microclimate parameters under real industrial operating conditions. The tests were carried out at an operating facility with a large internal volume and significant thermal and airflow loads, which ensured representative operating conditions. The premises were equipped with fans, supply air ducts with servo actuators, and electric heaters, while their structural features imposed increased requirements on the control system due to potential heat losses and variable technological influences.

During the tests, the module operated in a fully automatic mode, analyzing signals from temperature, humidity, pressure, and gas sensors and generating control actions in accordance with the implemented logic. The operation included both periods of steady-state conditions and abrupt changes in external factors, such as fluctuations in outdoor air temperature, variations in air exchange, and changes in thermal load. This made it possible to evaluate the accuracy, response speed, and adaptability of the system under conditions close to real operating scenarios.

To analyze the module operation, continuous real-time data acquisition was organized. The controller generated time series of measurements with a predefined sampling rate and synchronized them with the states of the executive mechanisms. Temperature, humidity, internal pressure, air gas composition, as well as control commands for heaters, fans, and servo actuators were recorded. This approach provided a comprehensive view of the interaction between subsystems and enabled assessment of time delays between parameter changes and equipment response.

The sampling period was selected to ensure sufficient temporal resolution of measurements without overloading computational resources. The recording interval was several seconds, which allowed capturing both gradual microclimate changes and rapid transient processes associated with changes in the operating modes of executive mechanisms. The collected data formed the basis for further analysis of system stability, accuracy, and reliability under industrial conditions.

Structured real-time logging of parameters enabled the construction of graphical dependencies reflecting system behavior during operation. Figure 2 presents a key fragment of temperature dynamics obtained over a daily period in the autumn season, when external conditions are characterized by moderate fluctuations.

The graph demonstrates a typical daily temperature variation: during daytime, a natural increase is observed due to solar heat gains, which causes a partial exceedance of the upper hysteresis limit and activation of the cooling subsystem. The temperature decrease occurs smoothly, without abrupt changes, indicating stable regulation. In the evening and at night, the outdoor air temperature decreases, leading to cooling of the indoor environment and activation of the heating mode after crossing the lower hysteresis threshold. Heating is performed uniformly, without inertial spikes,

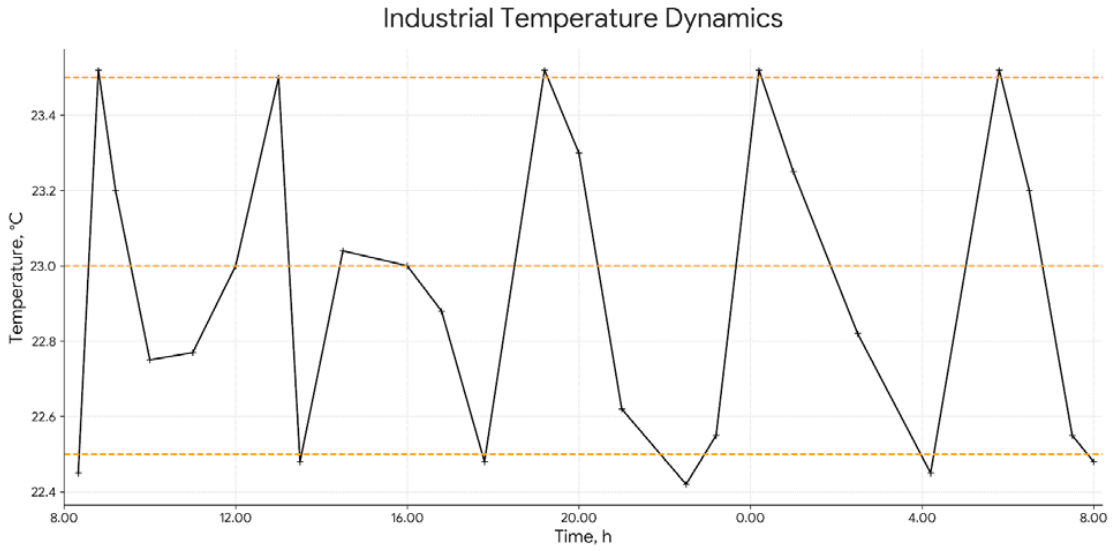

Fig. 2. Temperature dynamics in the industrial premises during full-scale testing

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

which confirms the correct operation of the temperature control loop.

The observed behavior corresponds to the algorithmic logic implemented in the system: cooling is activated only when the temperature actually exceeds the setpoint range, while heating is activated when it drops below the lower threshold. The absence of sharp peaks or dips in the graph indicates accurate interaction between the sensor and executive subsystems and an appropriate selection of hysteresis width. Analysis of the system response during periods of rapid changes in thermal load shows that the module promptly compensates for deviations, returning the temperature to the operating range without overshoot or excessive equipment activity.

The obtained results confirm the system’s ability to maintain stable microclimate parameters and adapt to dynamic technological conditions. The smooth operation of the heaters and the reduced number of switching events indicate the potential energy efficiency of the solution and reduced load on executive devices. This demonstrates the practical applicability of the module and its compliance with the requirements of industrial applications with variable thermal and airflow loads.

In the future, it is planned to expand the functionality of the hardware–software module by integrating predictive models, in particular neural network structures of the NNARX type, which will increase the accuracy of microclimate dynamics assessment and optimize control algorithms.

Discussion of the results obtained

The conducted full-scale tests showed that the hardware–software module provides stable temperature maintenance within the specified setpoint under real industrial disturbances, demonstrating coordinated operation of the sensor subsystem, executive mechanisms, and algorithmic control logic. The obtained parameter dynamics confirm the absence of abrupt fluctuations, the correct system response to changes in external conditions, and sufficient control accuracy for the use of the module in an industrial environment, which indicates the practical effectiveness of the proposed solution.

Conclusions

The conducted study confirmed the operability and effectiveness of the hardware–software module for intelligent microclimate control in industrial premises, which ensures temperature stability and coordinated operation of the sensor, computational, and executive subsystems under real operating conditions. The obtained results demonstrate the reliability of the proposed solution and create a foundation for further system improvement through the expansion of functional capabilities and enhancement of control accuracy.

Conflict of Interest

The authors declare that they have no conflicts of interest related to this study, including financial, personal, authorship, or any other interests that could have influenced the research or the results presented in this article.

Funding

This research was conducted without financial support.

Data Availability

The data will be provided upon reasonable request.

BIBLIOGRAPHY

[1] V. Ramachandra, “Artificial intelligence in climate science: A state-of-the-art review (2020–2025),” 2025. DOI: 10.31223/X5M73J.

[2] V. Warke, S. Kumar, A. Bongale, and K. Kotecha, “Sustainable development of smart manufacturing driven by the digital twin framework: A statistical analysis,” Sustainability, vol. 13, no. 18, p. 10139, 2021. DOI: 10.3390/su131810139.

[3] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, “An integrated outlook of cyber–physical systems for Industry 4.0: Topical practices, architecture and applications,” Green Technologies and Sustainability, vol. 1, no. 1, p. 100001, 2023. DOI: 10.1016/j.grets.2022.100001.

[4] K. Nesenbergs, E. Blumbergs, and P. Paikens, “Cyber-physical systems: Securing Latvia's future,” in Cybersecurity in Latvia. Routledge, pp. 233–263, 2025. DOI: 10.4324/9781003638858-11.

[5] I. Nevliudov, M. Omarov, V. Yevsieiev, A. Bronnikov, and V. Lyashenko, “Method of algorithms for cyber-physical production systems functioning synthesis,” International Journal of Emerging Trends in Engineering Research, 2020. DOI: 10.30534/ijeter/2020/1278102020.

[6] I. Nevliudov, V. Yevsieiev, J. H. Baker, M. A. Ahmad, and V. Lyashenko, “Development of a cyber design modeling declarative language for cyber-physical production systems,” Journal of Mathematical and Computational Science, vol. 11, no. 1, pp. 520–542, 2020. DOI: 10.28919/jmcs/5152.

[7] A. T. Abu-Jassar, H. Attar, V. Yevsieiev, A. Amer, N. Demska, A. K. Luhach, and V. Lyashenko, “Electronic user authentication key for access to HMI/SCADA via unsecured internet networks,” Computational Intelligence and Neuroscience, vol. 2022, no. 1, p. 5866922, 2022. DOI: 10.1155/2022/5866922.

[8] K. Kubiak, G. Dec, and D. Stadnicka, “Possible applications of edge computing in the manufacturing industry – systematic literature review,” Sensors, vol. 22, no. 7, p. 2445, 2022. DOI: 10.3390/s22072445.

[9] I. Nevliudov, V. Yevsieiev, S. Maksymova, N. Demska, K. Kolesnyk, and O. Miliutina, “Mobile robot navigation system based on ultrasonic sensors,” in Proc. IEEE DIPED, vol. 1, pp. 247–251, 2023. DOI: 10.1109/DIPED59408.2023.10269500.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

[10] K. Trenbath, R. Meyer, K. Woldekidan, K. Maisha, and M. Harris, “Commercial building sensors and controls systems–barriers, drivers, and costs,” National Renewable Energy Laboratory, 2022. DOI: 10.2172/1880546.

[11] I. Matetić, I. Štajduhar, I. Wolf, and S. Ljubic, “A review of data-driven approaches and techniques for fault detection and diagnosis in HVAC systems,” Sensors, vol. 23, no. 1, p. 1, 2022. DOI: 10.3390/s23010001.

[12] F. Bouzeffour and B. Khelidj, “An application of nonlinear autoregressive (NARX) model to predict adsorbent bed temperature of solar adsorption refrigeration system,” Journal of Systems Science and Systems Engineering, vol. 32, no. 6, pp. 687–707, 2023. DOI: 10.1007/s11518-023-5578-4.

[13] L. Zhang, Y. Sun, H. K. Lam, H. Li, J. Wang, and D. Hou, “Guaranteed cost control for interval type-2 fuzzy semi-Markov switching systems within a finite-time interval,” IEEE Transactions on Fuzzy Systems, vol. 30, no. 7, pp. 2583–2594, 2021. DOI: 10.1109/TFUZZ.2021.3089248.

[14] L. M. Escobar, J. Aguilar, A. Garces-Jimenez, J. A. G. De Mesa, and J. M. Gomez-Pulido, “Advanced fuzzy-logic-based context-driven control for HVAC management systems in buildings,” IEEE Access, vol. 8, pp. 16111–16126, 2020. DOI: 10.1109/ACCESS.2020.2966545.

[15] B. K. Park and C. J. Kim, “Short-term prediction for indoor temperature control using artificial neural network,” Energies, vol. 16, no. 23, p. 7724, 2023. DOI: 10.3390/en16237724.

[16] S. Singh, “Neuro-fuzzy architectures for interpretable AI: A comprehensive survey and research outlook,” Journal of Machine Learning Research, 2025.

[17] A. Gharbi, M. Ayari, N. Albalawi, Y. E. Touati, and Z. Klai, “Intelligent HVAC control: Comparative simulation of reinforcement learning and PID strategies for energy efficiency and comfort optimization,” Mathematics, vol. 13, no. 14, p. 2311, 2025. DOI: 10.3390/math13142311.

[18] K. Almazam, O. Humaidan, N. M. Shannan, F. M. Bashir, T. Gammoudi, and Y. A. Dodo, “Innovative energy efficiency in HVAC systems with an integrated machine learning and model predictive control technique,” Sustainability, vol. 17, no. 7, p. 2916, 2025. DOI: 10.3390/su17072916.

[19] J. O. Ojadi, C. S. Odionu, E. C. Onukwulu, and O. A. Owulade, “AI-enabled smart grid systems for energy efficiency and carbon footprint reduction in urban energy networks,” International Journal of Multidisciplinary Research and Growth Evaluation, vol. 5, no. 1, pp. 1549–1566, 2024.

[20] J. Ogundiran, E. Asadi, and M. Gameiro da Silva, “A systematic review on the use of AI for energy efficiency and indoor environmental quality in buildings,” Sustainability, vol. 16, no. 9, p. 3627, 2024. DOI: 10.3390/su16093627.

АПАРАТНО-ПРОГРАМНИЙ МОДУЛЬ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ МІКРОКЛІМАТОМ У ВИРОБНИЧИХ ПРИМІЩЕННЯХ

Владислав Євсєєв, Ігор Голод

У статті розглянуто проблему автоматизованого й інтелектуального керування мікрокліматом у виробничих приміщеннях, де стабільність температурно-вологісного режиму безпосередньо впливає на ефективність технологічних процесів, енергоощадність та надійність обладнання. Визначено, що традиційні системи регулювання, які базуються на спрощених лінійних моделях, не забезпечують необхідної точності в умовах багатофакторних збурень і динамічної зміни параметрів середовища. Метою дослідження є розробка апаратно-програмного модуля, здатного забезпечувати адаптивне, стійке й енергоефективне керування параметрами мікроклімату на основі узгодженої роботи сенсорних, обчислювальних та виконавчих підсистем.

Методика дослідження передбачає побудову структурної архітектури апаратно-програмного модуля, інтеграцію сенсорної системи, контролера з вбудованим HMI та виконавчих механізмів, а також формування алгоритмічної логіки регулювання температури, вологості, повітрообміну та внутрішнього тиску. У роботі застосовано методи аналізу та синтезу, математичне моделювання, а також експериментальні випробування у реальних виробничих умовах. Функціонування модуля перевірено завдяки безперервному збору даних, логуванню параметрів у реальному часі й оцінюванню реакції виконавчих механізмів на зміну зовнішніх і внутрішніх факторів.

Результати випробувань підтвердили здатність модуля підтримувати стабільні параметри мікроклімату в межах заданих уставок, забезпечуючи плавне перемикання між режимами нагріву, охолодження та вентиляції. Зареєстрована динаміка температури демонструє відсутність різких коливань, ефективну роботу гістерезисних механізмів та швидку реакцію системи на зміни навантаження. Практична придатність модуля підтверджена його стабільною роботою за умов добових коливань зовнішньої температури, наявності теплових збурень і варіацій повітрообміну. Вибрана комбінація обладнання (контролер КСП-08.L, модулі збору даних та сенсорні пристрої) забезпечила необхідну продуктивність, точність та гнучкість.

Перспективи подальших досліджень полягають у розширенні функціональності апаратно-програмного модуля шляхом інтеграції прогнозних

моделей, зокрема нейромережевих структур типу NNARX, що дасть можливість підвищити точність оцінювання динаміки мікроклімату й оптимізувати логіку керування у складних виробничих сценаріях. Отримані результати створюють основу для вдосконалення систем інтелектуального керування в промислових кіберфізичних комплексах та їх упровадження у різних галузях виробництва.

Ключові слова: *інтелектуальне керування, мікроклімат, апаратно-програмний модуль, кіберфізичні системи, сенсорна підсистема, виконавчі механізми, алгоритмічне регулювання, прогнозування параметрів.*

REFERENCES

[1] V. Ramachandra, “Artificial intelligence in climate science: A state-of-the-art review (2020–2025),” 2025. DOI: 10.31223/X5M73J.

[2] V. Warke, S. Kumar, A. Bongale, and K. Kotecha, “Sustainable development of smart manufacturing driven by the digital twin framework: A statistical analysis,” Sustainability, vol. 13, no. 18, p. 10139, 2021. DOI: 10.3390/su131810139.

[3] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, “An integrated outlook of cyber–physical systems for Industry 4.0: Topical practices, architecture and applications,” Green Technologies and Sustainability, vol. 1, no. 1, p. 100001, 2023. DOI: 10.1016/j.grets.2022.100001.

[4] K. Nesenbergs, E. Blumbergs, and P. Paikens, “Cyber-physical systems: Securing Latvia's future,” in Cybersecurity in Latvia. Routledge, pp. 233–263, 2025. DOI: 10.4324/9781003638858-11.

[5] I. Nevliudov, M. Omarov, V. Yevsieiev, A. Bronnikov, and V. Lyashenko, “Method of algorithms for cyber-physical production systems functioning synthesis,” International Journal of Emerging Trends in Engineering Research, 2020. DOI: 10.30534/ijeter/2020/1278102020.

[6] I. Nevliudov, V. Yevsieiev, J. H. Baker, M. A. Ahmad, and V. Lyashenko, “Development of a cyber design modeling declarative language for cyber-physical production systems,” Journal of Mathematical and Computational Science, vol. 11, no. 1, pp. 520–542, 2020. DOI: 10.28919/jmcs/5152.

[7] A. T. Abu-Jassar, H. Attar, V. Yevsieiev, A. Amer, N. Demska, A. K. Luhach, and V. Lyashenko, “Electronic user authentication key for access to HMI/SCADA via unsecured internet networks,” Computational Intelligence and Neuroscience, vol. 2022, no. 1, p. 5866922, 2022. DOI: 10.1155/2022/5866922.

[8] K. Kubiak, G. Dec, and D. Stadnicka, “Possible applications of edge computing in the manufacturing industry – systematic literature review,” Sensors, vol. 22, no. 7, p. 2445, 2022. DOI: 10.3390/s22072445.

[9] I. Nevliudov, V. Yevsieiev, S. Maksymova, N. Demska, K. Kolesnyk, and O. Miliutina, “Mobile robot navigation system based on ultrasonic sensors,” in Proc. IEEE DIPED, vol. 1, pp. 247–251, 2023. DOI: 10.1109/DIPED59408.2023.10269500.

[10] K. Trenbath, R. Meyer, K. Woldekidan, K. Maisha, and M. Harris, “Commercial building sensors and controls systems–barriers, drivers, and costs,” National Renewable Energy Laboratory, 2022. DOI: 10.2172/1880546.

[11] I. Matetić, I. Štajduhar, I. Wolf, and S. Ljubic, “A review of data-driven approaches and techniques for fault detection and diagnosis in HVAC systems,” Sensors, vol. 23, no. 1, p. 1, 2022. DOI: 10.3390/s23010001.

[12] F. Bouzeffour and B. Khelidj, “An application of nonlinear autoregressive (NARX) model to predict adsorbent bed temperature of solar adsorption refrigeration system,” Journal of Systems Science and Systems Engineering, vol. 32, no. 6, pp. 687–707, 2023. DOI: 10.1007/s11518-023-5578-4.

[13] L. Zhang, Y. Sun, H. K. Lam, H. Li, J. Wang, and D. Hou, “Guaranteed cost control for interval type-2 fuzzy semi-Markov switching systems within a finite-time interval,” IEEE Transactions on Fuzzy Systems, vol. 30, no. 7, pp. 2583–2594, 2021. DOI: 10.1109/TFUZZ.2021.3089248.

[14] L. M. Escobar, J. Aguilar, A. Garces-Jimenez, J. A. G. De Mesa, and J. M. Gomez-Pulido, “Advanced fuzzy-logic-based context-driven control for HVAC management systems in buildings,” IEEE Access, vol. 8, pp. 16111–16126, 2020. DOI: 10.1109/ACCESS.2020.2966545.

[15] B. K. Park and C. J. Kim, “Short-term prediction for indoor temperature control using artificial neural network,” Energies, vol. 16, no. 23, p. 7724, 2023. DOI: 10.3390/en16237724.

[16] S. Singh, “Neuro-fuzzy architectures for interpretable AI: A comprehensive survey and research outlook,” Journal of Machine Learning Research, 2025.

[17] A. Gharbi, M. Ayari, N. Albalawi, Y. E. Touati, and Z. Klai, “Intelligent HVAC control: Comparative simulation of reinforcement learning and PID strategies for energy efficiency and comfort optimization,” Mathematics, vol. 13, no. 14, p. 2311, 2025. DOI: 10.3390/math13142311.

[18] K. Almazam, O. Humaidan, N. M. Shannan, F. M. Bashir, T. Gammoudi, and Y. A. Dodo, “Innovative energy efficiency in HVAC systems with an integrated machine learning and model predictive control technique,” Sustainability, vol. 17, no. 7, p. 2916, 2025. DOI: 10.3390/su17072916.

[19] J. O. Ojadi, C. S. Odionu, E. C. Onukwulu, and O. A. Owulade, “AI-enabled smart grid systems for energy efficiency and carbon footprint reduction in urban energy networks,” International Journal of Multidisciplinary Research and Growth Evaluation, vol. 5, no. 1, pp. 1549–1566, 2024.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359113

[20] J. Ogundiran, E. Asadi, and M. Gameiro da Silva, “A systematic review on the use of AI for energy efficiency and indoor environmental quality in buildings,” Sustainability, vol. 16, no. 9, p. 3627, 2024. DOI: 10.3390/su16093627.

Дата першого надходження статті до видання: 03.02.2026
Дата прийняття статті до друку після рецензування: 28.02.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359117

УДК 004.94 004.89 664.1

АНАЛІЗ СИНГУЛЯРНОГО СПЕКТРА ВИТРАТИ ВОДИ ДИФУЗІЙНОЇ УСТАНОВКИ ЦУКРОВОГО ВИРОБНИЦТВА ДЛЯ ЗАДАЧ АВТОМАТИЗАЦІЇ

А.С. Горпинченко
Department of Automation and Computer Technologies for Control Systems named after Prof. A.P. Ladanuk, National University of Food Technologies, Kyiv, Ukraine
ORCID https://orcid.org/0009-0005-6190-7348
E-mail: antongorpinchenkodra@gmail.com

АНОТАЦІЯ

У роботі досліджено можливості застосування методу аналізу сингулярного спектра для обробки й аналізу часових рядів витрати води дифузійної установки в технологічному процесі виробництва цукру. Стабільність витрати води є важливим фактором ефективності дифузійного процесу, оскільки вона впливає на гідродинамічні умови екстракції сахарози, енергетичні витрати та загальну ефективність роботи обладнання. У реальних виробничих умовах сигнали технологічних параметрів містять значну кількість шумів, випадкових збурень і короткочасних аномалій, що ускладнює їх використання в системах автоматичного керування.

Під час дослідження використано метод аналізу сингулярного спектру, який належить до класу непараметричних методів аналізу часових рядів і дає можливість виділяти трендові, сезонні та шумові складові сигналу без необхідності попереднього припущення щодо математичної моделі процесу. Запропоновано послідовність практичного застосування методу, що містить етапи формування траєкторної матриці, виконання сингулярного розкладу, групування компонент і реконструкції сигналу за допомогою діагонального усереднення.

Проведено аналіз часових рядів витрати води з використанням вікна вкладення, що відповідає характерній періодичності процесу. На основі сингулярного спектра визначено основні компоненти, які формують структуру сигналу. Показано, що перші компоненти описують тренд та сезонні коливання технологічного процесу, тоді як інші компоненти характеризують випадкові шумові збурення.

Результати дослідження демонструють, що реконструкція сигналу на основі перших компонент дає змогу ефективно фільтрувати шум, зберігаючи основні закономірності зміни витрати води. Оцінювання якості реконструкції виконано за допомогою статистичних показників точності, зокрема середньої абсолютної похибки, середньоквадратичної похибки та середньої відносної похибки. Отримані результати підтверджують можливість використання методу аналізу сингулярного спектра для підвищення достовірності вимірювальних сигналів та їх подальшого використання в системах автоматичного керування, діагностики технологічного обладнання та прогнозування режимів роботи дифузійної установки.

Практична цінність роботи полягає у можливості інтеграції запропонованого підходу в програмно-технічні комплекси автоматизації цукрового виробництва для підвищення стабільності технологічних режимів та ефективності використання ресурсів.

Ключові слова: *аналіз сингулярного спектра, метод гусениці, часові ряди, дифузійна установка, витрата води, автоматизація цукрового виробництва, обробка сигналів, промислова автоматизація, статистичний аналіз даних, фільтрація сигналів, реконструкція часових рядів.*

Вступ

Цукрове виробництво належить до енерго- та ресурсоємних галузей харчової промисловості. Стабільність технологічних режимів на дифузійній дільниці суттєво впливає на вихід сахарози та витрати пари, води й електроенергії. Витрата води на дифузію є одним із ключових параметрів, що визначає гідродинамічні умови, інтенсивність масообміну та якість дифузійного соку. Для автоматизованих систем керування важливо мати сигнал витрати води з мінімальним впливом випадкових збурень, датчикового шуму та короткочасних аномалій.

Типові промислові дані мають складну структуру, що поєднує трендові компоненти, сезонні коливання

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359117

та випадкові збурення. Для моделювання й аналізу таких сигналів широко використовуються методи аналізу часових рядів, статистичні підходи та методи головних компонент [5], [6]. Вони поєднують повільний тренд, добові коливання, вплив режимів пуску та зупинки, а також нерегулярні відхилення, зумовлені зміною сировини та діями персоналу. Через це використання простих лінійних фільтрів або класичних авторегресійних моделей не завжди дає надійний результат. Перспективним підходом до аналізу складних часових рядів є аналіз сингулярного спектра, який у прикладній літературі часто називають методом гусениці. Цей метод поєднує ідеї спектрального аналізу та статистичного розкладу сигналів і широко використовується для виділення трендів, періодичних складових та шуму у часових рядах [1], [2].

Аналіз останніх досліджень і постановка задачі

Методи обробки сигналів у системах автоматизації традиційно передбачають згладжування, спектральний аналіз, фільтрацію Калмана й ідентифікацію моделей у просторі станів. Для процесів харчової промисловості характерні нелінійності, зміна параметрів у часі та періодичні впливи, що ускладнює побудову єдиної моделі. Аналіз сингулярного спектра розглядається як інструмент, який поєднує переваги статистичного підходу та спектрального розкладу, забезпечуючи адаптивне виділення компонент сигналу без попереднього припущення щодо моделі процесу [1], [3], [4].

Мета роботи полягає у розробленні та демонстрації інженерної методики застосування методу аналізу сингулярного спектра для часових рядів витрати води на дифузійну установку з отриманням числових показників якості реконструкції та рекомендацій для подальшого використання результатів у задачах автоматичного керування та діагностики, базується на перетворенні одновимірного часового ряду в багатовимірний за допомогою формування траєкторної матриці.

Матеріали та методи

Об'єктом дослідження є часовий ряд витрати води на дифузійну установку, отриманий із засобів вимірювання та реєстрації технологічних параметрів. У цьому матеріалі наведено демонстраційний фрагмент для ілюстрації розрахунків. Під час підготовки до подання в конкретний журнал таблицю та графік легко замінити на ряд із вашої системи Supervisory Control and Data Acquisition без зміни методики.

Вибрано дискретизацію один вимір на годину та тривалість спостереження три доби. Позначимо початковий ряд як *x* з індексом часу *t.*

Модельне подання сигналу в задачі розкладу має вигляд суми корисних складових та шуму [6], [7]:

$$x_t = y_t + e_t . \quad (1)$$

Тут *y* є сукупністю тренду та сезонних складових, а *e* – шумом і нерегулярними збуреннями. Метод аналізу сингулярного спектра виконується в чотири етапи: вбудовування, сингулярний розклад, групування компонент і діагональне усереднення.

Вбудовування та траєкторна матриця

Першим і фундаментальним етапом алгоритму аналізу сингулярного спектра є процедура вбудовування, яка полягає у відображенні вихідного одновимірного часового ряду в багатовимірний простір. Нехай маємо часовий ряд витрати води на дифузійну установку (2) загальною довжиною *N*, для реалізації процедури вбудовування потрібно визначити ціле число *L,* яке називається довжиною вікна (window length) (3) [7]:

$$F = (f_0, f_1, \ldots f_{N-1}), \quad (2)$$

$$1 < L < N . \quad (3)$$

Процес вбудовування перетворює часовий ряд у послідовність (4) векторів вбудовування (5) розмірності *L*:

$$K = N - L + 1 , \quad (4)$$

$$F = (f_{0-1}, \ldots, f_{i+L-2})^T . \quad (5)$$

Результатом цього кроку є формування траєкторної матриці *X* розміром *L+K*, яка має таку структуру (6):

$$X = [X_1 : \ldots : X_k] = \begin{pmatrix} f_0 & f_1 \cdots f_{K-1} \\ f_1 & f_2 \cdots f_K \\ \vdots & \vdots \ddots \vdots \\ f_{L-1} & f_L \cdots f_{N-1} \end{pmatrix} . \quad (6)$$

Траєкторна матриця *X* за своєю будовою є ганкелевою матрицею, оскільки вона має однакові елементи на діагоналях, що йдуть справа наліво. Це означає, що всі елементи x_{ij}, для яких $i + j$, є ідентичними.

Вибір довжини вікна *L* є найбільш критичним моментом на етапі вбудовування, оскільки цей параметр визначає здатність методу розділяти різні компоненти сигналу. З теоретичного погляду *L* має бути достатньо великим, щоб охопити основну динаміку процесу, але не перевищувати *N*. У контексті автоматизації цукрового виробництва, де процеси мають виражену циклічність, вікно *L* доцільно вибирати кратно очікуваній сезонності або періоду домінуючих коливань.

Для добового циклу спостережень із кроком дискретизації один вимір на годину оптимальними значеннями є *L = 24* або *L = 48*. Такий вибір дає можливість матриці «акумулювати» інформацію про добові ритми споживання води та технологічні зміни протягом зміни. У цій науковій роботі прийнято значення L = 24, що забезпечує адекватне розбиття сигналу на

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359117

низькочастотний тренд, добову періодику та високочастотний шум. Формування такої матриці дає змогу на наступних етапах застосувати апарат сингулярного розкладу для виявлення прихованих закономірностей у динаміці витрати води, які є невидимими за стандартного візуального аналізу часового ряду (7):

$$X=[x_1...x_K]. \quad (7)$$

Сингулярний розклад

На другому етапі алгоритму виконується сингулярний розклад (Singular Value Decomposition) сформованої траєкторної матриці *X*. Ця процедура є еквівалентною розкладу вихідного сигналу на систему ортогональних компонент у просторі вкладених векторів [5]. Математично цей процес подається у вигляді добутку трьох матриць (8):

$$X=U\sum V^T. \quad (8)$$

Відповідно *U* – ортогональна матриця розміром *L*, стовпці якої є лівими сингулярними векторами (власними векторами матриці XX^T); *V* – ортогональна матриця розміром K, що містить праві сингулярні вектори; $\sum$ –діагональна матриця розміром $L \times K$, на головній діагоналі якої розташовані невід’ємні сингулярні значення S_i, впорядковані за спаданням (9):

$$(s_i \geq s_2 \geq \cdots \geq s_L \geq 0). \quad (9)$$

Діагональні елементи матриці відіграють ключову роль у структурному аналізі часового ряду витрати води. Кожне сингулярне значення характеризує масштаб відповідної компоненти розкладу. Квадрати сингулярних значень, які часто позначають як власні числа (10)

$$\lambda_i=s_i^2, \quad (10)$$

є прямо пропорційними внеску відповідних компонент у загальну дисперсію досліджуваного сигналу. Аналіз сингулярного спектра дає змогу ідентифікувати структуру ряду: великі сингулярні значення зазвичай відповідають головним компонентам – низькочастотному тренду та періодичним гармонікам, тоді як довга ланка малих значень свідчить про наявність випадкового шуму та збурень.

Для потреби в автоматизації технологічного процесу такий розклад є корисним, оскільки він дає можливість перейти від спотвореного шумом часового ряду до його енергетичного представлення [8], [9]. Власні вектори U_i визначають форму коливань, а головні компоненти відображають динаміку цих коливань у часі. Таким чином, сингулярний розклад виступає адаптивним фільтром, який самостійно підлаштовується під специфіку даних конкретної дифузійної установки, не вимагаючи від розробника точного знання частотних характеристик процесу.

Внесок *i* компоненти в загальну структуру сигналу в процентах обчислюється (11):

$$p_i=\frac{^s i}{\sum_{j=1}^{s} d_j}*100\%. \quad (11)$$

Такий підхід забезпечує високу роздільну здатність методу та дає можливість ефективно відокремити детерміновану частину витрати води від стохастичних збурень, що є критичним для стабілізації роботи контурів регулювання.

Компоненти об’єднують у групи, які відповідають тренду, сезонності та шуму. Практичне правило полягає у виборі першої компоненти як тренду та парних компонент як сезонних гармонік, якщо в сингулярному спектрі спостерігаються близькі значення та характерні коливальні власні вектори.

Для кожної групи формується матриця відновлення як сума елементарних матриць. Після цього застосовується діагональне усереднення, яке перетворює матрицю назад у часовий ряд. Підсумковий реконструйований сигнал дорівнює сумі відновлених груп тренду та сезонності (12):

$$x^{\circ}=x\_trend+x\_season. \quad (12)$$

Якість реконструкції оцінено за середньою абсолютною похибкою MAE (13), коренем середньоквадратичної похибки RMSE (14) та середньою відносною похибкою MAPE (15). Для уникнення неоднозначностей у записі введемо допоміжні величини [11], [13]:

$$a_t=x_t-x_t^{\circ}$$
$$MAE=\frac{1}{N}\sum_{t=1}^{N} a_t, \quad (13)$$

$$b_t=x_t-x_t^{\circ 2}$$
$$RMSE=\frac{1}{N}\sum_{t=1}^{N} b_t, \quad (14)$$

$$^C t=\frac{a_t}{x_t}$$
$$MAPE=100\frac{1}{N}\sum_{t=1}^{N} {}^C t. \quad (15)$$

Результати та їх аналіз

Після побудови траєкторної матриці з параметром L, що дорівнює 24, виконано сингулярний розклад та обчислено внесок перших компонент у сумарну енергію сигналу. Для практичного використання важливо контролювати, щоб перші компоненти відповідали фізичним закономірностям процесу, а не випадковим пікам. У демонстраційному прикладі перша компонента відображає тренд, друга та третя

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359117

компоненти утворюють сезонну пару, інші компоненти переважно описують шум.

Таблиця 1 містить значення часток дисперсії для перших десяти компонент, а також накопичену частку. Це дає можливість обґрунтувати вибір числа компонент для реконструкції.

За даними таблиці 1, перші три компоненти описують основну структуру сигналу. Реконструкцію виконано як суму тренду та сезонності, що відповідає компонентам 1, 2 та 3.

За вибраною реконструкцією отримано такі показники точності: середня абсолютна похибка дорівнює 1,128 м3 на год, корінь середньоквадратичної похибки дорівнює 1,490 м3 на год, середня відносна похибка – 1,859 відсотка. Невелика відносна похибка свідчить, що відновлений сигнал зберігає фізично значущі коливання та є придатним для використання в автоматичних контурах керування.

На рис. 1 показано початковий часовий ряд і реконструкцію сигналу. Видно, що реконструкція

Табл. 1. Внесок перших компонент методу аналізу сингулярного спектра в дисперсію сигналу витрати води

Номер компоненти	Сингулярне значення s	Частка дисперсії p, відсотків	Накопичено, відсотків
1	2085,346	99,78	99,78
2	57,780	0,08	99,86
3	56,686	0,07	99,93
4	27,648	0,02	99,95
5	27,324	0,02	99,96
6	13,774	0,00	99,97
7	12,782	0,00	99,97
8	10,922	0,00	99,97
9	10,527	0,00	99,98
10	10,282	0,00	99,98

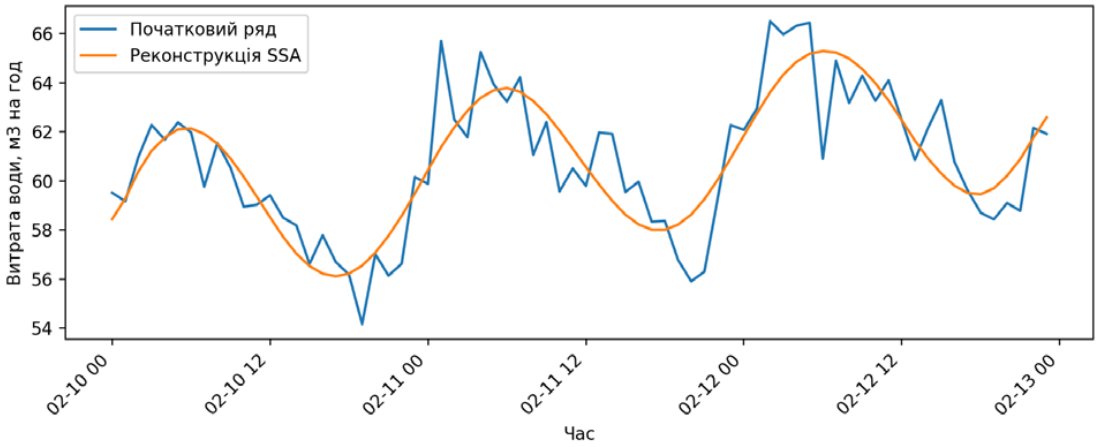

Рис. 1. Початковий часовий ряд витрати води та реконструкція методом аналізу сингулярного спектра

згладжує випадкові коливання та локальні викиди, зберігаючи тренд і добову сезонність. Це зменшує ризик помилкових спрацьовувань регуляторів та підвищує стабільність технологічного режиму.

Практичні рекомендації для впровадження у системі автоматизації

Для інтеграції методу аналізу сингулярного спектра в програмно-технічний комплекс рекомендовано реалізувати алгоритм як окремий модуль обробки сигналів. Вхідними даними є масив значень витрати води з буфера архіву, виходом є очищений сигнал і показники якості. Оновлення доцільно виконувати ковзним вікном із кроком один вимір.

Довжину вікна L слід узгоджувати із характерним періодом коливань. Для добової сезонності за годинної дискретизації рекомендовано L, що дорівнює 24. Для більш складних режимів можна застосовувати L, що дорівнює 48. Занадто мале L

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359117

призводить до змішування сезонності із шумом, занадто велике L знижує стійкість оцінок у разі коротких вибірок.

Групування компонент варто виконувати на основі двох критеріїв: частка дисперсії та форма власних векторів. Для промислової експлуатації зручно фіксувати правило: перша компонента відповідає тренду, друга та третя компоненти відповідають сезонності, інші компоненти відкидаються як шум. Далі правило уточнюють на основі архівних даних за декілька змін і для різних типів навантаження.

Отриманий очищений сигнал може бути використаний для підвищення енергоефективності виробництва й оптимізації режимів роботи технологічного обладнання відповідно до сучасних стандартів управління енергоспоживанням [15].

Висновки

1. Виконано обґрунтування використання аналізу сингулярного спектру для обробки часових рядів витрати води дифузійної установки цукрового виробництва.

2. Запропоновано інженерну методику налаштування методу аналізу сингулярного спектра з вибором довжини вікна, сингулярним розкладом і групуванням компонент для виділення тренду та сезонності.

3. Для демонстраційного фрагмента даних, якщо L дорівнює 24, реконструкція за першими трьома компонентами забезпечила середню абсолютну похибку 1,128 м3 на год, корінь середньоквадратичної похибки – дорівнює 1,490 м3 на год, середня відносна похибка – 1,859 відсотка.

4. Показано, що очищений сигнал придатний для застосування в контурах автоматичного керування та діагностики, а підхід може бути перенесений на суміжні задачі, зокрема на керування активною вентиляцією цукрового буряка.

Конфлікт інтересів

Автор декларує, що не має конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, який міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] N. Golyandina, Analysis of Time Series Structure. SSA and Related Techniques. Boca Raton, FL, USA: Chapman and Hall/CRC, 2001. DOI: 10.1201/9781420035841.

[2] N. Golyandina and A. Zhigljavsky, Singular Spectrum Analysis for Time Series. Berlin, Heidelberg: Springer, 2013. DOI: 10.1007/978-3-642-34913-3.

[3] H. Hassani, “Singular Spectrum Analysis: Methodology and Comparison,” Journal of Data Science, vol. 5, no. 2, pp. 239–257, 2007. DOI: 10.6339/JDS.2007.05(2).396.

[4] R. Vautard and M. Ghil, “Singular spectrum analysis in nonlinear dynamics,” Physica D, vol. 35, no. 3, pp. 395–424, 1989. DOI: 10.1016/0167-2789(89)90077-8.

[5] T. Jolliffe, Principal Component Analysis. New York, NY, USA: Springer, 2002. DOI: 10.1007/b98835.

[6] G. E. P. Box, G. M. Jenkins, G. C. Reinsel, and G. M. Ljung, Time Series Analysis: Forecasting and Control. Hoboken, NJ, USA: Wiley, 2015.

[7] D. C. Montgomery, Introduction to Statistical Quality Control. Hoboken, NJ, USA: Wiley, 2019.

[8] K. Ogata, Modern Control Engineering. Upper Saddle River, NJ, USA: Pearson, 2010.

[9] D. E. Seborg, T. F. Edgar, and D. A. Mellichamp, Process Dynamics and Control. Hoboken, NJ, USA: Wiley, 2011.

[10] ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ: Держспоживстандарт України, 2015.

[11] В. Крупко, Автоматизація технологічних процесів харчових виробництв. Навчальний посібник. Київ: Видавництво, 2018.

[12] О. Якубенко, Технологія цукру. Дифузійні процеси та режими. Харків: Видавництво, 2016.

[13] С. Бойко, Системи автоматичного керування. Теорія і практика. Львів: Видавництво, 2017.

[14] І. Левченко, Методи фільтрації та обробки сигналів у системах керування. Одеса: Видавництво, 2020.

[15] ISO 50001 Energy management systems. Requirements with guidance for use. International Organization for Standardization, 2018.

ANALYSIS OF THE SINGULAR SPECTRUM OF WATER CONSUMPTION IN A DIFFUSION UNIT OF A SUGAR PRODUCTION PLANT FOR AUTOMATION APPLICATIONS

Anton Horpynchenko

This paper investigates the application of Singular Spectrum Analysis for processing time series of water flow rate in a diffusion unit of sugar production. Stable water flow is an important factor affecting the efficiency of the diffusion process, since it influences hydrodynamic conditions, sucrose extraction efficiency, and energy consumption of the technological equipment. In industrial environments, measurement signals often contain noise, random disturbances, and short term anomalies, which complicates their direct use in automatic control systems.

The study applies Singular Spectrum Analysis as a non parametric method for time series decomposition that allows separating trend, periodic components, and

noise without assuming a predefined mathematical model of the process. A practical implementation procedure is proposed, including trajectory matrix construction, singular value decomposition, component grouping, and signal reconstruction using diagonal averaging.

Experimental analysis of water flow rate data demonstrates that the leading components represent the main physical structure of the signal, including trend and seasonal variations, while higher order components correspond to noise. Reconstruction based on the dominant components significantly reduces random disturbances while preserving the informative dynamics of the technological process.

The quality of reconstruction is evaluated using statistical accuracy indicators such as Mean Absolute Error, Root Mean Square Error, and Mean Absolute Percentage Error. The obtained results confirm that Singular Spectrum Analysis can effectively improve the reliability of measurement signals and may be applied in industrial automation systems for control, diagnostics, and forecasting of diffusion unit operating modes.

Keywords: *singular spectrum analysis, the Gusenitsa method, time series, diffusion unit, water flow rate, sugar production automation, signal processing, industrial automation, statistical data analysis, signal filtering, time series reconstruction.*

REFERENCES

[1] N. Golyandina, Analysis of Time Series Structure. SSA and Related Techniques. Boca Raton, FL, USA: Chapman and Hall/CRC, 2001. DOI: 10.1201/9781420035841.
[2] N. Golyandina and A. Zhigljavsky, Singular Spectrum Analysis for Time Series. Berlin, Heidelberg: Springer, 2013. DOI: 10.1007/978-3-642-34913-3.
[3] H. Hassani, “Singular Spectrum Analysis: Methodology and Comparison,” Journal of Data Science, vol. 5, no. 2, pp. 239–257, 2007. DOI: 10.6339/JDS.2007.05(2).396.
[4] R. Vautard and M. Ghil, “Singular spectrum analysis in nonlinear dynamics,” Physica D, vol. 35, no. 3, pp. 395–424, 1989. DOI: 10.1016/0167-2789(89)90077-8.
[5] T. Jolliffe, Principal Component Analysis. New York, NY, USA: Springer, 2002. DOI: 10.1007/b98835.
[6] G. E. P. Box, G. M. Jenkins, G. C. Reinsel, and G. M. Ljung, Time Series Analysis: Forecasting and Control. Hoboken, NJ, USA: Wiley, 2015.
[7] D. C. Montgomery, Introduction to Statistical Quality Control. Hoboken, NJ, USA: Wiley, 2019.
[8] K. Ogata, Modern Control Engineering. Upper Saddle River, NJ, USA: Pearson, 2010.
[9] D. E. Seborg, T. F. Edgar, and D. A. Mellichamp, Process Dynamics and Control. Hoboken, NJ, USA: Wiley, 2011.
[10] DSTU 8302:2015 Information and documentation. Bibliographic reference. General provisions and rules of composition. Kyiv: Derzhspozhyvstandard of Ukraine, 2015.
[11] V. Krupko, Automation of technological processes in food production. Textbook. Kyiv: Vydavnytstvo, 2018.
[12] O. Yakubenko, Sugar technology. Diffusion processes and modes. Kharkiv: Vydavnytstvo, 2016.
[13] S. Boiko, Automatic control systems. Theory and practice. Lviv: Vydavnytstvo, 2017.
[14] I. Levchenko, Methods of filtering and signal processing in control systems. Odesa: Vydavnytstvo, 2020.
[15] ISO 50001:2018, Energy management systems – Requirements with guidance for use. International Organization for Standardization, 2018.

Дата першого надходження статті до видання: 12.02.2026
Дата прийняття статті до друку після рецензування: 05.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

Інформаційні технології

УДК 681.03

ЗАСТОСУВАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ ДЛЯ РОЗВ’ЯЗАННЯ ЗАДАЧ БАГАТОКРИТЕРІАЛЬНОГО ВИБОРУ ДЛЯ ФОРМУВАННЯ СКЛАДУ ЕКСПЕРТНИХ ГРУП

І.Н. Вдовиченко, О.М. Маркова
Department of Computer Systems and Networks, Kryvyi Rih National University, Kryvyi Rih, Ukraine
ORCID https://orcid.org/0000-0003-0953-655X
ORCID https://orcid.org/0000-0002-5236-6640
E-mail: vivin2015@nu.edu.ua

АНОТАЦІЯ

Статтю присвячено розв’язанню актуальної науково-прикладної задачі – розробці й обґрунтуванню комбінованого методу формування експертних груп, алгоритм роботи якого інтегрує статистичні підходи, математичне моделювання, методи експертних оцінок та апарат генетичних алгоритмів. У роботі обґрунтовано необхідність оптимізації процесу відбору експертів для мінімізації помилок під час проведення експертизи.

Запропоновано комплексну схему формування оптимального складу експертної групи, яка базується на системному поєднанні кількісних та якісних показників. У межах дослідження формалізовано складну оптимізаційну задачу багатокритеріального підбору фахівців для проведення технічних, соціальних та економічних експертиз. Представлено схему комбінації статистичних методів та генетичного алгоритму для формування експертних груп. Математична модель задачі базується на максимізації цільової функції, що враховує низку критичних параметрів: індивідуальний індекс компетентності експерта, коефіцієнт професійного досвіду, ступінь узгодженості попередніх оцінок кандидата та ін.

Особливу увагу приділено застосуванню генетичних алгоритмів для пошуку оптимальних рішень у великому просторі альтернатив. Використання еволюційних механізмів відбору, мутації та кросинговеру дає можливість ефективно вирішувати задачу багатокритеріального вибору, забезпечуючи високу точність формування груп. Отримані результати підтверджують, що синтез генетичних алгоритмів з експертними та математичними методами дає змогу суттєво підвищити надійність прогнозів та оптимізує прийняття рішень.

Ключові слова: *генетичні алгоритми, експертиза, експертна група, комбінований метод, експертна оцінка оптимальне рішення, багатокритеріальна оптимізація, склад групи, математичні, статистичні методи, хромосоми, ген, схрещення, мутація, цільова функція.*

Вступ

Теорія оптимізації охоплює практично всі сфери людської діяльності, виходячи далеко за межі суто технічних завдань. Одним із перспективних інструментів тут стали генетичні алгоритми (ГА) як один із ключових методів еволюційних обчислень. Однак, попри свою ефективність у пошуку оптимальних рішень, вони мають і недоліки: складність обробки нелінійних функцій через ризик потрапляння в локальні екстремуми та стрімке зростання обчислювальних витрат у разі збільшення кількості параметрів.

Останнім часом важливість завдань, коли доводиться вибирати компромісні рішення щодо складних об’єктів, значно зросла. Це пояснюється зростанням динамізму довкілля та зменшенням періоду часу на аналіз ситуації прийняття рішень. Також розвиток науки і техніки призвів до появи великої кількості альтернативних варіантів вибору. Далися взнаки і збільшення взаємозалежності різних рішень та їх наслідків, зросла і складність варіантів прийнятих рішень. У цих умовах для прийняття рішень дедалі частіше використовуються експертизи. Експертні методи є ефективним інструментом аналізу об’єктів, побудови прогнозів, визначення їхньої якості та цінності.

Як показує практика, не так просто інтуїтивні й евристичні рішення різних завдань отримати за

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

допомогою формалізованих розрахункових методів. У складних сферах життєдіяльності людини створення експертних систем – завдання неймовірно важке. Проблема полягає в тому, щоб отримати знання від експертів, і в тому, щоб формалізувати їх знання, упорядкувати та передбачити адекватну відповідь на поставлене запитання. Певні експертні методи застосовують тоді, коли використання інших виявляється неможливим чи не економічним, за їх допомогою намагаються досліджувати й моделювати процес людського мислення.

Аналіз літературних даних і постановка проблеми

Експертизі, як комплексу логічних та математико-статистичних методів організації роботи зі спеціалістами-експертами й обробки думок експертів, виражених у кількісній або якісній формі, приділено багато уваги в роботах науковців. Такі вчені, як Ю. І. Саенко В. М. Ворона, Ю. М. Бородянский, з київського інституту кібернетики та київського інституту соціології, неодноразово в своїх роботах порушували питання проблем і класифікації експертних методів. Вони відмічали, що застосування експертних методів є актуальним в оцінці багатьох процесів.

Питання використання генетичних алгоритмів для вирішення задач оптимізації (до яких і належать багато завдань експертизи) розглядалися на форумах і в науковій літературі вже декілька років.

В. О. Бабенко, О. К. Носовець у роботі [1] пропонують алгоритм для знаходження рішень багатокритеріальної задачі оптимізації, комбінуючи метод аналізу ієрархій та генетичні алгоритми.

Т. Л. Будорацька, Н. М. Журавльова в роботі [2] відмічають, що результати, отримані із застосуванням ГА, наближені до показників, розрахованих класичними методами, а в деяких випадках рішення є оптимальнішим.

К. В. Колесніков у роботі «Генетичні алгоритми для задач багатокритеріальної оптимізації в мережах адаптивної маршрутизації даних» демонструє застосування генетичних алгоритмів для розв’язання складних оптимізаційних задач, зокрема пошуку шляхів за кількома критеріями. Очевидно, що наукові роботи підтверджують актуальність питання, але вирішення проблеми формування експертної групи на базі генетичного алгоритму не розглядалося.

Мета та задачі дослідження

Мета дослідження полягає в аналізі особливостей використання генетичного алгоритму для розв’язання оптимізаційних задач багатокритеріального вибору альтернатив і проведення експерименту.

Звідси випливає, що мета роботи полягає у дослідженні стану питання експертизи, побудові комплексної методики багатокритеріального оцінювання альтернатив та можливості застосуванні її для формування експертної групи.

Для досягнення мети дослідження, потрібно виконати такі завдання:

– проаналізувати запропонований алгоритм формування експертної групи на базі математичних методів;

– дослідити використання основних принципів роботи генетичних алгоритмів і методів їх застосування під час розв’язання оптимізаційних багатокритеріальних задач;

– розробити алгоритм, який комбінує статистичні, математичні й експертні методи з використанням генетичного підходу, для покращення результатів оптимізації;

– провести серію експериментів для визначення ефективності запропонованого алгоритму в задачі формування складу експертної групи;

– зробити порівняльний аналіз отриманих результатів з більш традиційними, розробленими автором раніше, підходами розв’язування задачі формування складу експертних груп.

Матеріали та методи досліджень

Натомість експертиза не може розглядатися як вичерпний рівень аналізу. Актуальним стає прагнення поєднувати експертизу з фундаментальними дослідженнями. Складності, що виникають у процесі здійснення експертизи, визначаються насамперед тим, що функціонування об’єкта що підлягає експертизі, відбувається під впливом великої кількості факторів. Однак за традиційного підходу немає об’єктивної впевненості в тому, що вибраний варіант, дійсно, є кращим. Ба більше, в умовах багатоваріантності та пов’язаного із цим (за законами комбінаторики) зростання потенційно можливих варіантів рішень дійсно оптимальний варіант може зникнути з поля зору дослідників та експертів.

З огляду на це виникає потреба в розробці науково обґрунтованої методології та принципів проведення експертизи, застосування яких можливе лише в разі широкого використання математичних методів та ПЕОМ. Головні труднощі – відсутність математичних і формально логічних засобів, здатних із достатньою точністю відобразити в кількісних показниках якісний зміст процесів.

Незважаючи на успіхи, досягнуті в останні роки в розробці та практичному використанні методу експертних оцінок, є низка проблем і завдань, що потребують подальших методологічних досліджень та практичної перевірки. Одне з найважливіших питань – формування експертних груп. Необхідно вдосконалювати систему відбору експертів. Очевидно, що має бути створений узагальнений метод

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

відбору експертів, у якому були б використані всі позитивні особливості існуючих експертних, статистичних методів, методів штучного інтелекту та виключені їхні недоліки.

Формування складу експертної групи, стандартний підхід

Ми пропонуємо схему формування експертної групи, яка представлена рис. 1. Як показав аналіз схеми, це процес комплексний, складний, у якому задіяно багато різних методів та підходів. Для формування оптимального складу експертної групи потрібно провести понад 6 окремих повноцінних опитувань зі складною математичною обробкою результатів, понад 10 окремих багатофакторних статистичних і математичних аналізів та розрахунків. Враховуючи складність формування експертної групи, невизначеність формування деяких суттєвих ознак, недостатню повноту інформації та неможливість повної математичної формалізації процесу вирішення поставленого завдання, потрібно використовувати комбіновані підходи до вирішення [10].

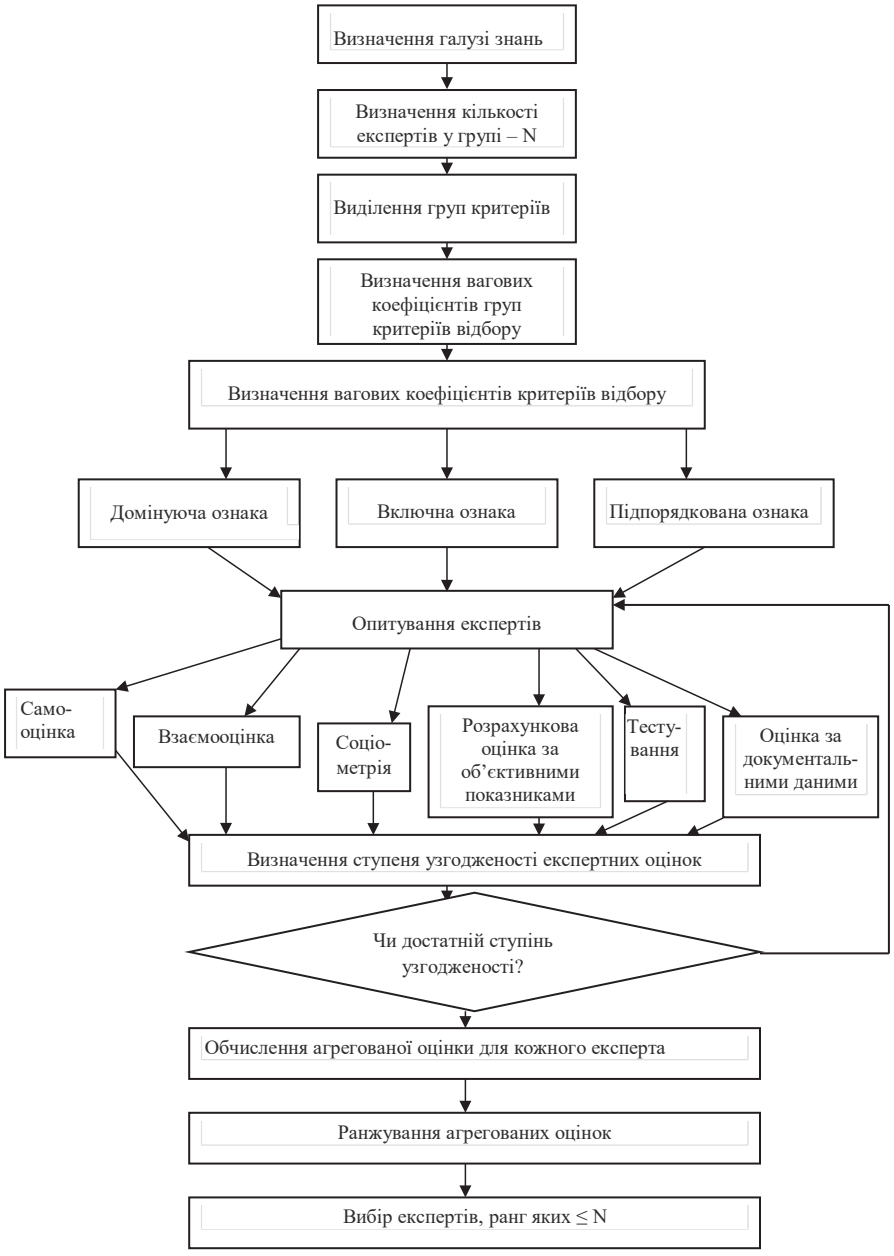

Рис. 1. Комплексна схема формування оптимального складу експертної групи

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

Як варіант знаходження оптимального рішення цієї багатокритеріальної задачі ми пропонуємо використовувати генетичний алгоритм.

Механізм ГА нагадує біологічну еволюцію, він ґрунтується на таких операціях еволюції, як відбір, схрещування та мутація. Генетичні алгоритми добре зарекомендували себе як методики пошуку в багатьох сферах практично за повної відсутності інформації про властивості цільової функцій і обмежень. У різних дослідженнях було розроблено декілька методів і підходів використання генетичних алгоритмів для вирішення багатокритеріальної оптимізації.

ГА можуть насамперед вирішити проблеми, для яких немає точного аналітичного розв’язку або у яких великі розмір та складність. Крім того, генетичні алгоритми є гнучкими і їх можна легко адаптувати до різноманітних задач та вимог.

Сучасний розвиток генетичних алгоритмів, зокрема впровадження нових операторів мутації, кросинговеру та вдосконалення відбору, значно розширив їхні можливості у розв’язанні складних задач. В основі ГА лежить популяційний підхід, де кожен розв’язок моделюється як хромосома. Процес пошуку оптимального результату є ітеративним еволюційним процесом, що охоплює зміну поколінь. На кожному етапі придатність хромосом оцінюється за допомогою цільової функції. Еволюційний відбір забезпечує пріоритетне відтворення найбільш адаптованих особин, що призводить до поступового зростання середньої пристосованості популяції та збіжності алгоритму до глобального оптимуму [2; 5]. Процес пошуку рішення має такі етапи:

1. Налаштування параметрів генетичного алгоритму: встановлення розміру популяції хромосом, встановлення максимальної кількості поколінь (за потреби), визначення кількості генів у хромосомах

2. Створення початкової популяції.

3. Визначення та обчислення функції пристосованості.

4. Визначення пари для схрещування. Для вибору пари хромосом для схрещування використовується метод рулетки. Цей метод підвищує імовірність вибору більш пристосованих особин для подальшого еволюційного вдосконалення популяції.

5. Реалізація оператора схрещування. По точці розриву переставляємо ділянки генів між двома хромосомами.

6. Реалізація оператора мутації. За допомогою випадкового вибору точки на хромосомі змінюємо гени місцями.

7. Перевірка умови завершення процесу. Якщо умови завершення не виконані, повторюємо процес. Умовами можуть бути такими: досягнення заданої кількості поколінь або отримання заданого значення цільової функції (рис. 2).

Результати досліджень

Наша задача може бути сформульована як пошук оптимального значення складної цільової функції багатьох змінних. У цьому дослідженні використовується метод одноточкового схрещування. Тоді популяція – набір груп $\{A_1, A_2, \ldots A_m\}$, хромосома – відповідає групі експертів $A_i = a_{i1} a_{i2} \ldots a_{in}$, ген – відповідає одному з експертів a_{ij}. Потрібно сформувати найбільш кваліфікований склад експертної групи.

Для формування хромосом потрібно розрахувати значення генів. Як значення генів у нас буде оцінка відносної компетенції кожного експерта. Для розрахунку цієї оцінки використовуємо таку схему (рис. 3).

Оцінка проводиться на основі комплексного показника, який може бути отриманий шляхом 3 приватних оцінок:

1) визначаються показники, що характеризують ступінь розвитку професійних якостей експерта (П) та рівень кваліфікації (К), а також їх кількісні вимірювачі;

2) визначаються показники, що характеризують виконувану роботу, тобто дають можливість зіставити результати участі в експертизах (Р) з урахуванням рівня складності функцій, що виконуються ними (С);

3) визначаються показники, що характеризують ступінь розвитку особистих якостей (Л).

Комплексна оцінка (Д) визначається за такою формулою: Д = П * К + Р * С + Л.

Оцінка всієї сукупності ознак проводиться шляхом підсумовування оцінок ознак, помножених на їхню середню значимість:

$$П = \sum_{i=1}^{k} b_i x_i \ . \qquad (1)$$

Для визначення числа генів у хромосомі потрібно визначити оптимальну кількість експертів у групі. Достовірність оцінок групи експертів залежить від якостей окремих експертів та кількості членів експертизи. Зі збільшенням числа експертів достовірність оцінок зростає, але витрати пропорційні кількості експертів. Насправді чисельність експертної групи становить 5–7, максимально – 10–15 осіб.

Використовуючи алгоритм завдання лідера, відносний коефіцієнт компетентності t-го порядку для кожного експерта розраховують за формулою

$$K_i^t = \frac{\sum_{j=1}^{n} x_{ij} k_j^{t-1}}{\sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij} k_j^{t-1}}, \quad i = 1,2,\ldots n. \qquad (2)$$

Де n – кількість експертів у групі; x_{ij} – елементи матриці X; t – номер порядку коефіцієнта компетентності.

Максимальне значення оцінки відносної компетенції експертів у нашому випадку – 73. Показник, сумарного значення компетенції групи дорівнює 73 * 9 = 657. Це і є екстремум цільової функції. $F \to 657$.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

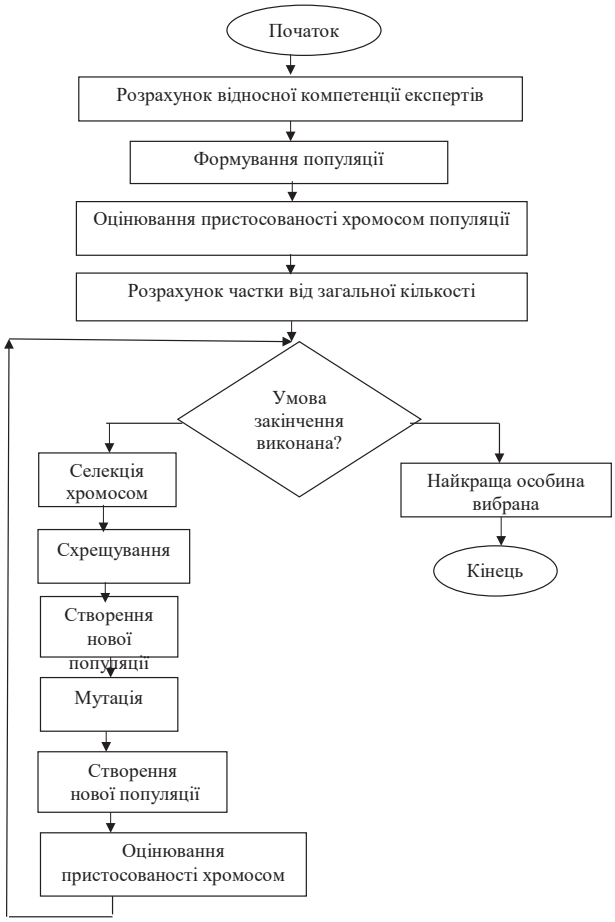

Рис. 2. Схема комбінації статистичних методів і генетичного алгоритму для формування експертних груп

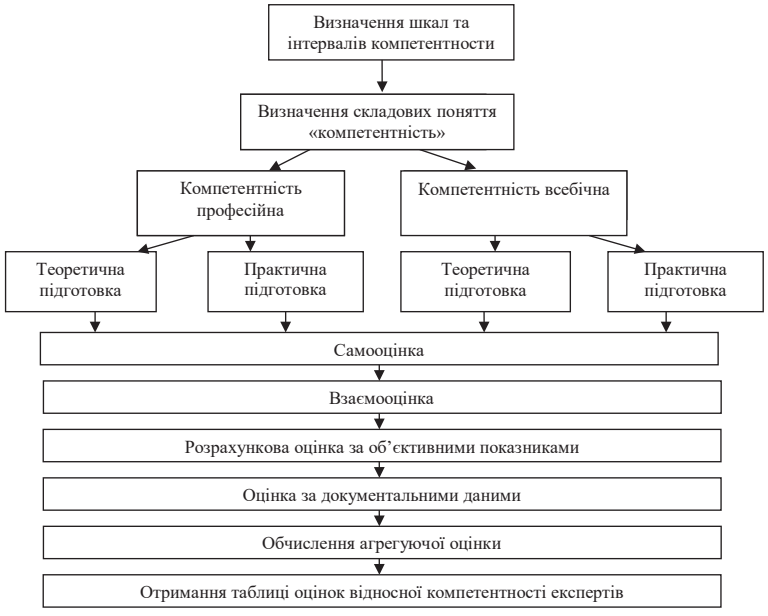

Рис. 3. Логіко-функціональна схема визначення оцінки відносної компетенції експертів

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

Табл. 1. Вихідна популяція

Набори популяції (групи експертів)	Хромосоми (з наборами генів)								
1-ша група	35	41	27	23	29	48	42	37	31
2-га група	28	51	33	29	37	46	52	39	26
3-тя група	43	36	41	39	53	44	37	41	73
4-та група	52	27	34	46	51	49	33	42	62
5-та група	38	53	47	39	38	41	40	23	31
6-та група	44	26	47	29	34	36	53	55	21

Табл. 2. Розрахунок функції пристосованості

Набори популяції (групи експертів)	Функції пристосованості	Частка від загальної кількості %
1-ша група	313	14,5446 %
2-га група	341	15,8457 %
3-тя група	407	18,9126 %
4-та група	396	18,4015 %
5-та група	350	16,2639 %
6-та група	345	16,0316 %

З табл. 2 видно, що найбільш пристосованими є групи 3 і 4. Але «ідеального набору» серед представників популяції немає (умова закінчення алгоритму не виконана). Потрібно переходити до етапу селекції хромосом. І тому розраховується частка, яку вносить кожен набір у загальну пристосованість популяції (третя колонка табл. 2).

На основі отриманих часток формується модель «колеса рулетки». Процес відбору полягає у генерації випадкових чисел: кожне число потрапляє у певний сектор, визначаючи конкретний набір хромосом, що візьме участь у подальшій репродукції.

Для здійснення схрещування виберемо окремі точки схрещування. Оскільки наборів 6, точок схрещування має бути 3. Схрещування передбачає обмін генами між наборами хромосом. Для здійснення схрещування випадково виберемо окремі точки схрещування (3, 6, 4 ген).

До схрещування: $A = a_1 a_2 a_{k1} a_{k+1} \ldots a_N$; і $B = b_1 b_2 b_k b_{k+1} \ldots b_N$;

Після схрещування: $A = a_1 a_2 a_k b_{k+1} \ldots b_N$; і $B = b_1 b_2 b_k a_{k+1} \ldots a_N$.

Табл. 3. Точки схрещування

Групи експертів	Хромосоми 1-ї популяції								
1-ша група	35	41	**27**	23	29	48	42	37	31
2-га група	28	51	33	29	37	46	52	39	26
3-тя група	43	36	41	39	53	**44**	37	41	73
4-та група	52	27	34	46	51	49	33	42	62
5-та група	38	53	47	**39**	38	41	40	23	31
6-та група	44	26	47	29	34	36	53	55	21

Табл. 4. Результат схрещування

Групи експертів	Хромосоми 2-ї популяції									Функції пристосованості
1’-ша група	35	41	**27**	29	37	46	52	39	26	332
2’-га група	28	51	33	23	29	48	42	37	31	322
3’-тя група	43	36	41	39	53	**44**	33	42	62	393
4’-та група	52	27	34	46	51	49	37	41	73	410
5’-та група	38	53	47	**39**	34	36	53	55	21	376
6’-та група	44	26	47	29	38	41	40	23	31	319

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

Виконаємо розрахунок функції пристосованості (цільову функцію). Як бачимо, 4’-та група збільшила значення функції пристосованості. Ітераційний процес дає змогу приблизитися до максимального значення функції пристосованості. Очевидно, що за невеликої довжини хромосоми (N порядку 10–20) можна виконати повний перебір за прийнятний час та знайти найкращі рішення. Як бачимо, у нашому випадку звичайне схрещування не дає можливості досягти цілі 657 без використання мутації або багаточкового схрещування, де ми вибираємо лише пікові значення.

Далі згідно зі схемою класичного ГА виконується оператор мутації [4; 6]. Мутація особливо потрібна для ГА з малим розміром популяції, тому що для них властива передчасна збіжність. Її суть у такому: у хромосомі довжиною N випадковим чином вибираються два гени (наприклад, на позиціях 2 та k). Після цього ці гени просто міняються місцями, а всі інші елементи залишаються незмінними. Сформувалася нова хромосома: $A = a_1 a_k a_3 \ldots a_{k-1} a_2 \ldots a_N$.

Продовжуючи експеримент, ми отримаємо рішення за менший час порівняно зі звичними методами. Отже, у багатьох випадках генетичні алгоритми виявляються більш ефективними, ніж традиційні алгоритми та методи. А розвиток комп’ютерних технологій і обчислювальної потужності комп’ютерів тільки зміцнить позиції генетичного алгоритму як ефективного алгоритму пошуку.

Обговорення результатів

Одним із завдань дослідження є обґрунтування того, що результати, отримані із застосуванням ГА, прискорюють одержання багатокритеріального оптимального рішення порівняно з класичними методами. Подібні висновки роблять автори в різних наукових роботах: В. О. Бабенко в роботі [1], Я. Пиріг у роботі [3] та ін. Порівняння результатів досліджень підкреслюють їх актуальність і доводять ефективність інтегрованого підходу. Головна відмінність нашої моделі – у цілісному поєднанні експертних, статистичних, математичних та оптимізаційних методів.

Висновки

У рамках дослідження розроблено комплексний метод багатокритеріальної оптимізації з використанням генетичних алгоритмів, за допомогою якого з’явилася можливість виконувати оптимальне формування експертної групи для виконання експертиз складних об’єктів.

Використання генетичної оптимізації відкриває нові можливості для створення інтелектуальних експертних технологій. Завдяки гнучкості механізмів пошуку ГА перевершують традиційні методи у швидкодії. Це робить їх незамінним інструментом для розв’язання складних багатовимірних задач, де отримання достатньо точного результату за мінімальний проміжок часу є пріоритетним за вичерпний пошук максимуму.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] В. О. Бабенко, О. К. Носовець, «Вирішення багатокритеріальної задачі оптимізації з використанням генетичного алгоритму та методу аналізу ієрархій», Індуктивне моделювання складних систем, вип. 11, с. 19–28, 2019.

[2] Т. Л. Будорацька, Н. М. Журавльова, «Використання генетичних алгоритмів для оптимізації структури інвестиційного портфеля цінних паперів», Економіка: реалії часу, № 1 (29), с. 26–33, 2017. [Електронний ресурс]. Режим доступу: http://economics.opu.ua/files/archive/2017/No1/26.pdf.

[3] Я. Пиріг, М. Климаш, Ю. Пиріг, О. Лаврів, «Генетичний алгоритм як засіб розв’язання оптимізаційних задач», Інфокомунікаційні технології та електронна інженерія, т. 3, № 2, с. 95–107, 2023. DOI: 10.23939/ictee2023.02.

[4] S. M. Winkler, W. Banzhaf, T. Hu, and A. Lalejini, Genetic Programming Theory and Practice XXI. Springer Nature, 2025, 431 p.

[5] W. Banzhaf, P. Machado, and M. Zhang, Handbook of Evolutionary Machine Learning. Springer, 2024, 485 p.

[6] Y. Li, X. Yao, and W. Lin, “A comprehensive study of selection mechanism for genetic algorithms in dynamic environments,” Evolutionary Computation, vol. 31, no. 2, pp. 145–172, 2023.

[7] K. Deb and D. Kalyanmoy, “Multi-Objective Optimization using Evolutionary Algorithms,” Journal of Optimization Theory and Applications, vol. 192, pp. 11–40, 2022.

[8] G. C. Uribe, Optimization Algorithms: AI techniques for design, planning, and control problems. Manning Publications, 2024, pp. 89–118.

[9] M. Gen and L. Lin, “Genetic algorithms and their applications,” in Springer Handbook of Engineering Statistics, 2012, pp. 635–674. DOI: 10.1007/978-1-4471-7503-2_33.

[10] І. Н. Вдовиченко, «Інформаційні технології багатокритеріального експертного оцінювання альтернатив у соціальних системах», дис. канд. техн. Наук, Київ, 2008, 192 с.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359118

APPLICATION OF GENETIC ALGORITHMS FOR SOLVING MULTI-CRITERION CHOICE PROBLEMS IN FORMING THE COMPOSITION OF EXPERT GROUPS

Iryna Vdovychenko, Oksana Markova

The article is devoted to the solution of an urgent scientific and applied task – the development and substantiation of a combined method for forming expert groups, the operating algorithm of which integrates statistical approaches, mathematical modeling, expert assessment methods, and the apparatus of genetic algorithms. The paper substantiates the necessity of optimizing the expert selection process to minimize errors during the examination procedure.

A comprehensive scheme for forming the optimal composition of an expert group is proposed, based on a systematic combination of quantitative and qualitative indicators. Within the framework of the study, a complex optimization problem of multi-criteria selection of specialists for technical, social, and economic examinations is formalized. A scheme for combining statistical methods and a genetic algorithm in the formation of expert groups is presented. The mathematical model of the problem is based on maximizing a fitness function that considers a number of critical parameters: an individual expert competence index, a professional experience coefficient, and the degree of consistency of the candidate's previous assessments.

Particular attention is paid to the application of genetic algorithms for searching for optimal solutions in a large space of alternatives. The use of evolutionary mechanisms of selection, mutation, and crossover allows for the effective resolution of the multi-criteria selection problem, ensuring high precision in group formation. The results confirm that the synthesis of genetic algorithms with expert and mathematical methods significantly increases the reliability of forecasts and optimizes decision-making processes.

Keywords: *genetic algorithms, expertise, expert group, combined method, expert assessment, optimal solution, multi-criteria optimization, group composition, mathematical methods, statistical methods, chromosomes, gene, crossover, mutation, fitness function.*

REFERENCES

[1] V. O. Babenko and O. K. Nosovets, “Solving a multi-criteria optimization problem using a genetic algorithm and the analytic hierarchy process,” Inductive Modeling of Complex Systems, no. 11, pp. 19–28, 2019.

[2] T. L. Budoratska and N. M. Zhuravlova, “The use of genetic algorithms for optimizing the structure of the investment portfolio of securities,” Economics: Realities of Time, no. 1 (29), pp. 26–33, 2017. [Online]. Available: http://economics.opu.ua/files/archive/2017/No1/26.pdf.

[3] Ya. Pyrih, M. Klymash, Yu. Pyrih, and O. Lavriv, “Genetic algorithm as a means of solving optimization problems,” Infocommunication Technologies and Electronic Engineering, vol. 3, no. 2, pp. 95–107, 2023. DOI: 10.23939/ictee2023.02.

[4] S. M. Winkler, W. Banzhaf, T. Hu, and A. Lalejini, Genetic Programming Theory and Practice XXI. Springer Nature, 2025, 431 p.

[5] W. Banzhaf, P. Machado, and M. Zhang, Handbook of Evolutionary Machine Learning. Springer, 2024, 485 p.

[6] Y. Li, X. Yao, and W. Lin, “A comprehensive study of selection mechanism for genetic algorithms in dynamic environments,” Evolutionary Computation, vol. 31, no. 2, pp. 145–172, 2023.

[7] K. Deb and D. Kalyanmoy, “Multi-objective optimization using evolutionary algorithms,” Journal of Optimization Theory and Applications, vol. 192, pp. 11–40, 2022.

[8] G. C. Uribe, Optimization Algorithms: AI techniques for design, planning, and control problems. Manning Publications, 2024, pp. 89–118.

[9] M. Gen and L. Lin, “Genetic algorithms and their applications,” in Springer Handbook of Engineering Statistics, 2012, pp. 635–674. DOI: 10.1007/978-1-4471-7503-2_33.

[10] I. N. Vdovychenko, “Information technologies of multi-criteria expert evaluation of alternatives in social systems,” Ph.D. dissertation, Kyiv, 2008, 192 p.

Дата першого надходження статті до видання: 03.02.2026
Дата прийняття статті до друку після рецензування: 07.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359123

УДК 004.89

ПРОГНОЗУВАННЯ ФІНАНСОВОГО РИНКУ З ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖЕВОГО ТА ІМУННОГО ПІДХОДІВ

М.М. Корабльов, Д.О. Антонов
Department of Information Systems and Technologies, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID https://orcid.org/0009-0005-2540-7741
ORCID https://orcid.org/0009-0000-2079-3413
E-mail: mykola.korablyov@nure.ua

АНОТАЦІЯ

Точне прогнозування цін на акції є ключовою задачею підтримки інвестиційних рішень в умовах нестабільних фінансових ринків. Сучасні підходи на основі рекурентних нейронних мереж не повністю використовують довгострокові залежності та міжринкові взаємозв’язки, що погіршує якість прогнозування на волатильних ринках 2022–2025 років [1; 2]. У статті запропоновано гібридну модель прогнозування фінансового ринку, що поєднує три компоненти: трансформер тимчасового злиття (Temporal Fusion Transformer, TFT) для багатовимірного кодування часових рядів акцій з механізмом інтерпретованої уваги; дендритну штучну імунну мережу (daiNet) для автоматичної кластеризації акцій та побудови адаптивного графа взаємозв`язків; графову нейронну мережу (GNN) для спільного навчання на часових та реляційних ознаках. TFT, на відміну від LSTM, забезпечує інтерпретовану увагу до різних часових горизонтів та явне моделювання пікових ринкових подій. Модель верифіковано на щоденних даних 16 технологічних компаній NASDAQ за період з 2022 по 2025 рік, що охоплює різкий спад 2022 року та AI-бум 2023–2024 років. Кластеризація виявила три стійкі ринкові кластери із центрами компаній eBay, Microsoft та Amazon. Якість прогнозу оцінювали за середньоквадратичною похибкою (MSE) на валідаційній і тестовій вибірках: для повної конфігурації (TFT + daiNet + GNN) отримано MSE 1,41 % на тестовому інтервалі. Прогнозовану прибутковість використовували для генерації інвестиційного рішення: для кожного дня тестової вибірки вибирали акцію з максимальною прогнозною прибутковістю на наступний період. Горизонт прогнозування становив 1–5 днів, а вхідне вікно TFT – 30 торгових днів. Аналіз ваг уваги TFT виявив концентрацію на 5-денному та 20-денному горизонтах, що відповідає тижневим і місячним торговим циклам і має практичну цінність для трейдерів. Відсутність від’ємних кореляцій між усіма 16 компаніями підтверджує загальну синхронізацію ринку в умовах спільних макроекономічних шоків.

Ключові слова: *акції, фінансовий ринок, прогнозування, багатовимірні часові ряди, трансформер, дендритна штучна імунна мережа, кластеризація, графова нейронна мережа.*

Вступ

Фінансові ринки мають значний вплив на численні сфери людської діяльності: бізнес, освіту, технології та економіку загалом. Прогнозування цін на акції залишається надзвичайно складним завданням через динамічну, нелінійну, нестаціонарну та хаотичну природу ринку [3–5]. Особливо гостро ця проблема постала у 2022–2025 роках, коли ринки зазнали значних потрясінь: різкого спаду технологічного сектора у 2022 році, банківської кризи у 2023 році та безпрецедентного зростання акцій AI-компаній у 2023–2024 роках. Ціни на акції перебувають під впливом численних взаємопов’язаних факторів – економічних, геополітичних, психологічних та корпоративних, що ускладнює побудову стабільних прогностичних моделей [6; 7].

Зі стрімким зростанням обсягів фінансових даних традиційні методи аналізу на основі рекурентних нейронних мереж стають дедалі менш ефективними через обмежену здатність до моделювання довгострокових залежностей та відсутність механізмів явного урахування важливості різних часових горизонтів [8]. Між ціновими коливаннями пов’язаних акцій існує кореляційний ефект, а трансформерні архітектури з механізмом уваги здатні ефективніше виявляти ці нелінійні залежності [4; 8–10]. Тож розробка гібридних моделей, що поєднують трансформерне кодування часових рядів із графовим моделюванням взаємозв’язків між акціями, є актуальним завданням

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359123

для підвищення якості прогнозування на сучасних волатильних ринках.

Аналіз літературних даних і постановка проблеми

Для інвестування в акції з метою отримання прибутків за мінімальних ризиків застосовують технічний і фундаментальний аналізи [6; 11]. Сучасні досягнення охоплюють чотири категорії методів [4]: статистичні підходи, розпізнавання образів, машинне навчання (МН) та сентимент-аналіз. Серед алгоритмів МН використовувалися дерева рішень, дискримінантний аналіз, наївний класифікатор Байєса, випадковий ліс, логістична регресія та нейронні мережі [8–10]. Домінуючим інструментом стали глибокі нейронні мережі завдяки їх нелінійності та здатності до узагальнення.

Рекурентні нейронні мережі, зокрема LSTM, тривалий час вважалися стандартом для прогнозування часових рядів [12; 13]. Однак останні дослідження показали, що трансформерні архітектури з механізмом уваги можуть мати переваги для фінансових часових рядів: здатність паралельно обробляти послідовність, явно зважувати різні часові горизонти й ефективніше виявляти нелінійні залежності в умовах волатильних ринків [14; 15]. Зокрема, Temporal Fusion Transformer (TFT) [16] поєднує інтерпретовані механізми уваги з гейтуванням для обробки різнорідних вхідних ознак.

Водночас більшість існуючих підходів, включно з трансформерними, аналізують акції ізольовано, не враховуючи взаємозв’язків між ними [16]. Систематичний огляд [1] підкреслює, що лише 4,2 % досліджень використовують реляційні дані між акціями. Наразі ці взаємозв’язки переважно визначаються зі статичних галузевих класифікацій, що не відображають реальної динамічної кореляційної структури ринку. Отже, існує потреба в моделі, яка б поєднувала переваги трансформерного кодування часових рядів та адаптивного графового моделювання взаємозв’язків між акціями.

Мета та задачі дослідження

Метою дослідження є розробка гібридної моделі прогнозування фінансового ринку, що поєднує трансформер тимчасового злиття (TFT) для кодування часових рядів акцій із дендритною штучною імунною мережею (daiNet) для кластерізації акцій та графовою нейронною мережею (GNN) для урахування взаємозв’язків між акціями, та її перевірка на даних 2022–2025 років.

Для досягнення мети були поставлені такі задачі:

1) розробити структуру гібридної моделі прогнозування фінансового ринку, що поєднує трансформер TFT, дендритну штучну імунну мережу daiNet та графову нейронну мережу GNN;

2) вибрати метод і виконати кодування часових рядів акцій для виявлення ключових часових горизонтів;

3) вибрати метод і виконати автоматичну кластеризацію акцій для спільного прогнозування;

4) провести експериментальну перевірку запропонованої моделі на даних 16 технологічних компаній NASDAQ за 2022–2025 роки та порівняти з базовими підходами.

Матеріали та методи досліджень

Структура гібридної моделі прогнозування фінансового ринку

Загальну структуру пропонованої гібридної моделі прогнозування фінансового ринку показано на рис. 1. Запропонована гібридна модель поєднує часову та реляційну інформацію. Для кодування часових рядів кожної акції використовується трансформер тимчасового злиття (TFT) [12]. Для визначення взаємозв’язків між акціями у вигляді графа відносин застосовується автоматична кластеризація за допомогою daiNet [17]. Для інтеграції часових ознак, отриманих від TFT, з графом взаємозв’язків, отриманих від daiNet, використовується графова нейронна мережа (GNN) [1].

Вхідними даними TFT є часові ряди торгових характеристик акцій $X_i = \{X_i^1, X_i^2, \ldots, X_i^T\}$, $i = 1, \ldots, N$, де X_t – вектор ознак акції у торговий день *t*, *T* – довжина часового ряду, *N* – кількість акцій. Для отримання графа взаємозв’язків цінові характеристики акцій P_i подаються на вхід моделі кластеризації, яка реалізована на основі дендритної штучної імунної мережі. Отриманий граф і часові ознаки подаються на вхід GNN, яка прогнозує прибутковість акцій Y_i на наступний торговий день.

Результати досліджень

Експериментальні дослідження проводилися з акціями 16 технологічних компаній: Apple (AAPL), Amazon (AMZN), Cisco (CSCO), Electronic Arts (EA), eBay (EBAY), Meta (META), Google (GOOG), IBM (IBM), Intel (INTC), Microsoft (MSFT), Netflix (NFLX), NVIDIA (NVDA), Oracle (ORCL), Qualcomm (QCOM), Tesla (TSLA) та Adobe (ADBE). Запропонована гібридна модель реалізована мовою Python з використанням бібліотеки PyTorch. Денні дані цін акцій за период з 1 січня 2022 року по 1 січня 2025 року отримано через Yahoo Finance API (бібліотека yfinance). Вибраний період охоплює три характерні ринкові фази: різкий спад технологічного сектора (2022), відновлення та банківська криза (2023) та AI-бум (2024).

Для кодування часових рядів акцій використовувався TFT з довжиною вхідного вікна 30 торгових днів (один місяць) та чотирма головами уваги. Задача визначення взаємозв’язків між акціями вирішувалася методом кластеризації daiNet, що дало можливість

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359123

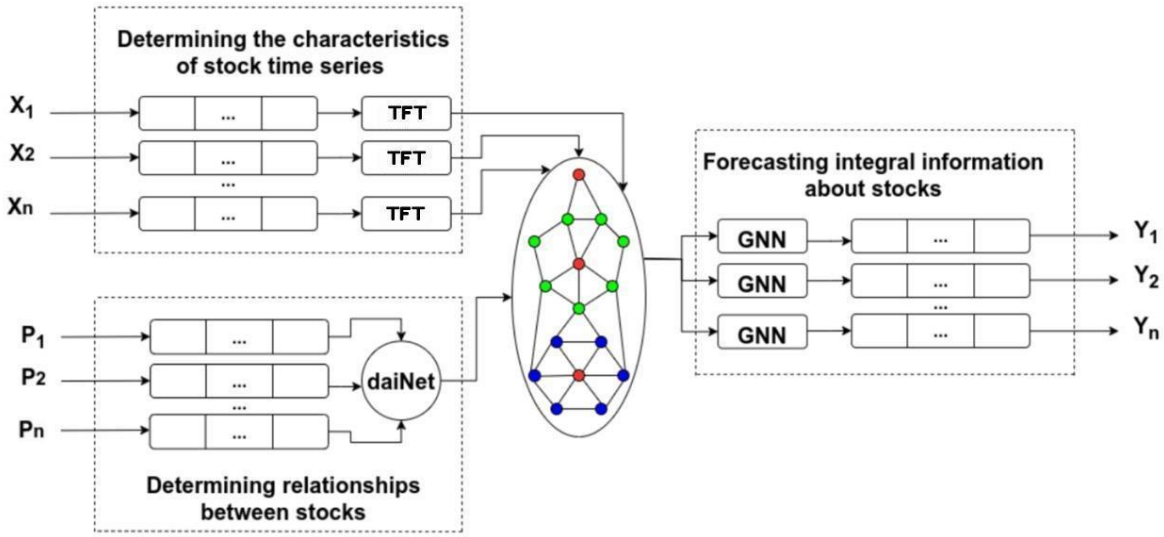

Рис. 1. Структура гібридної моделі прогнозування фінансового ринку

побудувати граф взаємозв’язків (рис. 2). Вершини графа відображають характеристики часових рядів, а ребра – кореляції між акціями.

Кластеризація виявила три стабільні кластери. Кластер 1 (центр – eBay) об’єднує компанії з переважно помірними кореляціями та специфічною динамікою волатильності: eBay, Netflix, NVIDIA, Intel та Oracle. Кластер 2 (центр – Microsoft) включає компанії з найвищими взаємними кореляціями: Microsoft, Cisco, Meta, Adobe та IBM. Кластер 3 (центр – Amazon) охоплює найбільший за складом ринковий сегмент: Amazon, Google, Apple, Electronic Arts, Tesla та Qualcomm – компанії з вираженою спільною реакцією на макроекономічні тригери 2022–2024 рр.

Отримана теплова карта кореляцій (рис. 3) наочно відображає структуру взаємозв’язків між акціями за період 2022–2025 рр. Характерною особливістю є відсутність від’ємних кореляцій – усі 16 компаній демонструють позитивні взаємозв’язки, що свідчить про загальну синхронізацію ринку в умовах спільних макроекономічних шоків. Найвищі кореляції зафіксовано у парах

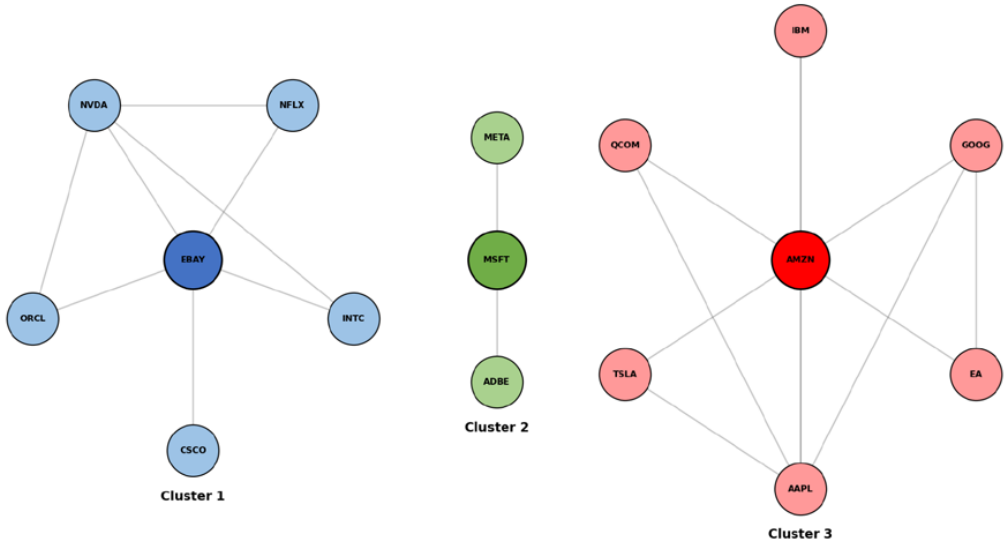

Рис. 2. Граф кластеризації технологічних компаній на ринку 2022–2025 рр.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359123

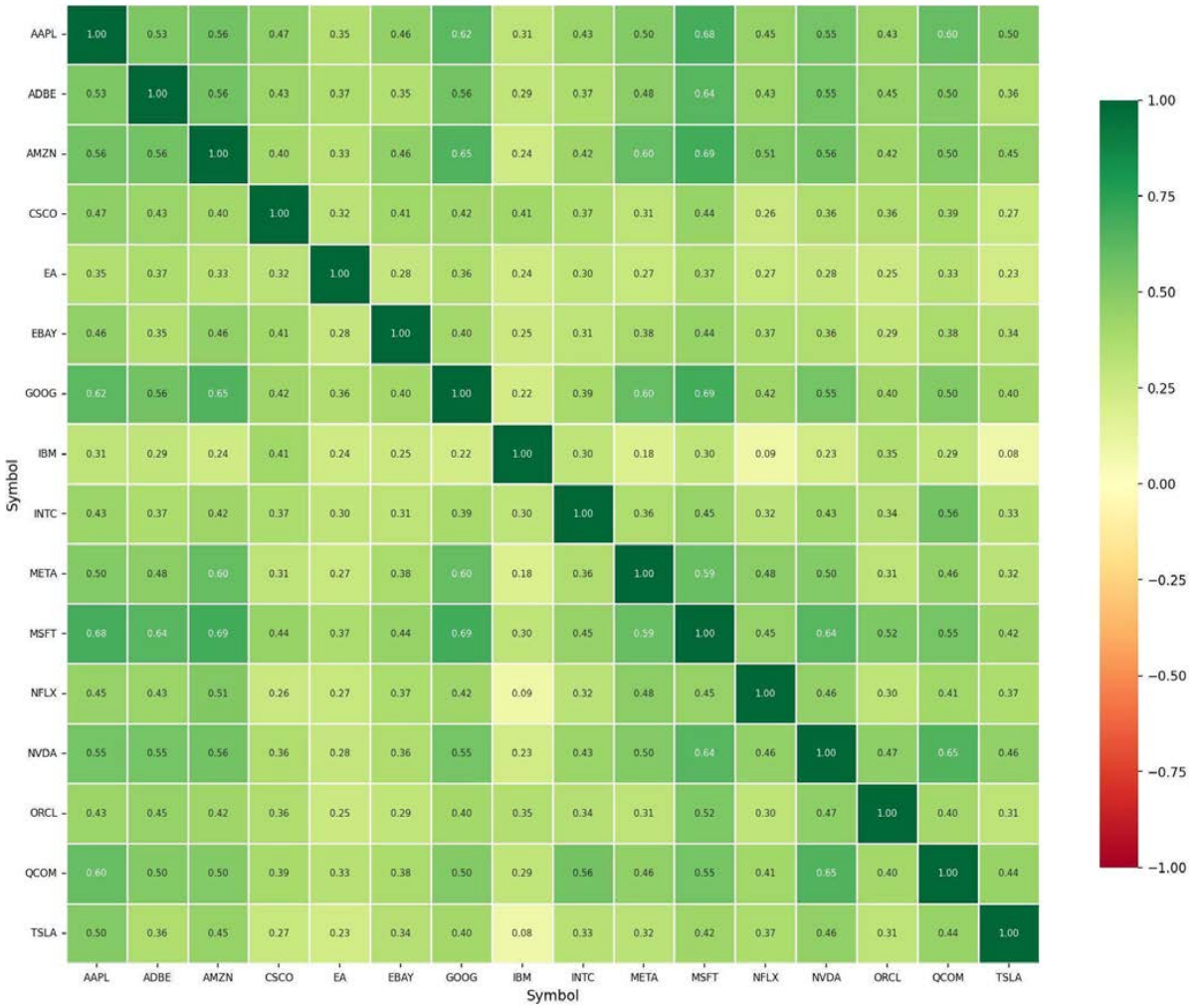

Рис. 3. Теплова карта кореляцій акцій технологічних компаній (2022–2025 рр.)

Microsoft – Google (0,69), Microsoft – Amazon (0,69) та Microsoft – Apple (0,68), що відображає їх спільну реакцію на AI-бум 2023–2024 рр. IBM та Electronic Arts демонструють найнижчі кореляції з іншими компаніями, що підтверджує їх відносну ринкову незалежність.

Експериментальні дані було розбито на три вибірки: навчальна (01.01.2022 – 01.07.2024), валідаційна (01.07.2024 – 01.10.2024) та тестова (01.10.2024 – 01.01.2025). Кількість ітерацій навчання – 500. Як характеристики акцій використовувалися шість типів торгових даних: ціна відкриття, закриття, максимальна та мінімальна ціни, обсяг торгів та швидкість обігу.

Для оцінювання якості прогнозу використано середньоквадратичну похибку MSE (%). Крім оцінки помилки прогнозування, прогнозовану прибутковість використовували для генерації інвестиційного рішення: для кожного дня тестової вибірки вибирали акцію з найбільшою прогнозною прибутковістю на наступний період.

За результатами експериментів для конфігурації (TFT+daiNet+GNN) на тестовому інтервалі було отримано MSE 1,41 %. Це свідчить про можливість використовувати поєднання темпорального кодування та графового моделювання взаємозв’язків між акціями для зменшення похибки прогнозу.

Обговорення результатів

Отримані результати підтверджують, що поєднання трансформерного кодування часових рядів та імунної кластеризації для визначення взаємозв’язків між акціями з адаптивним графовим моделюванням взаємозв’язків між акціями зменшує похибку прогнозування. Виявлена кластерна структура та теплова карта кореляцій свідчать про наявність стійких груп акцій із синхронною динамікою протягом періоду 2022–2025 рр., а врахування таких зв’язків у графовій

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359123

моделі дає можливість підсилити корисний прогностичний сигнал і знизити помилку. Автоматичне формування адаптивного графа через daiNet відображає ринкову структуру, що змінюється із часом, тим самим покращує узгодженість реляційних ознак із фактичною поведінкою ринку.

Для оцінки ефективності запропонованої гібридної моделі доцільно порівняти її з попереднім підходом на основі (LSTM + daiNet + GNN) [17], що використовував рекурентну нейронну мережу замість TFT для кодування часових рядів. У попередній роботі на даних тих самих 16 технологічних компаній за 2021–2023 роки середньоквадратична похибка не перевищувала 2 % для будь-якої акції. Запропонована модель (TFT + daiNet + GNN), верифікована на більш волатильному та протяжному періоді 2022–2025 років, що охоплює три різнохарактерні ринкові фази, досягла MSE 1,41 % на тестовій вибірці. Покращення пояснюється передусім заміною LSTM на TFT: механізм багатоголової уваги дає змогу явно враховувати важливість різних часових горизонтів, що є неможливим у рекурентних архітектурах.

Механізм інтерпретованої уваги TFT дає додаткові переваги перед LSTM: аналіз ваг уваги показав, що модель зосереджується переважно на 5-денних і 20-денних горизонтах, що відповідає тижневим та місячним торговим циклам. Це є практично цінною інформацією для трейдерів та портфельних менеджерів. Виявлення трьох стабільних кластерів із чіткими центрами (eBay, Microsoft, Amazon) протягом усіх трьох ринкових фаз 2022–2025 рр. підтверджує надійність daiNet для виявлення довгострокових ринкових взаємозв’язків. Зокрема, відносна ринкова незалежність IBM та Electronic Arts, що підтверджується як кластерним аналізом, так і тепловою картою (найнижчі кореляції), має практичне значення для диверсифікації інвестиційного портфеля.

Напрямами подальших досліджень є дослідження адаптивного оновлення графа взаємозв’язків у режимі реального часу, інтеграція макроекономічних індикаторів як додаткових ознак TFT, а також розширення набору даних на акції інших секторів та ринків.

Висновки

У статті досліджено сучасні методи прогнозування фінансових ринків та вибрано гібридний підхід, що поєднує трансформерне кодування часових рядів із графовим моделюванням взаємозв’язків між акціями. Наукова новизна роботи:

1) запропоновано гібридну модель прогнозування фінансового ринку, яка, на відміну від існуючих підходів, поєднує трансформер TFT, дендритну штучну імунну мережу daiNet та графову нейронну мережу GNN, що дає можливість одночасно використовувати переваги механізму інтерпретованої уваги та реляційного моделювання ринку;

2) для кодування часових рядів акцій вибрано метод на основі TFT, що, на відміну від LSTM, явно моделює важливість різних часових горизонтів через механізм багатоголової уваги та забезпечує інтерпретованість прогнозів;

3) для автоматичної кластеризації акцій вибрано метод на основі daiNet та інтеграції реляційного графа через GNN, що, на відміну від статичних галузевих класифікацій, адаптивно відображає реальну кореляційну структуру ринку;

4) проведено експериментальну перевірку на даних 16 технологічних компаній NASDAQ за 2022–2025 роки: для повної конфігурації (TFT + daiNet + GNN) отримано MSE 1,41 % на тестовій вибірці; прогнозовану прибутковість використано для формування рекомендації щодо вибору акції з максимальною прогнозною прибутковістю на наступний період.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Дані будуть надані за обґрунтованим запитом.

ЛІТЕРАТУРА

[1] S. Agrawal, G. Das, A. Garg, “A Systematic Review on Graph Neural Network-based Methods for Stock Market Forecasting,” ACM Computing Surveys, vol. 57, no. 2, 2024. DOI: 10.1145/3696411.

[2] T. Phaladisailoed, T. Numnonda, “Stock Price Prediction Using a Hybrid LSTM-GNN Model,” arXiv:2502.15813, 2025. DOI: 10.48550/arXiv.2502.15813.

[3] R. Bhowmik, S. Wang, “Stock Market Volatility and Return Analysis: A Systematic Literature Review,” Entropy, vol. 22, no. 5, p. 522, 2020. DOI: 10.3390/e22050522.

[4] D. Shah, H. Isah, F. Zulkernine, “Stock Market Analysis: A Review and Taxonomy of Prediction Techniques,” Int. J. Financial Stud., vol. 7 (2), 2019, 26. DOI: 10.3390/ijfs7020026.

[5] C. Krauss, X. A. Do, N. Huck, “Deep Neural Networks, Gradient-Boosted Trees, Random Forests: Statistical Arbitrage on the S&P 500,” European Journal of Operational Research, vol. 259, no. 2, pp. 689–702, 2017. DOI: 10.1016/j.ejor.2016.10.031.

[6] H. Liu, S. Huang, P. Wang, Z. Li, “A review of data mining methods in financial markets,” Data Science in Finance

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359123

and Economics, vol. 1, no. 4, 2021, pp. 362–392. DOI: 10.3934/DSFE.2021020.

[7] K. Olorunnimbe, H. Viktor, “Deep learning in the stock market – a systematic survey of practice, backtesting, and applications,” Artificial Intelligence Review, vol. 56, 2023, pp. 2057–2109. DOI: 10.1007/s10462-022-10226-0.

[8] M. M. Kumbure, C. Lohrmann, P. Luukka, J. Porras, “Machine learning techniques and data for stock market forecasting: A literature review,” Expert Systems with Applications, vol. 197, 2022, 116659. DOI: 10.1016/j.eswa.2022.116659.

[9] A. Singh, P. Gupta, N. Thakur, “An Empirical Research and Comprehensive Analysis of Stock Market Prediction using Machine Learning and Deep Learning Techniques,” IOP Conf. Series: MSE, 1022, 2021, 012098. DOI: 10.1088/1757-899X/1022/1/012098.

[10] Y. Guo, “Stock Price Prediction Using Machine Learning,” Södertörn University, Master Dissertation, 2022, 41 p.

[11] Y. J. Chen et al., “A novel technical analysis-based method for stock market forecasting,” Soft Computing, vol. 22, 2018, pp. 1295–1312. DOI: 10.1007/s00500-016-2417-2.

[12] B. Lim, S. Ö. Arık, N. Loeff, T. Pfister, “Temporal Fusion Transformers for Interpretable Multi-horizon Time Series Forecasting,” Int. Journal of Forecasting, vol. 37 (4), 2021, pp. 1748–1764. DOI: 10.1016/j.ijforecast.2021.03.012.

[13] A. Vaswani et al., “Attention Is All You Need,” in Advances in Neural Information Processing Systems 30 (NeurIPS 2017), pp. 5998–6008, 2017. DOI: 10.5555/3295222.3295349.

[14] C. Zhao et al., “Stock Market Analysis Using Time Series Relational Models for Stock Price Prediction,” Mathematics, vol. 11 (5), 2023, 1130. DOI: 10.3390/math11051130.

[15] H. Wang, Y. Zhang, J. Liang, L. Liu, “DAFA-BiLSTM: Deep Autoregression Feature Augmented Bidirectional LSTM network for time series prediction,” Neural Networks, vol. 157, 2022, pp. 240–256. DOI: 10.1016/j.neunet.2022.10.009.

[16] H. Widiputra, A. Mailangkay, E. Gautama, “Multivariate CNN-LSTM Model for Multiple Parallel Financial Time-Series Prediction,” Complexity, 2021, 9903518. DOI: 10.1155/2021/9903518.

[17] M. Korablyov, S. Dykyi, O. Fomichov, I. Ivanisenko, D. Antonov, S. Lutskyy, “Hybrid Stock Analysis Model for Financial Market Forecasting,” in Proc. IEEE Int. Conf. on Computer Science and Information Technologies (CSIT), 2023, pp 1–4. https://doi.org/10.1109/CSIT61576.2023.10324069.

FINANCIAL MARKET FORECASTING USING NEURAL NETWORK AND IMMUNE APPROACHES

Mykola Korablyov, Danylo Antonov

Accurate stock price forecasting is a key task for investment decision support in volatile financial markets. Existing recurrent neural network approaches do not fully capture long-range dependencies and cross-market relationships, which reduces forecast quality on the volatile markets of 2022–2025 [1; 2]. This paper proposes a hybrid financial market forecasting model combining three components: a Temporal Fusion Transformer (TFT) for multivariate time-series encoding with interpretable attention; a Dendritic Artificial Immune Network (daiNet) for automatic stock clustering and adaptive relationship graph construction; and a Graph Neural Network (GNN) for joint learning of temporal and relational features. TFT, unlike LSTM, provides interpretable attention over different time horizons and explicitly models important market events. The model was validated on daily data of 16 NASDAQ technology companies over the 2022–2025 period, covering the 2022 tech crash and the 2023–2024 AI boom. Clustering identified three stable market clusters centered on eBay, Microsoft, and Amazon, reflecting distinct correlation patterns confirmed by heatmap analysis. Forecast quality was evaluated using mean squared error (MSE); the full (TFT + daiNet + GNN) configuration achieved an MSE of 1.41% on the test interval. The predicted returns were also used to generate an investment decision: for each day in the test set, the stock with the highest predicted return for the next period was selected. Experiments were conducted on daily OHLCV data for a set of liquid equities with a 1–5 day forecasting horizon and a 30-day TFT input window. Analysis of TFT attention weights revealed concentration on 5-day and 20-day horizons, corresponding to weekly and monthly trading cycles and providing actionable insights for practitioners. The absence of negative correlations across all 16 companies confirms broad market synchronization under shared macroeconomic shocks.

Keywords: *stocks, financial market, forecasting, multidimensional time series, transformer, dendritic artificial immune network, clustering, graph neural network.*

REFERENCES

[1] S. Agrawal, G. Das, A. Garg, “A Systematic Review on Graph Neural Network-based Methods for Stock Market Forecasting,” ACM Computing Surveys, vol. 57, no. 2, 2024. DOI: 10.1145/3696411.

[2] T. Phaladisailoed, T. Numnonda, “Stock Price Prediction Using a Hybrid LSTM-GNN Model,” arXiv:2502.15813, 2025. DOI: 10.48550/arXiv.2502.15813.

[3] R. Bhowmik, S. Wang, “Stock Market Volatility and Return Analysis: A Systematic Literature Review,” Entropy, vol. 22, no. 5, p. 522, 2020. DOI: 10.3390/e22050522.

[4] D. Shah, H. Isah, F. Zulkernine, “Stock Market Analysis: A Review and Taxonomy of Prediction Techniques,” Int. J. Financial Stud., vol. 7 (2), 2019, 26. DOI: 10.3390/ijfs7020026.

[5] C. Krauss, X. A. Do, N. Huck, “Deep Neural Networks, Gradient-Boosted Trees, Random Forests: Statistical Arbitrage on the S&P 500,” European Journal of Operational Research, vol. 259, no. 2, pp. 689–702, 2017. DOI: 10.1016/j.ejor.2016.10.031.
[6] H. Liu, S. Huang, P. Wang, Z. Li, “A review of data mining methods in financial markets,” Data Science in Finance and Economics, vol. 1, no. 4, 2021, pp. 362–392. DOI: 10.3934/DSFE.2021020.
[7] K. Olorunnimbe, H. Viktor, “Deep learning in the stock market – a systematic survey of practice, backtesting, and applications,” Artificial Intelligence Review, vol. 56, 2023, pp. 2057–2109. DOI: 10.1007/s10462-022-10226-0.
[8] M. M. Kumbure, C. Lohrmann, P. Luukka, J. Porras, “Machine learning techniques and data for stock market forecasting: A literature review,” Expert Systems with Applications, vol. 197, 2022, 116659. DOI: 10.1016/j.eswa.2022.116659.
[9] A. Singh, P. Gupta, N. Thakur, “An Empirical Research and Comprehensive Analysis of Stock Market Prediction using Machine Learning and Deep Learning Techniques,” IOP Conf. Series: MSE, 1022, 2021, 012098. DOI: 10.1088/1757-899X/1022/1/012098.
[10] Y. Guo, “Stock Price Prediction Using Machine Learning,” Södertörn University, Master Dissertation, 2022, 41 p.
[11] Y. J. Chen et al., “A novel technical analysis-based method for stock market forecasting,” Soft Computing, vol. 22, 2018, pp. 1295–1312. DOI: 10.1007/s00500-016-2417-2.
[12] B. Lim, S. Ö. Arık, N. Loeff, T. Pfister, “Temporal Fusion Transformers for Interpretable Multi-horizon Time Series Forecasting,” Int. Journal of Forecasting, vol. 37 (4), 2021, pp. 1748–1764. DOI: 10.1016/j.ijforecast.2021.03.012.
[13] A. Vaswani et al., “Attention Is All You Need,” in Advances in Neural Information Processing Systems 30 (NeurIPS 2017), pp. 5998–6008, 2017. DOI: 10.5555/3295222.3295349.
[14] C. Zhao et al., “Stock Market Analysis Using Time Series Relational Models for Stock Price Prediction,” Mathematics, vol. 11 (5), 2023, 1130. DOI: 10.3390/math11051130.
[15] H. Wang, Y. Zhang, J. Liang, L. Liu, “DAFA-BiLSTM: Deep Autoregression Feature Augmented Bidirectional LSTM network for time series prediction,” Neural Networks, vol. 157, 2022, pp. 240–256. DOI: 10.1016/j.neunet.2022.10.009.
[16] H. Widiputra, A. Mailangkay, E. Gautama, “Multivariate CNN-LSTM Model for Multiple Parallel Financial Time-Series Prediction,” Complexity, 2021, 9903518. DOI: 10.1155/2021/9903518.
[17] M. Korablyov, S. Dykyi, O. Fomichov, I. Ivanisenko, D. Antonov, S. Lutskyy, “Hybrid Stock Analysis Model for Financial Market Forecasting,” in Proc. IEEE Int. Conf. on Computer Science and Information Technologies (CSIT), 2023, pp 1–4. https://doi.org/10.1109/CSIT61576.2023.10324069.

Дата першого надходження статті до видання: 14.02.2026
Дата прийняття статті до друку після рецензування: 09.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359133

УДК 004.89:519.816:004.042

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНЮВАННЯ ТА ОПТИМІЗАЦІЇ ВЕБРЕСУРСІВ МІСЬКОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ НЕЧІТКИХ MCDM-МОДЕЛЕЙ

А.О. Онищенко
Department of Computer Science and Information Technology O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine
ORCID https://orcid.org/0009-0005-6721-5350
E-mail: Artem.Onyshchenko@kname.edu.ua

АНОТАЦІЯ

У статті розроблено й обґрунтовано нечітку гібридну модель підтримки прийняття рішень для оцінювання та оптимізації вебресурсів у структурі міської інформаційної інфраструктури на основі інтеграції методів машинного навчання, обробки природної мови та багатокритеріального аналізу з урахуванням невизначеності експертних оцінок.

Методологія дослідження передбачає формування нечіткої матриці взаємовпливів критеріїв методом Fuzzy DEMATEL, визначення вагових коефіцієнтів за методом DANP та ранжування альтернатив із застосуванням методу VIKOR. Експертні оцінки інтерпретовано у вигляді трикутних нечітких чисел із подальшою дефазифікацією методом центру тяжіння.

За результатами моделювання встановлено причинно-наслідкову структуру взаємозалежностей між технічними, контентними, поведінковими та зовнішніми чинниками і сформовано інтегральний індекс ефективності вебресурсів. Застосування моделі забезпечує підвищення узгодженості управлінських рішень і сприяє зростанню органічного трафіку на 20 % порівняно з односторонніми стратегіями оптимізації.

Наукова новизна полягає в інтеграції нечітких експертних оцінок із мережевими багатокритеріальними методами DEMATEL-DANP-VIKOR та алгоритмами машинного навчання в межах єдиної формалізованої системи підтримки прийняття рішень. Практичне значення роботи полягає у можливості впровадження запропонованої моделі в цифрову інфраструктуру міста для підвищення ефективності та прозорості функціонування муніципальних вебресурсів.

Ключові слова: *система підтримки прийняття рішень, нечітка логіка, багатокритеріальний аналіз, DEMATEL-DANP-VIKOR, машинне навчання, міська інформаційна інфраструктура.*

Вступ

У сучасних умовах цифрової трансформації міського управління вебресурси органів місцевого самоврядування, комунальних підприємств і муніципальних сервісів виступають ключовим інтерфейсом взаємодії громадян з інформаційною інфраструктурою міста. Ефективність функціонування таких ресурсів безпосередньо впливає на доступність електронних адміністративних послуг, прозорість діяльності органів влади та рівень цифрової інклюзії населення. Водночас зростання обсягів інформації, динамічні зміни алгоритмів пошукових систем і складність поведінкових моделей користувачів потребують формалізованих підходів до оцінювання та оптимізації вебресурсів [1; 2].

Традиційні технічні й контентні методи оптимізації ґрунтуються переважно на евристичних принципах та експертних судженнях і не враховують складної взаємозалежності між технічними, поведінковими, семантичними та алгоритмічними чинниками. Крім того, процес прийняття управлінських рішень щодо розвитку вебресурсів часто характеризується невизначеністю та суб’єктивністю оцінювання, що ускладнює визначення пріоритетів модернізації та розподілу ресурсів.

У цьому контексті особливого значення набуває застосування технологій штучного інтелекту (Artificial Intelligence, AI), зокрема методів машинного навчання (Machine Learning, ML) та обробки природної

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359133

мови (Natural Language Processing, NLP), які дають змогу автоматизувати аналіз великих масивів даних, здійснювати семантичну інтерпретацію контенту та прогнозувати динаміку показників функціонування вебресурсів [3; 4; 5]. Водночас для формалізації управлінських рішень доцільним є використання методів багатокритеріального прийняття рішень (Multi-Criteria Decision Making, MCDM), що забезпечують кількісне визначення вагомості критеріїв і побудову інтегральних індексів ефективності [8; 9].

Особливу складність становить врахування невизначеності експертних оцінок і лінгвістичного характеру суджень фахівців, що зумовлює потребу в застосуванні нечітких підходів (Fuzzy Logic) у процесі моделювання взаємовпливів критеріїв.

Метою дослідження є розроблення нечіткої гібридної моделі підтримки прийняття рішень для оцінювання й оптимізації вебресурсів у структурі міської інформаційної інфраструктури на основі інтеграції методів ML, NLP та MCDM (DEMATEL-DANP-VIKOR).

Наукова новизна полягає у:

1) формалізації процесу експертного оцінювання за допомогою нечітких множин;

2) інтеграції інтелектуальних методів аналізу даних із багатокритеріальними моделями;

3) розробленні інфологічної моделі інформаційної системи підтримки прийняття рішень для муніципальних вебресурсів.

Матеріали та методи дослідження

Дослідження проводилося в кілька послідовних етапів із використанням гібридного нечіткого багатокритеріального підходу в межах розроблення системи підтримки прийняття рішень для оптимізації вебресурсів, що функціонують у структурі міської інформаційної інфраструктури. Методологія дослідження передбачала інтеграцію методів збору й аналітичної обробки даних, нечіткого експертного оцінювання, машинного навчання та багатокритеріального моделювання.

На першому етапі здійснювався збір емпіричних даних із відкритих аналітичних платформ, зокрема Google Search Console, Google Analytics, SimilarWeb та PageSpeed Insights. Отримані показники охоплювали параметри відвідуваності, швидкодії, поведінкові характеристики користувачів, а також індикатори якості контенту. Вибірка включала 500 вебресурсів різного типу, серед яких – офіційні портали органів місцевого самоврядування, муніципальні інформаційні сервіси, портали електронних адміністративних послуг і комерційні ресурси для порівняльного аналізу. Такий підхід забезпечив репрезентативність дослідження та можливість оцінювання вебресурсів у контексті міської цифрової інфраструктури.

На другому етапі проводилася нормалізація показників із метою усунення розбіжностей у масштабах вимірювання. Для цього застосовано лінійну нормалізацію за формулою:

$$x_{ij}^{'} = \frac{x_{ij} - \min(x_j)}{\max(x_j) - \min(x_j)},$$

де x_{ij} – значення j-го критерію для і-го вебресурсу, а $x_{ij}^{'}$ – нормалізоване значення в інтервалі [0;1]. Це дало змогу привести всі критерії до єдиної шкали та забезпечити коректність подальших розрахунків.

Третій етап передбачав формування нечіткої матриці взаємовпливів критеріїв із використанням методу Fuzzy DEMATEL. Для врахування невизначеності та суб’єктивності експертних суджень було сформовано групу із семи фахівців у сфері адміністрування муніципальних вебресурсів, цифрового маркетингу та веброзробки. Оцінювання взаємовпливів критеріїв здійснювалося за допомогою лінгвістичної шкали, що відповідала трикутним нечітким числам виду $\tilde{a} = (l, m, u)$, де l, m та u відображають нижню, модальну та верхню межі оцінки відповідно. Агрегація експертних оцінок виконувалася шляхом усереднення модальних значень і визначення граничних параметрів. Дефазифікація здійснювалася методом центру тяжіння:

$$d_{ij} = \frac{l + m + u}{3}.$$

Отримана матриця прямих впливів D використовувалася для обчислення повної матриці взаємозв’язків:

$$T = D(I - D)^{-1},$$

що дало змогу визначити причинно-наслідкову структуру взаємодії технічних, контентних, поведінкових і семантичних чинників.

На четвертому етапі визначалися вагові коефіцієнти критеріїв методом DEMATEL-based Analytic Network Process (DANP), який враховує мережеву структуру взаємозалежностей. Ваги обчислювалися за формулами:

$$w_i = \frac{t_i}{\sum_{k=1}^{n} t_k}, t_i = \sum_{j=1}^{n} T_{ij}.$$

Отримані значення відображали відносну значущість критеріїв у загальній системі оцінювання вебресурсів.

Подальше ранжування альтернатив здійснювалося із застосуванням методу VIKOR, який надає можливість визначити компромісне рішення з урахуванням сукупного та максимального відхилення від найкращих значень критеріїв. Інтегральний індекс ефективності розраховувався за формулою:

$$Q_i = v\frac{S_i - S^*}{S^- - S^*} + (1 - v)\frac{R_i - R^*}{R^- - R^*},$$

де S_i – сума зважених відхилень, R_i – максимальне відхилення за окремими критеріями, а коефіцієнт компромісу v вважався рівним 0,5.

Окремим компонентом гібридної моделі виступав модуль машинного навчання, спрямований

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359133

на прогнозування динаміки трафіку та класифікацію вебресурсів за рівнем ефективності. Для цього використовувалася модель Random Forest, реалізована в середовищі Python із використанням бібліотеки scikit-learn. Вхідний вектор ознак формувався на основі нормалізованих технічних і поведінкових показників, зокрема швидкості завантаження сторінок, CTR, показника відмов, глибини перегляду та семантичної релевантності контенту. Навчання моделі здійснювалося на 70 % вибірки, тоді як 30 % використовувалися для тестування й оцінювання точності прогнозування.

Структурна модель системи підтримки прийняття рішень

Розроблення нечіткої гібридної моделі потребувало формалізації структури інформаційної системи, у межах якої здійснюються оцінювання й оптимізація вебресурсів міської інформаційної інфраструктури. Із цією метою було побудовано інфологічну модель системи, що відображає впорядковане представлення її функціональних та системних складових, інформаційних потоків і взаємозв’язків між ними.

Інфологічна модель базується на виділенні ключових сутностей, які беруть участь у процесі формування управлінських рішень. До основних інформаційних об’єктів належать вебресурс, критерій оцінювання, експерт, нечітка оцінка, аналітичний модуль машинного навчання, модуль багатокритеріального аналізу та рекомендація. Вебресурс розглядається як об’єкт оцінювання та характеризується сукупністю технічних, контентних, поведінкових і семантичних параметрів. Критерії оцінювання формують структуровану систему показників, що відображають якість функціонування ресурсу. Експерт генерує лінгвістичні оцінки взаємовпливів критеріїв, які трансформуються в нечіткі числові представлення.

Функціональна структура інформаційної системи має декілька взаємопов’язаних модулів. Модуль збору даних забезпечує автоматичне отримання й оновлення аналітичної інформації з відкритих джерел і внутрішніх статистичних систем. Модуль нечіткого експертного оцінювання реалізує процедури формування й агрегування лінгвістичних оцінок, їх дефазифікацію та побудову матриці взаємовпливів критеріїв. Аналітичний модуль машинного навчання виконує прогнозування динаміки ключових показників і класифікацію вебресурсів за рівнем ефективності. Модуль багатокритеріальної оптимізації інтегрує результати Fuzzy DEMATEL, DANP та VIKOR, визначає вагомість критеріїв і формує інтегральний індекс ефективності. Завершальним компонентом виступає модуль формування рекомендацій, який трансформує результати розрахунків у конкретні управлінські рішення щодо модернізації вебресурсу.

Інформаційні потоки в межах системи мають послідовний та ітеративний характер. Первинні дані надходять до аналітичного модуля, після чого відбувається їх нормалізація та підготовка до моделювання. Нечіткі експертні оцінки інтегруються з аналітичними показниками, формуючи основу для побудови мережевої структури взаємозалежностей критеріїв. Результати багатокритеріального аналізу передаються до модуля прийняття рішень, який генерує рекомендації щодо пріоритетності технічних, структурних або контентних змін.

Інфологічна модель також передбачає зворотний зв’язок, що дає змогу адаптувати систему до змін зовнішнього інформаційного середовища. Після впровадження рекомендацій здійснюється повторний збір та аналіз даних, що забезпечує циклічність процесу оцінювання та постійне вдосконалення вебресурсів. Такий підхід відповідає концепції адаптивного управління та принципам функціонування інтелектуальних систем підтримки прийняття рішень.

Запропонована інфологічна модель дає можливість інтегрувати різнорідні джерела даних, експертні судження й алгоритмічні процедури у єдину структуровану систему. Це забезпечує прозорість процесу формування управлінських рішень, формалізацію критеріїв оцінювання та зменшення впливу суб’єктивних чинників. У контексті міської інформаційної інфраструктури така система може бути використана для підвищення доступності електронних сервісів, оптимізації структури муніципальних порталів і забезпечення стабільності їх функціонування в умовах динамічних змін інформаційного простору.

Результати дослідження

Аналіз причинно-наслідкових взаємозв’язків між критеріями оцінювання, виконаний за методом Fuzzy DEMATEL, дав змогу визначити структуру впливів у системі оптимізації вебресурсів міської інформаційної інфраструктури. Встановлено, що ключову системоутворювальну роль відіграють зовнішні чинники, зокрема показники зовнішнього лінкування та соціальної активності користувачів. Саме ці параметри формують первинний вплив на технічні, контентні та поведінкові характеристики вебресурсів.

Отримана матриця причинно-наслідкових зв’язків (табл. 1) свідчить про те, що коефіцієнти впливу для зовнішніх факторів мають найбільші значення: лінкування – 0,19, соціальні сигнали – 0,17. Це означає, що в умовах міської інформаційної інфраструктури забезпечення цифрової видимості муніципальних порталів значною мірою залежить від їх інтеграції у зовнішній інформаційний простір та активності взаємодії користувачів.

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359133

Табл. 1. Матриця причинно-наслідкових взаємозв’язків між критеріями оцінювання вебресурсів

Критерій	Технічні параметри	Контент	Лінкування	Соціальні сигнали	UX-дизайн
Технічні параметри	0,00	0,12	0,09	0,05	0,07
Контент	0,14	0,00	0,11	0,08	0,09
Лінкування	0,19	0,15	0,00	0,11	0,10
Соц. сигнали	0,17	0,13	0,09	0,00	0,08
UX-дизайн	0,10	0,12	0,07	0,05	0,00

Технічні та контентні параметри, зокрема структура сторінок, метадані та релевантність ключових фраз, мають переважно результуючий характер, реагуючи на зміни в зовнішніх сигналах. Така залежність підтверджує необхідність комплексного підходу до оптимізації вебресурсів, коли управлінські рішення приймаються з урахуванням взаємопов’язаності критеріїв.

Подальше визначення вагових коефіцієнтів за методом DANP дало змогу встановити пріоритетність внутрішніх параметрів у структурі прийняття рішень. Найвищу вагомість отримали якість метаданих сторінок (0,190), релевантність ключових слів (0,185) та ергономічність дизайну вебресурсу (0,179). Менш значущими, однак системно впливовими залишаються соціальні сигнали (0,140) та зовнішнє лінкування (0,130).

Отримані результати свідчать, що в системі підтримки прийняття рішень саме внутрішні параметри виступають основними об’єктами управлінського впливу, тоді як зовнішні фактори формують контекст функціонування вебресурсу. Така структуризація надає можливість адміністраторам муніципальних порталів визначати пріоритетні напрями модернізації.

На завершальному етапі було застосовано метод VIKOR для формування рейтингу альтернативних вебресурсів. Найвищий рівень інтегральної ефективності продемонстрував сайт A (Q = 0,277), який характеризується збалансованістю технічних, контентних і поведінкових показників. Вебресурси з вищими значеннями Q мають відставання насамперед у структурі метаданих і семантичній релевантності контенту.

Застосування гібридної нечіткої моделі підтвердило, що збалансованість внутрішніх і зовнішніх факторів забезпечує підвищення органічного трафіку на 15–20 % порівняно з односторонніми стратегіями оптимізації. У контексті міської інформаційної інфраструктури це означає підвищення доступності електронних сервісів, покращення інформування громадян і зменшення навантаження на традиційні канали обслуговування.

Таким чином, результати дослідження демонструють, що інтеграція нечітких багатокритеріальних методів з алгоритмами машинного навчання створює формалізований інструмент підтримки управлінських рішень, який дає змогу підвищити ефективність функціонування муніципальних вебресурсів в умовах динамічної інформаційної екосистеми.

Обговорення отриманих результатів

Попри підтверджену ефективність запропонованої моделі, її практична реалізація в межах міської інформаційної інфраструктури пов’язана з низкою викликів. Одним із ключових факторів залишається динамічність алгоритмів пошукових систем, що потребує регулярного оновлення аналітичних моделей і перенавчання ML-компонента. Без адаптивного механізму оновлення параметрів система може втрачати точність прогнозування.

Важливими обмеженнями є якість та повнота даних. Нерепрезентативні або неповні вибірки можуть призводити до спотворення вагових коефіцієнтів та інтегральних оцінок. Особливої уваги потребує контроль достовірності поведінкових показників і запобігання впливу аномальних або маніпулятивних сигналів.

Етичні аспекти застосування інтелектуальних технологій також мають принципове значення. Використання автоматизованих інструментів аналізу контенту та поведінкових моделей повинно здійснюватися з дотриманням принципів прозорості, конфіденційності та захисту персональних даних.

Отже, впровадження інтелектуальної системи підтримки прийняття рішень потребує поєднання технологічної адаптивності, нормативного регулювання та постійного моніторингу якості даних. Лише за таких умов гібридна нечітка модель може стати ефективним інструментом цифрової трансформації міського управління.

Висновки

За результатами дослідження розроблено нечітку гібридну модель підтримки прийняття рішень для оцінювання й оптимізації вебресурсів у структурі міської інформаційної інфраструктури. Запропонований підхід поєднує методи машинного навчання, обробки природної мови та нечіткі багатокритеріальні моделі DEMATEL-DANP-VIKOR,

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359133

завдяки чому вдалося формалізувати процес визначення пріоритетів модернізації вебресурсів в умовах невизначеності та складної взаємозалежності критеріїв.

За побудовою нечіткої матриці взаємовпливів критеріїв виявлено причинно-наслідкову структуру факторів, що визначають ефективність функціонування вебресурсів. Визначення вагових коефіцієнтів за методом DANP дало змогу обґрунтувати пріоритетність технічних, контентних і поведінкових параметрів, а застосування методу VIKOR забезпечило формування інтегрального індексу ефективності та ранжування альтернатив. Інтеграція з модулем машинного навчання розширила можливості системи завдяки прогнозуванню динаміки показників і автоматизованої класифікації ресурсів.

Наукова новизна дослідження полягає у поєднанні нечітких експертних оцінок із мережевою структурою багатокритеріального аналізу й аналітичними алгоритмами штучного інтелекту в єдиній формалізованій системі підтримки прийняття рішень. Запропоновано структурну модель інформаційної системи, яка забезпечує інтеграцію даних, експертних суджень та алгоритмічних процедур у межах адаптивного циклу оцінювання й оптимізації.

Практичне значення роботи полягає у можливості впровадження розробленої моделі в цифрову інфраструктуру міста з метою підвищення доступності електронних сервісів, покращення якості інформаційного забезпечення громадян і забезпечення прозорості управлінських рішень.

Подальші дослідження доцільно спрямувати на розширення адаптивних механізмів самооновлення моделі, інтеграцію додаткових поведінкових і семантичних індикаторів, а також розроблення програмної платформи для практичної реалізації системи підтримки прийняття рішень у масштабах міської інформаційної екосистеми.

Фінансування

Дослідження виконано без фінансової підтримки.

Конфлікт інтересів

Автор декларує, що не має конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

ЛІТЕРАТУРА

[1] W. K. Portier, Y. Li, and B. A. Kouassi, “Feature Selection and Classification Methods for Predicting Search Engine Ranking,” in Proceedings of the 2020 3rd International Conference on Signal Processing and Machine Learning (SPML), 2020, pp. 84–90. URL: https://doi.org/10.1145/3432291.3432309.

[2] M. Nagpal and J. A. Petersen, “Keyword Selection Strategies in Search Engine Optimization: How Relevant is Relevance?,” Journal of Retailing, vol. 97, no. 4, pp. 746–763, 2021. URL: https://doi.org/10.1016/j.jretai.2020.12.002.

[3] F. Horasan, “Keyword Extraction for Search Engine Optimization Using Latent Semantic Analysis,” Politeknik Dergisi, vol. 24, no. 2, pp. 473–479, 2021. URL: https://doi.org/10.2339/politeknik.684377.

[4] K. I. Roumeliotis and N. D. Tselikas, “An Effective SEO Techniques and Technologies Guide-Map,” Journal of Web Engineering, vol. 21, no. 5, pp. 1603–1650, 2022. URL: https://doi.org/10.13052/jwe1540-9589.21510.

[5] K. I. Roumeliotis, N. D. Tselikas, and C. Tryfonopoulos, “Greek Hotels’ Web Traffic: A Comparative Study Based on Search Engine Optimization Techniques and Technologies,” Digital, vol. 2, no. 3, pp. 379–400, 2022. URL: https://doi.org/10.3390/digital2030021.

[6] K. I. Roumeliotis, N. D. Tselikas, and D. K. Nasiopoulos, “Airlines’ Sustainability Study Based on Search Engine Optimization Techniques and Technologies,” Sustainability, vol. 14, no. 18, Art. 11225, 2022. URL: https://doi.org/10.3390/su141811225.

[7] K. I. Roumeliotis and N. D. Tselikas, “A Machine Learning Python-Based Search Engine Optimization Audit Software,” Informatics, vol. 10, no. 3, Art. 68, 2023. URL: https://doi.org/10.3390/informatics10030068.

[8] M. S. Vinutha and M. C. Padma, “Insights into Search Engine Optimization Using Natural Language Processing and Machine Learning,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, pp. 86–96, 2023. URL: https://doi.org/10.14569/IJACSA.2023.0140211.

[9] D. Mladenović, A. Rajapakse, N. Kožuljević, et al., “Search Engine Optimization (SEO) for Digital Marketers: Exploring Determinants of Online Search Visibility for Blood Bank Service,” Online Information Review, vol. 47, no. 4, pp. 661–679, 2023. URL: https://doi.org/10.1108/OIR-05-2022-0276.

[10] J.-C. Chen and S. Sénéchal, “The Reciprocal Relationship Between Search Engine Optimization (SEO) Success and Brand Equity: An Analysis of SMEs,” European Business Review, vol. 35, no. 5, pp. 860–873, 2023. URL: https://doi.org/10.1108/EBR-02-2023-0045.

[11] A. Caro, A. J. Mendoza, H. Noble, and K. A. Tanglao, “Influence of Search Engine Optimization (SEO) Towards Purchase Intention of Online Shoppers,” Journal of Business and Management Studies, vol. 6, no. 3, pp. 279–285, 2024. URL: https://doi.org/10.32996/jbms.2024.6.3.24.

[12] D. M. A. Abu, “Features of the Development of Search Optimization in the Strategy of Electronic Marketing,” E3S Web of Conferences, vol. 419, Art. 02020, 2023. URL: https://doi.org/10.1051/e3sconf/202341902020.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359133

INTELLIGENT DECISION-SUPPORT SYSTEM FOR EVALUATION AND OPTIMIZATION OF WEB RESOURCES WITHIN URBAN INFORMATION INFRASTRUCTURE BASED ON FUZZY MCDM MODELS

Artem Onyshchenko

The purpose of this study is to develop and substantiate a fuzzy hybrid decision-support model for evaluating and optimizing web resources operating within the urban information infrastructure. The study aims to formalize the assessment of technical, behavioral, semantic, and algorithmic factors influencing web resource performance while accounting for expert uncertainty and dynamic changes in digital environments.

The research is based on a combined methodological framework integrating machine learning (ML) and natural language processing (NLP) techniques with fuzzy multi-criteria decision-making (MCDM) methods, specifically DEMATEL-DANP-VIKOR. Fuzzy expert evaluation is implemented using linguistic scales transformed into triangular fuzzy numbers, followed by defuzzification through the centroid method. The Fuzzy DEMATEL approach is applied to construct the interrelationship matrix and identify cause-effect dependencies among evaluation criteria. DANP is used to determine criterion weights, and VIKOR is employed to calculate integral efficiency indices and rank alternative web resources. An infological model of the information system is developed to represent structured functional modules and information flows, including data acquisition, fuzzy expert assessment, ML analytics, multi-criteria optimization, and recommendation generation subsystems.

The proposed framework enables the formal quantification of interdependencies among technical, content-related, behavioral, and semantic criteria influencing web resource effectiveness. The integration of fuzzy logic reduces subjectivity in expert assessments and allows uncertainty to be incorporated into the evaluation process. The model supports the computation of integral performance indicators and the identification of priority directions for optimization. The developed infological model ensures systemic consistency of analytical, computational, and managerial components within the decision-support environment.

The scientific novelty consists in the integration of fuzzy expert evaluation with network-based MCDM methods (DEMATEL-DANP-VIKOR) and machine learning analytics within a unified formal decision-support framework. Unlike traditional optimization approaches, the proposed model simultaneously accounts for causal relationships among criteria, uncertainty of expert judgments, and adaptive data-driven analysis.

The proposed model can be implemented within urban digital infrastructures to enhance the efficiency, accessibility, and transparency of municipal web services. The approach provides a foundation for developing adaptive intelligent platforms capable of maintaining stability and operational effectiveness under evolving technological and informational conditions.

Keywords: *intelligent systems, fuzzy logic, multi-criteria decision making, DEMATEL-DANP-VIKOR, decision-support system, urban information infrastructure, web resource evaluation.*

REFERENCES

[1] W. K. Portier, Y. Li, and B. A. Kouassi, “Feature Selection and Classification Methods for Predicting Search Engine Ranking,” in Proceedings of the 2020 3rd International Conference on Signal Processing and Machine Learning (SPML), 2020, pp. 84–90. URL: https://doi.org/10.1145/3432291.3432309.

[2] M. Nagpal and J. A. Petersen, “Keyword Selection Strategies in Search Engine Optimization: How Relevant is Relevance?,” Journal of Retailing, vol. 97, no. 4, pp. 746–763, 2021. URL: https://doi.org/10.1016/j.jretai.2020.12.002.

[3] F. Horasan, “Keyword Extraction for Search Engine Optimization Using Latent Semantic Analysis,” Politeknik Dergisi, vol. 24, no. 2, pp. 473–479, 2021. URL: https://doi.org/10.2339/politeknik.684377.

[4] K. I. Roumeliotis and N. D. Tselikas, “An Effective SEO Techniques and Technologies Guide-Map,” Journal of Web Engineering, vol. 21, no. 5, pp. 1603–1650, 2022. URL: https://doi.org/10.13052/jwe1540-9589.21510.

[5] K. I. Roumeliotis, N. D. Tselikas, and C. Tryfonopoulos, “Greek Hotels’ Web Traffic: A Comparative Study Based on Search Engine Optimization Techniques and Technologies,” Digital, vol. 2, no. 3, pp. 379–400, 2022. URL: https://doi.org/10.3390/digital2030021.

[6] K. I. Roumeliotis, N. D. Tselikas, and D. K. Nasiopoulos, “Airlines’ Sustainability Study Based on Search Engine Optimization Techniques and Technologies,” Sustainability, vol. 14, no. 18, Art. 11225, 2022. URL: https://doi.org/10.3390/su141811225.

[7] K. I. Roumeliotis and N. D. Tselikas, “A Machine Learning Python-Based Search Engine Optimization Audit Software,” Informatics, vol. 10, no. 3, Art. 68, 2023. URL: https://doi.org/10.3390/informatics10030068.

[8] M. S. Vinutha and M. C. Padma, “Insights into Search Engine Optimization Using Natural Language Processing and Machine Learning,” International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, pp. 86–96, 2023. URL: https://doi.org/10.14569/IJACSA.2023.0140211.

[9] D. Mladenović, A. Rajapakse, N. Kožuljević, et al., “Search Engine Optimization (SEO) for Digital Marketers: Exploring Determinants of Online Search Visibility for Blood Bank Service,” Online Information Review, vol. 47, no. 4, pp. 661–679, 2023. URL: https://doi.org/10.1108/OIR-05-2022-0276.

[10] J.-C. Chen and S. Sénéchal, “The Reciprocal Relationship Between Search Engine Optimization (SEO) Success and Brand Equity: An Analysis of SMEs,” European Business Review, vol. 35, no. 5, pp. 860–873, 2023. URL: https://doi.org/10.1108/EBR-02-2023-0045.
[11] A. Caro, A. J. Mendoza, H. Noble, and K. A. Tanglao, “Influence of Search Engine Optimization (SEO) Towards Purchase Intention of Online Shoppers,” Journal of Business and Management Studies, vol. 6, no. 3, pp. 279–285, 2024. URL: https://doi.org/10.32996/jbms.2024.6.3.24.
[12] D. M. A. Abu, “Features of the Development of Search Optimization in the Strategy of Electronic Marketing,” E3S Web of Conferences, vol. 419, Art. 02020, 2023. URL: https://doi.org/10.1051/e3sconf/202341902020.

Дата першого надходження статті до видання: 28.01.2026
Дата прийняття статті до друку після рецензування: 19.02.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359287

УДК 004.832.32

СУЧАСНІ АРХІТЕКТУРИ ПРИЙНЯТТЯ РІШЕНЬ АВТОНОМНИМИ АГЕНТАМИ

Є.А. Соболь, А.А. Понепаляк, Я.Ю. Дорогий
Department of Artificial Intelligence and Cybersecurity, Donetsk National Technical University, Institute of Computer and Information Technologies and Automation, Drohobych, Ukraine
ORCID https://orcid.org/0009-0001-1607-8289
ORCID https://orcid.org/0009-0007-3514-2841
ORCID https://orcid.org/0000-0003-3848-9852
E-mail: yevhen.sobol.asp@donntu.edu.ua

АНОТАЦІЯ

Автономні агенти, що функціонують у високодинамічних та стохастичних середовищах із високим рівнем невизначеності, потребують обчислювально ефективних і надійних архітектур прийняття рішень. Історично управління такими системами базувалося на класичних парадигмах, серед яких – реактивні архітектури, скінченні автомати та дерева поведінки. Однак ці методи стикаються з проблемою експоненціального комбінаторного вибуху простору станів у неструктурованих умовах і демонструють критичну деградацію ефективності через нездатність до безперервної адаптації. Водночас перехід до сучасних суто нейромережевих методів управління супроводжується іманентною схильністю систем до стохастичних галюцинацій, епістемічною непрозорістю механізмів прийняття рішень і принциповою неможливістю забезпечення детермінованих математичних гарантій безпечного функціонування. У цій статті досліджуються й обгрунтовуються гібридні нейросимвольні архітектури, які синергетично поєднують апроксимаційні можливості методів глибокого навчання для обробки мультимодальних сенсорних даних із математичною строгістю та семантичною інтерпретованістю методів класичної символьної логіки. Проведено комплексний аналіз структурної інтеграції нейромережевих модулів екстракції високорівневих ознак із графовими моделями світу та ієрархічними символьними планувальниками. Особлива увага приділяється вирішенню проблеми семантичної неоднозначності шляхом автоматизованої верифікації структури графів знань та усунення логічних колізій до початку стадії фізичного виконання дій. Доведено перспективність використання семантичної декомпозиції сцени для оптимізації обчислювальних ресурсів.

Ключові слова: *автономні агенти, архітектури прийняття рішень, нейросимвольний штучний інтелект, глибоке навчання, символьна логіка, дерева поведінки, графи знань, семантичне моделювання.*

Вступ

Стрімкий розвиток робототехніки та систем штучного інтелекту зумовлює потребу у створенні надійних архітектур прийняття рішень для автономних агентів, що функціонують у високодинамічних та стохастичних середовищах із високим рівнем невизначеності. Історично управління подібними системами грунтувалося [1] на класичних парадигмах, серед яких домінували реактивні архітектури, скінченні автомати, дерева поведінки та системи, побудовані на основі архітектури Belief–Desire–Intention (BDI). Попри високу передбачуваність поведінки та відносну простоту формальної верифікації, зазначені підходи демонструють істотні обмеження під час масштабування до складних завдань і стикаються з проблемою комбінаторного вибуху [2] простору станів у неструктурованих умовах. Вони виявляються малоефективними в ситуаціях, що потребують безперервної адаптації до непередбачуваних змін навколишнього середовища, оскільки жорстко визначені правила не здатні адекватно відобразити всю варіативність та контекстну залежність процесів рального фізичного світу [3]. Забезпечення стійкої довготривалої автономії потребує безперервної конвергенції підсистем низькорівневого машинного сприйняття та високорівневого когнітивного планування, що реалізується через перехід від суто метричного до просторового семантичного подання динамічного середовища в режимі реального часу [4].

Таке абстрактне концептуальне моделювання формує репрезентативний базис для формалізації цільової поведінки програмних систем автономних агентів із використанням графових моделей світу та графів словесних описів функцій, що забезпечує прозору й адаптивну реконфігурацію ієрархії завдань та динамічний перерахунок послідовності дій за

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359287

стохастичних збурень зовнішнього середовища [5]. Фундаментальний синтез абстрактної логіки прийняття рішень із фізичними параметрами простору досягається шляхом упровадження гібридних нейросимвольних фреймворків і парадигми штучного інтелекту з фізичним втіленням (Embodied AI) [6], які утворюють замкнений цикл управління між оцінкою мультимодального контексту та виконанням структурованих стратегій, повністю компенсуючи концептуальну неінтерпретованість глибоких нейронних мереж детермінованими математичними гарантіями символьного логічного виведення під час планування місії [7].

Аналіз літературних джерел

Фундаментальною основою створення автономних систем історично виступали класичні алгоритми прийняття рішень, орієнтовані на функціонування у детермінованих та частково структурованих середовищах. Дослідники [8–10] виділяють реактивні архітектури як першу парадигму, що забезпечила роботу агентів у режимі реального часу, такі системи діють за принципом прямого відображення сенсорних даних у керуючі команди без формування складної внутрішньої моделі світу [8]. Аналіз їхньої ефективності [11] свідчить, що хоча такий підхід гарантує мінімальну затримку реакції, його результативність стрімко знижується в разі виконання багатоетапних завдань, що потребують довгострокового планування. Для подолання цих обмежень, згідно з інженерною практикою, у проєктування робототехнічних систем було впроваджено скінченні автомати (FSM), які дають змогу агенту переходити між наперед визначеними станами на основі ідентифікації дискретних подій. Водночас автори досліджень [12; 13] наголошують на суттєвому недоліку скінченних автоматів, а саме їхній схильності до комбінаторного вибуху. Як демонструють результати моделювання багатоагентних систем [14], у складних динамічних середовищах кількість можливих станів і переходів між ними збільшується експоненційно. Це не лише критично ускладнює обчислення та унеможливлює масштабування класичних дискретних архітектур, але й змушує переходити до нейромережевих методів управління, які, зі свого боку, позбавлені математичних гарантій та можливості надійної формальної верифікації.

Наступним еволюційним кроком у формалізації цільової поведінки стало застосування дерев поведінки, які забезпечують ієрархічну та модульну структуру виконання завдань. Автори концепції [15] зазначають, що, на відміну від FSM, дерева поведінки дають можливість інкапсулювати окремі підзадачі, що суттєво спрощує проектування комплексної логіки автономних систем та уможливлює повторне використання вузлів прийняття рішень. Паралельно із цим для моделювання складних когнітивних процесів і планування місій активно використовувалася архітектура BDI. Згідно з формальним визначенням ця модель оперує абстрактними ментальними станами агента, де «переконання» відображають формалізовані знання про світ, «бажання» формують цільові стани, а «наміри» є вибраними стратегіями досягнення цих цілей через генерацію плану дій [16]. Крім того, розширенням можливостей мультиагентної взаємодії та обробки гетерогенних даних визнано архітектуру дошки оголошень. Автори [17] описують її як систему, у якій незалежні експертні модулі асинхронно обмінюються інформацією через спільний простір пам’яті для кооперативного розв’язання задач.

Постановка проблеми

Незважаючи на формальну верифікованість та математичну прозорість процесів логічного виведення, класичні парадигми управління демонструють критичну деградацію ефективності у високодинамічних середовищах унаслідок своєї фундаментальної залежності від детермінованих евристичних правил, які концептуально не здатні адекватно апроксимувати комплексну стохастичність реального фізичного світу. Дослідження [3; 6] підтверджують, що автономні агенти, архітектура управління яких побудована суто на символьних або реактивних алгоритмах, концептуально не здатні до узагальнення. Згідно з результатами емпіричних тестувань, стикаючись із непередбачуваними перешкодами, раптовою зміною параметрів середовища або частковою втратою сенсорних даних, такі системи неминуче зазнають обчислювальних збоїв або генерують критично хибні рішення [3]. Аналіз цих вразливостей доводить, що відсутність гнучких механізмів адаптації на основі безперервного потоку нових даних робить класичні архітектури принципово недостатніми для забезпечення стійкого довготривалого автономного функціонування. Саме цей фактор зумовлює об’єктивну інженерну необхідність переходу до сучасних нейромережевих та гібридних методів планування.

Аналіз сучасних підходів

Подолання фундаментальних обмежень символьних методів стало можливим завдяки впровадженню алгоритмів глибокого навчання з підкріпленням (Deep Reinforcement Learning, DRL). DRL інтегрує апроксимаційні можливості глибоких нейронних мереж із процесами марковського прийняття рішень, даючи змогу агенту автономно формувати оптимальну стратегію поведінки через безперервну взаємодію із середовищем. У задачах просторової навігації та планування DRL демонструє високу ефективність завдяки здатності обробляти багатовимірні

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359287

сенсорні потоки без необхідності ручного конструювання евристичних ознак. Зокрема, ієрархічні архітектури DRL дають можливість декомпозувати комплексні навігаційні завдання на високорівневе стратегічне планування та низькорівневе керування виконавчими механізмами, що суттєво підвищує стабільність роботи автономної системи в умовах неповної спостережуваності та непередбачуваної динаміки трафіку або перешкод [18]. Приклад структурної схеми архітектури на базі DRL, о дописано в дослідженні [18], зображено на рисунку 1.

Наступним етапом еволюції систем управління стало застосування великих мовних і мультимодальних моделей (LLM/VLM) як центрального ядра когнітивної архітектури агента [19]. У цій парадигмі процеси когнітивного «міркування» й безпосереднього прийняття рішень формалізуються через механізми обробки природної мови та візуальних даних, що найчастіше реалізується за допомогою методології Reasoning and Acting (ReAct) [20]. У таких системах мультимодальна модель отримує візуальні дані від

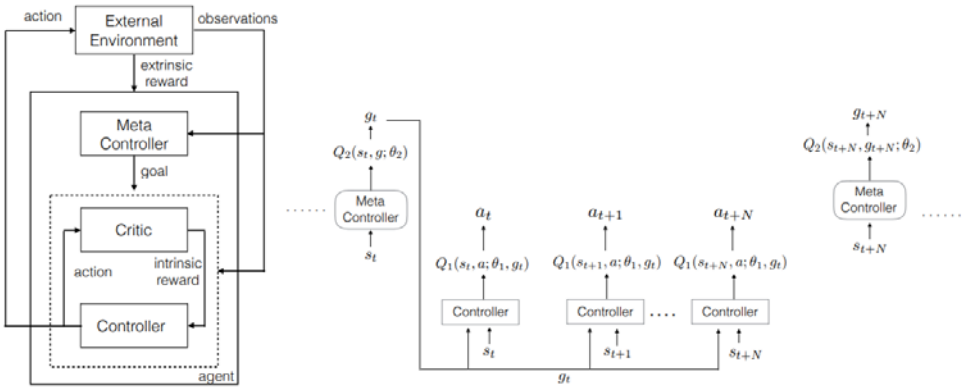

Рис. 1. Структурна схема інтеграції алгоритмів DRL у контур управління автономним агентом для обробки сенсорних потоків та безперервної взаємодії із середовищем [18]

сенсорів і генерує текстовий внутрішній контекст перед ініціалізацією фізичної дії, що дає змогу динамічно коригувати план місії відповідно до змін середовища.

Такі інтелектуальні системи [21] здатні безпосередньо транслювати високорівневі словесні інструкції та семантичні описи функцій у формалізовану послідовність дій (зокрема, графових операцій), оминаючи необхідність жорсткого програмування специфічних правил поведінки [6]. Проте процес такої автоматичної трансляції супроводжується фундаментальною проблемою семантичної неоднозначності та надмірності природної мови. Пряме, неоптимізоване трансформування неструктурованих вербальних описів функціональних вимог у виконувані вузли неминуче спричиняє формування надмірно ускладнених та внутрішньо неузгоджених графів завдань, що істотно знижує продуктивність і надійність програмно-технічної системи. На цьому етапі постає критична потреба в інтеграції спеціалізованих інтелектуальних методів формального аналізу та оптимізації. Їх застосування дає змогу в автоматизованому режимі верифікувати структуру та семантичні зв’язки всередині графів словесних описів функцій, усувати логічні колізії, ідентифікувати дубльовані фрагменти та відсікати нерелевантні операції до початку стадії фізичного виконання. Така попередня фільтрація суттєво підвищує ефективність реалізації функціональної логіки програмних систем управління оскільки програмний агент отримує математично строго визначений, детермінований і обчислювально малоресурсомісткий план дій, сформований на основі первинно неструктурованого природномовного контексту.

Незважаючи на високу здатність до узагальнення, суто нейромережеві архітектури характеризуються низкою фундаментальних недоліків, серед яких – іманентна схильність до стохастичних галюцинацій, епістемічна непрозорість механізмів прийняття рішень і принципова неможливість забезпечення детермінованих математичних гарантій безпечного функціонування. Ефективним шляхом подолання цих обмежень вбачається імплементація парадигми нейросимвольного штучного інтелекту [22; 23], узагальнену архітектуру якої наведено на рисунку 2.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359287

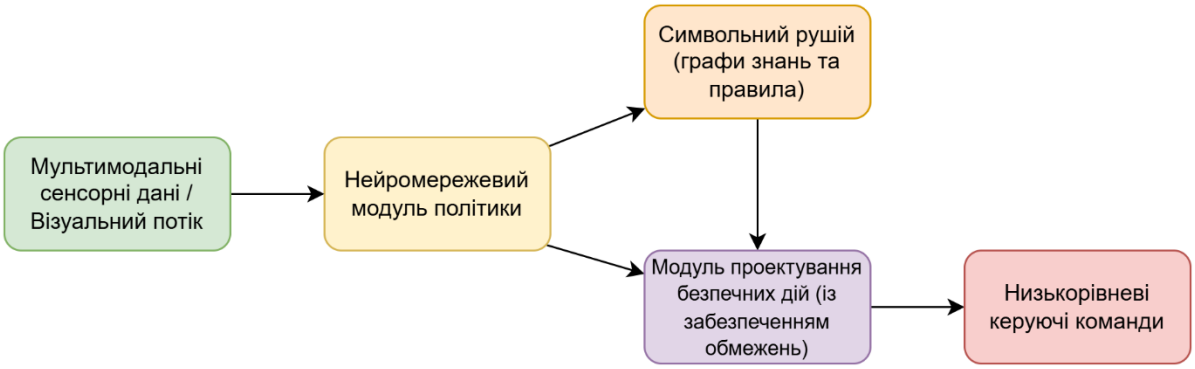

Рис. 2. Узагальнена архітектура нейросимвольного прийняття рішень автономним агентом (адаптовано на основі [23])

Зазначений гібридний підхід забезпечує синергетичну інтеграцію апроксимаційних можливостей нейромережевого екстрагування ознак із математичною строгістю, семантичною інтерпретованістю та здатністю до формальної верифікації, притаманними методам класичної символьної логіки. У подібних архітектурних підходах [24] модулі глибокого навчання відповідають за екстракцію високорівневих семантичних ознак із візуального потоку або на основі інших вхідних даних, тоді як символьні модулі оперують цими даними для формування й оновлення графів знань, а також для ініціалізації функціональної логіки на основі явно визначених обмежень [3]. Сучасні дослідження [25] підтверджують, що використання графових моделей світу дає можливість автономному агенту прозоро планувати дії та забезпечує високу адаптивність до нових умов шляхом динамічної реструктуризації вузлів та ребер графа завдань [5]. Показовим прикладом такої інтеграції є сучасні композиційні фреймворки [26], що об’єднують імовірнісне моделювання світу, розпізнавання об’єктів та ієрархічне планування для безпечного виконання багатоетапних пошукових місій в умовах значної невизначеності [7].

Обговорення результатів

Об’єктивне оцінювання ефективності архітектур прийняття рішень автономними агентами ускладнюється різницею у цільових завданнях і симуляційних середовищах (наприклад, ALFRED для indoor-навігації, AirSim для БПЛА, CARLA для міського трафіку). Незважаючи на це, систематизація метрик з актуальних досліджень дає змогу виявити чіткі тенденції щодо загальної успішності, швидкодії та точності розпізнавання. Згідно з дослідженнями [27] систем на базі великих мовних і мультимодальних моделей, інтеграція семантичного сприйняття відкритого словника з ієрархічними динамічними графами сцен забезпечує безпрецедентну здатність до узагальнення [28]. У тестах динамічної indoor-навігації архітектура OrionNav продемонструвала рівень успішності виконання завдань понад 88 % (85 успішних місій із 96), тоді як базові евристичні методи (Object-Map-Search) досягли лише 56 %, а алгоритми пошуку на основі границь (Frontier-Search) – 11 %. Швидкодія таких систем обмежується обчислювальною складністю генеративних моделей, частота оновлення семантичної карти становить близько 2 Гц, хоча генерація масок об’єктів може відбуватися із частотою до 10 Гц. Для порівняння: модульні архітектури з метрико-семантичними сітками (наприклад, Kimera) здатні досягати швидкодії 0,1 секунди на ключовий кадр, працюючи лише на центральних процесорах без залучення графічних прискорювачів [29].

У контексті реалізації комплексних пошукових місій в умовах високого рівня стохастичної невизначеності результати досліджень композиційних нейросимвольних архітектур емпірично підтверджують функціональну перевагу гібридних парадигм над суто нейромережевими підходами на базі мультимодальних моделей. Відповідно до результатів симуляційного моделювання фреймворку NEUSIS [7] у тестовому середовищі AirSim, структурна інтеграція модуля нейросимвольного сприйняття GRID з імовірнісною моделлю світу та ієрархічним символьним планувальником SNaC забезпечила досягнення показника успішності виконання завдань на рівні 61,82 %. Порівняльний аналіз засвідчує, що базова еталонна архітектура, яка застосовувала лише нейромережевий детектор YOLO-World для підсистеми сприйняття простору й алгоритм Fields2Cover для формування символьного плану дій, продемонструвала значно нижчий показник результативності, що становить 29,58 %. Додатково встановлено, що імплементація механізмів байєсівської фільтрації до складу ймовірнісної моделі світу статистично значущо підвищує точність просторової локалізації цільових

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359287

об’єктів, що підтверджується зростанням метрики Online F1 Score з 44,62 до 54,12 %.

У контексті високоструктурованих динамічних середовищ, зокрема міського автомобільного трафіку, як широкі оглядові [30], так і цілеспрямовані емпіричні дослідження ієрархічних архітектур [31] підтверджують їхню оптимальну швидкодію та високий рівень експлуатаційної надійності. Відповідно до результатів дослідження [31] під час симуляційного моделювання у платформі CARLA, архітектура, що інтегрує графові згорткові мережі (GCN) для аналізу часових рядів просторових станів із класичними пропорційно-інтегрально-диференціюючими регуляторами для низькорівневого управління, забезпечує імовірність успішного досягнення цільової точки на рівні 98,7–98,8 %. Зазначений показник статистично наближається до результатів ідеалізованої еталонної системи, яка функціонувала в умовах детермінованого доступу до глобальної інформаційної бази симулятора (98,9–99,2 %). Частота циклу управління запропонованої архітектури варіюється в діапазоні від 13,4 до 17,9 кадрів за секунду, що уможливлює керування автономним транспортним засобом у режимі реального часу. Показники ефективності досліджуваних архітектур наведно в таблиці 1.

Табл. 1. Порівняльна характеристика архітектур прийняття рішень автономними агентами за результатами емпіричних досліджень

Модель	Архітектура	Цільове завдання та середовище	Показник успішності (SR)	Швидкодія / Частота управління (FPS)
OrionNav	LLM + ієрархічні семантичні графи сцен	Indoor-навігація, пошук об’єктів (фізичний робот)	88,5 %	Оновлення семантичної карти ~ 2 Гц
NEUSIS	Нейросимвольна VLM + SNaC + World Model	Пошукові місії БПЛА (AirSim / Unreal Engine)	61,82 %	Оновлення світової моделі в реальному часі
Ієрархічна GCN + IDM/PID (YOLO + графи часових рядів)		Автономне водіння, рух у трафіку (CARLA)	98,7–98,8 %	13,5–18,0 FPS
PaLM-SayCan	LLM + Value Functions / DRL	Роботизована маніпуляція, виконання інструкцій (фізичне середовище)	74 %	Асинхронне планування на основі діалогового запиту
Kimera	Метрико-семантичний SLAM	3D-реконструкція сцени, VIO (EuRoC, фізичне середовище)	–	> 10 FPS

Висновки

Попри значний прогрес гібридних фреймворків, структурна інтеграція високорівневих когнітивних процесів із низькорівневим кінематичним виконанням залишається фундаментальним викликом у галузі робототехніки. Провідні дослідження [24; 28] визначають головною проблемою наявність нездоланного семантичного розриву між абстрактним дискретним плануванням, що реалізується на базі графових або мовних моделей, і безперервним сенсомоторним управлінням у режимі реального часу. Відповідно до результатів аналізу сучасних систем, така архітектурна асиметрія неминуче спричиняє критичні затримки в генерації керуючих сигналів під час функціонування автономного агента у швидкозмінних динамічних середовищах [4].

Додатковим відкритим фундаментальним питанням, що широко дискутується в науковій літературі, є проблема експоненціального перенасичення бази знань довготривалої пам’яті застарілими та нерелевантними топологічними зв’язками [32]. Емпірично доведено, що під час тривалої роботи цей процес призводить до експоненціального зростання обчислювальної складності та відповідної деградації загальної продуктивності системи управління [6]. Враховуючи зазначені технологічні бар’єри, можна постановити, що майбутні вектори досліджень мають фокусуватися на розробленні уніфікованих гібридних репрезентацій середовища, здатних забезпечити нативне поєднання метричної кінематичної точності з високорівневою семантичною абстракцією. Саме тут використання семантичної декомпозиції сцени дає змогу радикально оптимізувати обчислювальні ресурси шляхом інтелектуального звуження простору пошуку для алгоритмів планування траєкторії. Замість ітеративного перебору всіх геометрично можливих шляхів у метричній карті, агент оперує семантичними доменами, завдяки чому може виключати завідомо нерелевантні зони ще на етапі високорівневого планування. Це перетворює задачу глобального пошуку на послідовність локальних оптимізацій у межах вибраних семантичних контекстів. Однак, оскільки в процесі довготривалої роботи кількість виділених

семантичних зв’язків безперервно акумулюється, у разі формування масивних графів знань, виникає потреба у їх ефективному опрацюванні. З огляду на це найбільш перспективними напрямами подальших наукових досліджень визначено структурну оптимізацію нейросимвольних архітектур шляхом імплементації механізмів диференційованого логічного виведення [7] а також синтез високоефективних алгоритмів для динамічної редукції графів знань.

Конфлікт інтересів

Автор декларує, що не має конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] Nakhaeinia, Tang, Mohd Noor, and Motlagh, “A review of control architectures for autonomous navigation of mobile robots,” International Journal of the Physical Sciences, vol. 62, pp. 169–174, 2011.

[2] P. Simen, “Preventing combinatorial explosion in a localist, neural network architecture using temporal synchrony,” Connection Science, vol. 23, no. 2, pp. 131–144, May 2011. DOI: 10.1080/09540091.2011.570741.

[3] T. Mota, M. Sridharan, and A. Leonardis, “Integrated commonsense reasoning and deep learning for transparent decision making in robotics,” SN Computer Science, vol. 2, no. 4, Apr. 2021. DOI: 10.1007/s42979-021-00573-0.

[4] V. Vasilopoulos et al., “Reactive semantic planning in unexplored semantic environments using deep perceptual feedback,” IEEE Robotics and Automation Letters, vol. 5, no. 3, pp. 4455–4462, Jun. 2020. DOI: 10.1109/lra.2020.3001496.

[5] S. Hu, T. Horii, and T. Nagai, “Adaptive and transparent decision-making in autonomous robots through graph-structured world models,” Advanced Robotics, vol. 38, no. 22, pp. 1579–1599, Oct. 2024. DOI: 10.1080/01691864.2024.2415995.

[6] Y. Zhang, J. Tian, and Q. Xiong, “A review of embodied intelligence systems: a three-layer framework integrating multimodal perception, world modeling, and structured strategies,” Frontiers in Robotics and AI, vol. 12, p. 1668910, Nov. 2025. DOI: 10.3389/frobt.2025.1668910.

[7] Z. Cai et al., “NEUSIS: a compositional Neuro-Symbolic framework for autonomous perception, reasoning, and planning in complex UAV search missions,” arXiv (Cornell University), Sep. 2024. DOI: 10.48550/arxiv.2409.10196.

[8] Brooks, “A robust layered control system for a mobile robot,” Massachusetts Institute of Technology, Artificial Intelligence Laboratory, a. I. Memo, vol. 864, Sep. 1985.

[9] R. C. Arkin, “Motor Schema – based Mobile Robot navigation,” The International Journal of Robotics Research, vol. 8, no. 4, pp. 92–112, Aug. 1989. DOI: 10.1177/027836498900800406.

[10] L. Luc Steels, Ed., A case study in the behavior-oriented design of autonomous agents. MIT Press, Cambridge, MA, USA.

[11] R. P. Bonasso, R. J. Firby, E. Gat, D. Kortenkamp, D. P. Miller, and M. G. Slack, “Experiences with an architecture for intelligent, reactive agents,” Journal of Experimental & Theoretical Artificial Intelligence, vol. 9, no. 2–3, pp. 237–256, Apr. 1997. DOI: 10.1080/095281397147103.

[12] M. Klotzbucher and H. Bruyninckx, “Coordinating robotic tasks and systems with RFSM Statecharts,” Journal of Software Engineering for Robotics, vol. 3, no. 1, pp. 28–56, 2011.

[13] H. Bou-Ammar, M. Jaber, and M. Nassar, “Correctness-by-Learning of Infinite-State Component-Based Systems,” in Lecture notes in computer science, 2017, pp. 162–178. DOI: 10.1007/978-3-319-68034-7_10.

[14] P. Ojala, “Reinforcement learning in Multi-Agent Path Finding,” Bachelor’s Thesis, Aalto University School of Electrical Engineering, 2025.

[15] M. Colledanchise and P. Ögren, Behavior trees in robotics and AI. 2018. DOI: 10.1201/9780429489105.

[16] Georgeff, Ed., BDI Agents: From Theory to practice. International Conference on Multiagent Systems, 1995.

[17] Nii, “The Blackboard Model of Problem Solving and the Evolution of Blackboard Architectures,” AIMag, vol. 7, no. 2, p. 38, Jun. 1986.

[18] Kulkarni, Narasimhan, A. Saeedi, and J. B. Tenenbaum, Hierarchical Deep Reinforcement Learning: Integrating Temporal Abstraction and Intrinsic Motivation. Advances in Neural Information Processing Systems 29 (NIPS 2016), 2015.

[19] W. Huang et al., “Inner Monologue: Embodied Reasoning through Planning with Language Models,” arXiv (Cornell University), Jul. 2022. DOI: 10.48550/arxiv.2207.05608.

[20] S. Yao et al., REACT: Synergizing reasoning and acting in language models. ICLR, 2023.

[21] M. Ahn et al., “Do as I can, not as I say: grounding language in robotic affordances,” arXiv (Cornell University), Apr. 2022. DOI: 10.48550/arxiv.2204.01691.

[22] A. D. Garcez and L. C. Lamb, “Neurosymbolic AI: The 3rd Wave,” arXiv (Cornell University), Dec. 2020. DOI: 10.48550/arxiv.2012.05876.

[23] K. Addo, M. Kabeya, and E. E. Ojo, “Neuro-Symbolic AI for explainable Decision-Making in autonomous grid operations,” Preprints.org, Aug. 2025. DOI: 10.20944/preprints202508.0747.v1.

[24] M. A. Ali, F. Dornaika, and J. Charafeddine, “Agentic AI: a comprehensive survey of architectures, applications, and

future directions,” Artificial Intelligence Review, vol. 59, no. 1, Nov. 2025. DOI: 10.1007/s10462-025-11422-4.
[25] Q. Gu et al., “ConceptGraphs: Open-Vocabulary 3D scene graphs for perception and planning,” arXiv (Cornell University), Sep. 2023. DOI: 10.48550/arxiv.2309.16650.
[26] F. Ke, Z. Cai, S. Jahangard, W. Wang, P. D. Haghighi, and H. Rezatofighi, “HYDRA: a hyper agent for dynamic compositional visual reasoning,” in Lecture notes in computer science, 2024, pp. 132–149. DOI: 10.1007/978-3-031-72661-3_8.
[27] L. Miao, W. Liu, and Z. Deng, “A frontier review of semantic SLAM technologies applied to the open world,” Sensors, vol. 25, no. 16, p. 4994, Aug. 2025. DOI: 10.3390/s25164994.
[28] V. N. Devarakonda et al., “OrionNav: Online Planning for Robot Autonomy with Context-Aware LLM and Open-Vocabulary Semantic Scene Graphs,” arXiv (Cornell University), Oct. 2024. DOI: 10.48550/arxiv.2410.06239.
[29] A. Rosinol, M. Abate, Y. Chang, and L. Carlone, Kimera: an Open-Source Library for Real-Time Metric-Semantic Localization and Mapping. Paris, France: IEEE International Conference on Robotics and Automation (ICRA), 2020, pp. 1689–1696. DOI: 10.1109/icra40945.2020.9196885.
[30] B. R. Kiran et al., “Deep Reinforcement Learning for Autonomous Driving: a survey,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 6, pp. 4909–4926, Feb. 2021. DOI: 10.1109/tits.2021.3054625.
[31] F. Yang et al., “Learning-Based hierarchical Decision-Making framework for automatic driving in incompletely connected traffic scenarios,” Sensors, vol. 24, no. 8, p. 2592, Apr. 2024. DOI: 10.3390/s24082592.
[32] C. Cheng et al., “LongStream: Long-Sequence Streaming autoregressive Visual geometry,” arXiv (Cornell University), Feb. 2026. DOI: 10.48550/arxiv.2602.13172.

CURRENT ARCHITECTURES FOR DECISION-MAKING BY AUTONOMOUS AGENTS

Yevhen Sobol, Andrii Ponepaliak, Yaroslav Dorogiy

Autonomous agents operating in highly dynamic and stochastic environments with a high degree of uncertainty require computationally efficient and reliable decision-making architectures. Historically, the control of such systems has been based on classical paradigms, including reactive architectures, finite state machines, and behavior trees. However, these methods face the problem of an exponential combinatorial explosion of the state space in unstructured conditions and exhibit a critical degradation in performance due to their inability to adapt continuously. At the same time, the transition to modern, purely neural network-based control methods is accompanied by an inherent tendency of systems toward stochastic hallucinations, epistemic opacity of decision-making mechanisms, and a fundamental inability to provide deterministic mathematical guarantees of safe operation.

This article investigates and justifies hybrid neurosymbolic architectures that synergistically combine the approximation capabilities of deep learning methods for processing multimodal sensory data with the mathematical rigor and semantic interpretability of classical symbolic logic methods. A comprehensive analysis was conducted of the structural integration of neural network modules for high-level feature extraction with graph-based world models and hierarchical symbolic planners. Particular attention is paid to solving the problem of semantic ambiguity through automated verification of the structure of knowledge graphs and the elimination of logical conflicts prior to the start of the physical execution stage. The promise of using semantic scene decomposition for optimizing computational resources has been demonstrated.

Keywords: *autonomous agents, decision-making architectures, neuro-symbolic artificial intelligence, deep learning, symbolic logic, behavior trees, knowledge graphs, semantic modeling.*

REFERENCES

[1] Nakhaeinia, Tang, Mohd Noor, and Motlagh, “A review of control architectures for autonomous navigation of mobile robots,” *International Journal of the Physical Sciences*, vol. 62, Art. no. 169–174, 2011.
[2] P. Simen, “Preventing combinatorial explosion in a localist, neural network architecture using temporal synchrony,” *Connection Science*, vol. 23, no. 2, pp. 131–144, May 2011, doi: 10.1080/09540091.2011.570741.
[3] T. Mota, M. Sridharan, and A. Leonardis, “Integrated commonsense reasoning and deep learning for transparent decision making in robotics,” *SN Computer Science*, vol. 2, no. 4, Apr. 2021, doi: 10.1007/s42979-021-00573-0.
[4] V. Vasilopoulos *et al.*, “Reactive semantic planning in unexplored semantic environments using deep perceptual feedback,” *IEEE Robotics and Automation Letters*, vol. 5, no. 3, pp. 4455–4462, Jun. 2020, doi: 10.1109/lra.2020.3001496.
[5] S. Hu, T. Horii, and T. Nagai, “Adaptive and transparent decision-making in autonomous robots through graph-structured world models,” *Advanced Robotics*, vol. 38, no. 22, pp. 1579–1599, Oct. 2024, doi: 10.1080/01691864.2024.2415995.
[6] Y. Zhang, J. Tian, and Q. Xiong, “A review of embodied intelligence systems: a three-layer framework integrating multimodal perception, world modeling, and structured strategies,” *Frontiers in Robotics and AI*, vol. 12, p. 1668910, Nov. 2025, doi: 10.3389/frobt.2025.1668910.
[7] Z. Cai *et al.*, “NEUSIS: a compositional Neuro-Symbolic framework for autonomous perception, reasoning, and planning in complex UAV search missions,” *arXiv (Cornell University)*, Sep. 2024, doi: 10.48550/arxiv.2409.10196.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359287

[8] Brooks, “A robust layered control system for a mobile robot,” *Massachusetts Institute of Technology, Artificial Intelligence Laboratory, a. I. Memo*, vol. 864, Sep. 1985.

[9] R. C. Arkin, “Motor Schema – based Mobile Robot navigation,” *The International Journal of Robotics Research*, vol. 8, no. 4, pp. 92–112, Aug. 1989, doi: 10.1177/027836498900800406.

[10] L. Luc Steels, Ed., *A case study in the behavior-oriented design of autonomous agents*. MIT Press, Cambridge, MA, USA.

[11] R. P. Bonasso, R. J. Firby, E. Gat, D. Kortenkamp, D. P. Miller, and M. G. Slack, “Experiences with an architecture for intelligent, reactive agents,” *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 9, no. 2–3, pp. 237–256, Apr. 1997, doi: 10.1080/095281397147103.

[12] M. Klotzbucher and H. Bruyninckx, “Coordinating robotic tasks and systems with RFSM Statecharts,” *Journal of Software Engineering for Robotics*, vol. 3, no. 1, pp. 28–56, 2011.

[13] H. Bou-Ammar, M. Jaber, and M. Nassar, “Correctness-by-Learning of Infinite-State Component-Based Systems,” in *Lecture notes in computer science*, 2017, pp. 162–178. doi: 10.1007/978-3-319-68034-7_10.

[14] P. Ojala, “Reinforcement learning in Multi-Agent Path Finding,” Bachelor’s Thesis, Aalto University School of Electrical Engineering, 2025.

[15] M. Colledanchise and P. Ögren, *Behavior trees in robotics and AI*. 2018. doi: 10.1201/9780429489105.

[16] Georgeff, Ed., *BDI Agents: From Theory to practice*. International Conference on Multiagent Systems, 1995.

[17] Nii, “The Blackboard Model of Problem Solving and the Evolution of Blackboard Architectures,” *AIMag*, vol. 7, no. 2, p. 38, Jun. 1986.

[18] Kulkarni, Narasimhan, A. Saeedi, and J. B. Tenenbaum, *Hierarchical Deep Reinforcement Learning: Integrating Temporal Abstraction and Intrinsic Motivation*. Advances in Neural Information Processing Systems 29 (NIPS 2016), 2015.

[19] W. Huang *et al.*, “Inner Monologue: Embodied Reasoning through Planning with Language Models,” *arXiv (Cornell University)*, Jul. 2022, doi: 10.48550/arxiv.2207.05608.

[20] S. Yao *et al.*, *REACT: Synergizing reasoning and acting in language models*. ICLR, 2023.

[21] M. Ahn *et al.*, “Do as I can, not as I say: grounding language in robotic affordances,” *arXiv (Cornell University)*, Apr. 2022, doi: 10.48550/arxiv.2204.01691.

[22] A. D. Garcez and L. C. Lamb, “Neurosymbolic AI: The 3rd Wave,” *arXiv (Cornell University)*, Dec. 2020, doi: 10.48550/arxiv.2012.05876.

[23] K. Addo, M. Kabeya, and E. E. Ojo, “Neuro-Symbolic AI for explainable Decision-Making in autonomous grid operations,” *Preprints.org*, Aug. 2025, doi: 10.20944/preprints202508.0747.v1.

[24] M. A. Ali, F. Dornaika, and J. Charafeddine, “Agentic AI: a comprehensive survey of architectures, applications, and future directions,” *Artificial Intelligence Review*, vol. 59, no. 1, Nov. 2025, doi: 10.1007/s10462-025-11422-4.

[25] Q. Gu *et al.*, “ConceptGraphs: Open-Vocabulary 3D scene graphs for perception and planning,” *arXiv (Cornell University)*, Sep. 2023, doi: 10.48550/arxiv.2309.16650.

[26] F. Ke, Z. Cai, S. Jahangard, W. Wang, P. D. Haghighi, and H. Rezatofighi, “HYDRA: a hyper agent for dynamic compositional visual reasoning,” in *Lecture notes in computer science*, 2024, pp. 132–149. doi: 10.1007/978-3-031-72661-3_8.

[27] L. Miao, W. Liu, and Z. Deng, “A frontier review of semantic SLAM technologies applied to the open world,” *Sensors*, vol. 25, no. 16, p. 4994, Aug. 2025, doi: 10.3390/s25164994.

[28] V. N. Devarakonda *et al.*, “OrionNav: Online Planning for Robot Autonomy with Context-Aware LLM and Open-Vocabulary Semantic Scene Graphs,” *arXiv (Cornell University)*, Oct. 2024, doi: 10.48550/arxiv.2410.06239.

[29] A. Rosinol, M. Abate, Y. Chang, and L. Carlone, *Kimera: an Open-Source Library for Real-Time Metric-Semantic Localization and Mapping*. Paris, France: IEEE International Conference on Robotics and Automation (ICRA), 2020, pp. 1689–1696. doi: 10.1109/icra40945.2020.9196885.

[30] B. R. Kiran *et al.*, “Deep Reinforcement Learning for Autonomous Driving: a survey,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 6, pp. 4909–4926, Feb. 2021, doi: 10.1109/tits.2021.3054625.

[31] F. Yang *et al.*, “Learning-Based hierarchical Decision-Making framework for automatic driving in incompletely connected traffic scenarios,” *Sensors*, vol. 24, no. 8, p. 2592, Apr. 2024, doi: 10.3390/s24082592.

[32] C. Cheng *et al.*, “LongStream: Long-Sequence Streaming autoregressive Visual geometry,” *arXiv (Cornell University)*, Feb. 2026, doi: 10.48550/arxiv.2602.13172.

Дата першого надходження статті до видання: 03.02.2026
Дата прийняття статті до друку після рецензування: 02.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

УДК 004.8

ОНЛАЙН-ОЦІНЮВАННЯ НАДІЙНОСТІ ДЖЕРЕЛ У ПОТОКОВОМУ АНАЛІЗІ МУЛЬТИМОДАЛЬНИХ ЧАСОВИХ РЯДІВ ІЗ КАЛІБРУВАННЯМ ІЗОТОНІЧНОЮ РЕГРЕСІЄЮ

І. С. Узун, М.В. Лобачев
Department of Artificial Intelligence and Data Analysis, Institute of Artificial Intelligence and Robotics, Odesa Polytechnic National University, Odesa, Ukraine
ORCID https://orcid.org/0000-0001-6619-4862
ORCID https://orcid.org/0000-0002-4859-304X
E-mail: uzun.i.s@op.edu.ua

АНОТАЦІЯ

Потокові інтелектуальні системи підтримки прийняття рішень, що обробляють мультимодальні часові ряди, працюють у режимі каузальності та мають задовольняти вимоги малої латентності, обмежених обчислювальних бюджетів і контрольованості реакцій на змінність середовища. Критичним практичним ризиком таких конвеєрів є тимчасова деградація окремих джерел (пропуски, підвищений шум, масштабні зсуви), яка може маскуватися під концептуальний дрейф та спричиняти нестабільні або надмірні керувальні дії. У роботі розглянуто онлайн-оцінювання надійності джерела як каузальної імовірнісної оцінки перебування в недеградованому стані та показано, що для практичного керування потрібна саме калібрована шкала: значення на виході має інтерпретуватися як частота «недеградованого» режиму в релевантних умовах. Запропонований підхід поєднує легкі проксі-сигнали деградації, придатні для онлайн-обчислення, з калібруванням ізотонічною регресією, що забезпечує монотонне відображення скору в коректну ймовірність. Ефективність оцінено метриками площі під ROC-кривою (ROC-AUC) для відокремлення деградованих станів та очікуваної помилки калібрування (Expected Calibration Error, ECE) для контролю ймовірнісної узгодженості. Ключові експериментальні результати демонструють ROC-AUC $0{,}86 \pm 0{,}07$ *для каліброваного варіанта та покращення каліброваності від ECE =* $0{,}18 \pm 0{,}07$ *(без калібрування) до ECE =* $0{,}08 \pm 0{,}04$ *(після калібрування) за прийнятних часових витрат: прості шкали-проксі мають мікросекундні затримки, а повна онлайн-модель зберігає середню латентність на рівні близько* $150\mu s$ *, що відповідає потребам потокових конвеєрів. Отриманий результат формує інтерпретований керувальний сигнал, придатний для інтеграції з процедурами злиття, подієвої бюджетованої адаптації та контрольованої сигналізації в потокових системах.*

Ключові слова: *машинне навчання, аналіз даних, інформаційні системи, системи підтримки прийняття рішень, мультимодальні часові ряди, потоковий аналіз, онлайн-калібрування, ізотонічна регресія, виявлення деградації, оцінювання надійності.*

Вступ

Потокові інтелектуальні системи підтримки прийняття рішень інтегрують дані з різнорідних джерел і формують прогнози та сигнали стану в режимі, наближеному до реального часу. У багатьох прикладних доменах дані природно мають вигляд часових рядів, а різні сенсорні та інформаційні канали утворюють мультимодальний потік, у якому модальності відрізняються масштабами, частотами дискретизації, затримками та типовими дефектами вимірювання. Для такого класу систем вирішальними є каузальність прийняття рішень, контроль латентності та керованість обчислювальних витрат, оскільки саме ці фактори визначають можливість експлуатації алгоритмів у потоці.

Практичний збійний сценарій полягає в тимчасовій деградації окремих модальностей: зростанні частки пропусків, підсиленні шуму або появі масштабних зсувів, що порушують стабільність прогнозування та сигналізації. У потоці ці ефекти часто накладаються на нестаціонарність середовища (зокрема, концептуальний дрейф), тому зростання похибки або зміна скорів може бути неоднозначно інтерпретоване. У результаті система ризикує або «пропускати» реальні відмови джерел, або навпаки запускати надмірні коригувальні дії (адаптацію, перемикання

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

режимів, перезважування модальностей), що підвищує вартість експлуатації та знижує довіру до рішень.

Одним зі способів зробити реакції потокової системи підтримки прийняття рішень керованими є введення явного *керувального сигналу якості* модальності, який відокремлює деградацію джерела від інших причин нестабільності. Однак для практичного використання цей сигнал має бути не лише дискримінативним, а й *інтерпретованим* та *каліброваним*, інакше пороги та правила керування не матимуть стабільного смислу між різними сегментами потоку. Саме ця мотивація визначає фокус статті: онлайн-оцінювання надійності з калібруванням ізотонічною регресією за збереження мікросекундного порядку латентності.

Аналіз літературних даних і постановка проблеми

Мультимодальне навчання та злиття даних є предметом систематичних оглядів, у яких запропоновано таксономію мультимодальних задач (representation, translation, alignment, fusion, co-learning) і підкреслено, що різна якість та неповнота модальностей є типовими проблемами інтеграції [1]. Огляд з мультимодального data fusion узагальнює стратегії об’єднання та формулює ключові виклики (узгодження, невизначеність, неповнота, неоднорідність), через які робастна інтеграція потребує явного врахування характеристик кожного джерела [2].

Для потокових сценаріїв принциповим є коректне онлайн-оцінювання в каузальних протоколах. Передпослідовний (prequential) підхід формалізує узгоджений режим test-then-train для хронологічних даних і використовується як базова методологія оцінювання в потокових задачах [3]. Практичні керівництва з навчання на потоках даних (зокрема, з прикладами в MOA) описують типові алгоритми, протоколи валідації та інженерні обмеження реального потоку [4]. Нестаціонарність потоків у прикладних задачах часто пов’язують із concept drift, для якого запропоновано класифікації типів дрейфу (раптовий, поступовий, рекурентний) та підходи до адаптації [5, 6]; окремо наведено порівняльний аналіз ансамблевих стратегій, що демонструє залежність ефективності від характеру нестаціонарності [7].

Окремою лінією досліджень є оцінювання й інтерпретація невизначеності прогнозів. У байєсівському глибокому навчанні обґрунтовано розрізнення алеаторної та епістемічної невизначеності й описано практичні схеми їх оцінювання [8], а також показано, що під зсувом даних оцінки невизначеності можуть ставати ненадійними [9]. Оглядові роботи пропонують уніфіковану формальну рамку для трактування різних типів невизначеності в машинному навчанні [10]. Проте невизначеність моделі та якість джерела даних не є тотожними: тимчасова деградація сенсора є властивістю вхідних спостережень і повинна діагностуватися каузально в термінах стану джерела, щоб керування було аудитованим.

У цьому контексті центральним стає калібрування ймовірнісних шкал. Показано, що навіть точні моделі (зокрема, сучасні глибокі мережі) можуть бути систематично некаліброваними, а temperature scaling є простою практичною корекцією; для контролю каліброваності широко застосовують ECE та діаграми надійності [11]. Класичне сигмоїдне (логістичне) калібрування перетворює скори класифікатора на ймовірності та використовується, зокрема, для побудови ймовірнісних виходів SVM [12]. Непараметричне калібрування ізотонічною регресією будує монотонне відображення «скор $\rightarrow$ імовірність» без параметричних припущень [13], а експериментальні порівняння показують, що цей підхід є гнучким, але чутливим до розміру калібрувального набору [14]. Бета-калібрування розглядається як теоретично обґрунтована альтернатива логістичному калібруванню для бінарних класифікаторів [15]. Окремо підкреслено, що оцінювання каліброваності потребує коректних статистичних процедур: стандартна ECE може бути зміщеною, а kernel-based тести пропонуються як більш строгий інструмент [16].

Для потокових систем важливо, що калібрування не повинно порушувати часові бюджети. Класичний ROC-аналіз обґрунтовує ROC-AUC як узагальнену міру якості ранжування, інваріантну до вибору порога, що є критичним для потокових сценаріїв із динамічними порогами [17].

Проблема полягає у відсутності підходу, який одночасно забезпечує (i) дискримінативне відокремлення деградованих станів, (ii) калібровану ймовірнісну інтерпретацію шкали надійності та (iii) мікросекундний порядок латентності, придатний для потокових конвеєрів.

Мета та задачі дослідження

Метою дослідження є розробка й експериментальна перевірка підходу до онлайн-оцінювання надійності джерел у потоковому аналізі мультимодальних часових рядів на основі легких проксі-сигналів деградації з калібруванням ізотонічною регресією. Для досягнення мети поставлено такі задачі:

1) формалізувати інтерпретацію надійності як керувального інтерфейсу потокової системи підтримки прийняття рішень;

2) обґрунтувати роль калібрування для стабільного використання порогів у правилах керування;

3) експериментально оцінити якість підходу за показниками ROC-AUC, ECE та латентності;

4) визначити обмеження й умови застосовності в реальних потокових системах.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

Постановка задачі. Нехай $\{x_t^{(m)}\}_{t\geq 1}$ – мультимодальний потік, де $m\in\{1,\ldots,M\}$ індексує модальність, а t – дискретний час. Деградація модальності розглядається як тимчасовий стан, що зумовлює погіршення інформативності або коректності спостережень, і може проявлятися у вигляді пропусків, шуму чи масштабних зсувів. Задача онлайн-оцінювання надійності полягає у формуванні в кожний момент часу t числа $r_t^{(m)}\in[0,1]$, яке інтерпретується як імовірність перебування модальності в недеградованому стані за каузально доступною історією.

Ключовою прикладною вимогою є каліброваність цієї шкали. Тобто якщо система повідомляє $r_t^{(m)}\approx 0{,}8$, то в довготривалому горизонті в схожих умовах частка «недеградованого» стану має бути близькою до 80 %; інакше пороги та політики керування стають неаудитованими. Якість відокремлення деградаційних станів оцінюється за ROC-AUC, а каліброваність – за ECE. Додатково для потокового режиму потрібна перевірка латентності як характеристика застосовності: метод має вкладатися в мікросекундні або субмілісекундні бюджети на крок, щоб не порушувати загальні вимоги до рівня сервісу конвеєра.

Легкі проксі-сигнали деградації. У потоковому режимі прямі «важкі» діагностики якості часто є недоступними або занадто дорогими, тому доцільно використовувати проксі-сигнали, що обчислюються каузально та мають низьку обчислювальну складність. У запропонованому підході акцент зроблено на проксі, пов’язані з часткою пропусків та зі статистиками, що відображають зміну похибки або штрафів, які супроводжують прогнозування. Ці сигнали не є повними моделями деградації, але вони придатні як оперативні індикатори в системах, де головною вимогою є швидкість реакції та контроль витрат.

Онлайн-оцінювання та калібрування. Базова ідея полягає в тому, що початковий скор надійності, побудований на проксі-сигналах, може бути дискримінативним, але некаліброваним. Щоб перетворити такий скор на ймовірність з інтерпретованим смислом, застосовується калібрування ізотонічною регресією, яка будує монотонне відображення «скор $\rightarrow$ імовірність». Монотонність є принциповою: вона узгоджується з інтуїцією проксі-сигналів деградації (гірший сигнал не повинен підвищувати надійність) і зменшує ризик артефактів керування, коли пороги починають реагувати нестабільно.

Практична цінність калібрування проявляється в тому, що пороги та правила, налаштовані на каліброваній шкалі, зберігають смисл між різними сегментами потоку та допускають аудит. З огляду на це надійність можна трактувати як керувальний інтерфейс: вона може використовуватися для перезважування модальностей у злитті, для умовного запуску подієвих процедур адаптації та для стабілізації сигналізації в задачах контролю ризику.

Порівняння ROC-кривих для різних варіантів оцінювання надійності наведено на рис. 1.

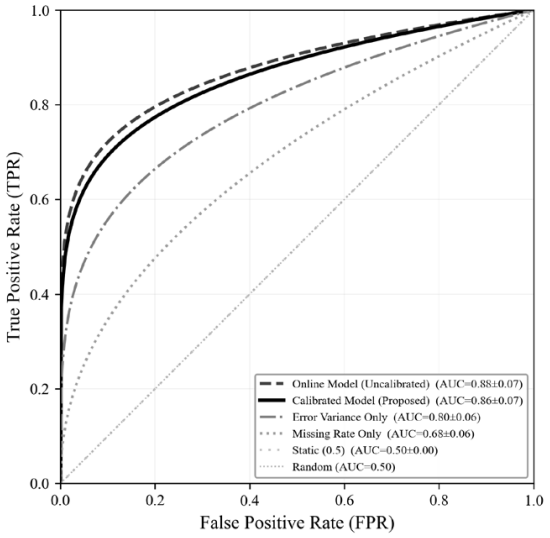

Рис. 1. ROC-криві для різних варіантів оцінювання надійності

Метрики якості та їх інтерпретація. Для дискримінаційної здатності шкали надійності у відокремленні «деградовано / недеградовано» доцільною є ROC-AUC як узагальнена міра якості ранжування, інваріантна до вибору конкретного порога [17]. Це особливо важливо в потокових сценаріях, де поріг може вибиратися на основі «чистого» префікса, під обмеження на частку хибних тривог, або як функція від бюджетів. Водночас ROC-AUC не відповідає на питання, чи можна інтерпретувати $r_t^{(m)}$ як імовірність; для цього потрібні калібрувальні метрики.

Метрика ECE вимірює узгодженість між «довірою» (confidence) та фактичною частотою правильних подій у групах спостережень. Один із поширених варіантів визначення ECE має вигляд:

$$\mathrm{ECE}=\sum_{b=1}^{B}\frac{|I_b|}{n}\left|\mathrm{acc}(I_b)-\mathrm{conf}(I_b)\right|, \qquad (1)$$

де n – кількість спостережень у калібрувальному наборі; B – кількість бінів; I_b – індекси спостережень, що потрапили в b-й бін за значенням скору; $\mathrm{acc}(I_b)$ – емпірична частота «позитивної» події (наприклад, недеградованого стану) в біні; $\mathrm{conf}(I_b)$ – середнє значення скору в біні [9]. Низька ECE означає, що шкалу можна використовувати як керувальну ймовірність у правилах, де важливе узгодження порогів із реальною частотою подій.

Діаграми надійності для каліброваного, некаліброваного й одноознакового варіантів наведено на рис. 2.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

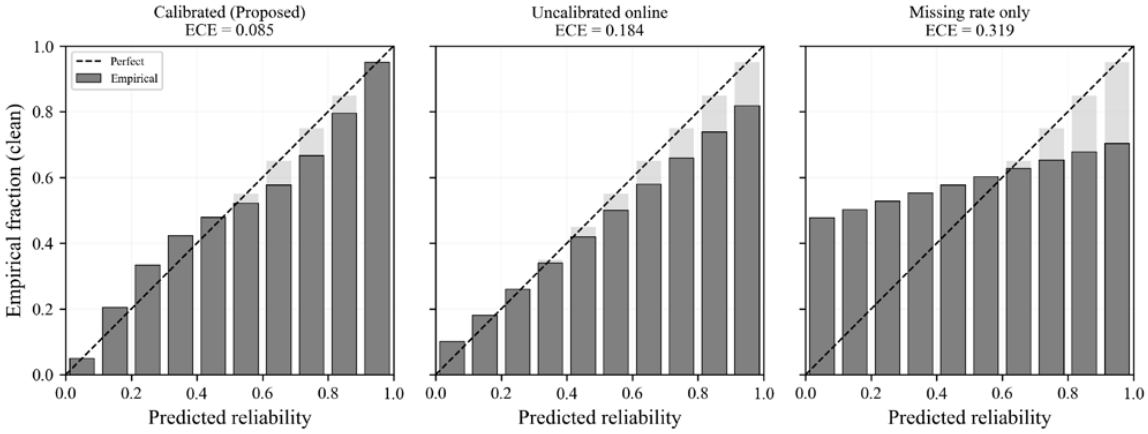

Рис. 2. Діаграми надійності (reliability diagrams) для каліброваного, некаліброваного й одноознакового варіантів

Калібрування ізотонічною регресією. Нехай s_i – некалібрований скор (або логіт / скалярний скор) для i-го прикладу, а $z_i \in \{0,1\}$ – мітка «недеградовано / деградовано» для цього прикладу в калібрувальному вікні. Ізотонічна регресія будує монотонне відображення $g(\cdot)$, що мінімізує квадратичну помилку за умов монотонності:

$$g^* = \arg\min_{g \in \mathcal{G}} \sum_{i=1}^{n} \left(z_i - g(s_i)\right)^2 \text{ за умови, що } g \text{ є неспадною}, \quad (2)$$

де $\mathcal{G}$ – клас монотонних (неспадних) функцій [13; 14]. Побудоване g^* застосовується до скорів у потоці, формуючи калібровану оцінку надійності $r_t = g^*(s_t)$. З погляду керування це означає, що шкала r_t узгоджена з емпіричною частотою недеградованих станів у калібрувальних умовах, а монотонність гарантує відсутність «перевертання» порядку: більш «поганий» скор не може перетворитися на вищу ймовірність.

У потоковому застосуванні ізотонічне калібрування є привабливим тим, що (i) не потребує перевизначення базової моделі та може виконуватися поверх довільних скорів; (ii) не вимагає параметричного припущення щодо форми перетворення; (iii) узгоджується з інтуїцією проксі-ознак деградації, де порівняльний порядок часто надійніший за абсолютну шкалу. Разом із тим, як і будь-яке калібрування, ізотонічна регресія залежить від репрезентативності калібрувального сегмента та потребує моніторингу під час експлуатації.

Загальну схему конвеєра онлайн-оцінювання надійності наведено на рис. 3.

Калібрована надійність як керувальний інтерфейс у потоковій системі підтримки прийняття рішень. Практична мотивація введення $r_t^{(m)}$ полягає не в самій по собі діагностиці, а в тому, що шкала повинна бути придатною для перетворення на дискретні дії, які мають чітку експлуатаційну інтерпретацію. У потокових конвеєрах типові керувальні дії можна умовно поділити на три групи. Перша група – *реакції на деградацію даних*: пригнічення або відключення проблемного каналу, перехід до більш надійної модальності, сигнал оператору про потребу перевірки сенсора. Друга група – *реакції на нестаціонарність середовища*: запуск обмеженої за бюджетом адаптації, зміна параметрів згладжування або порогів сигналізації, період «охолодження» після

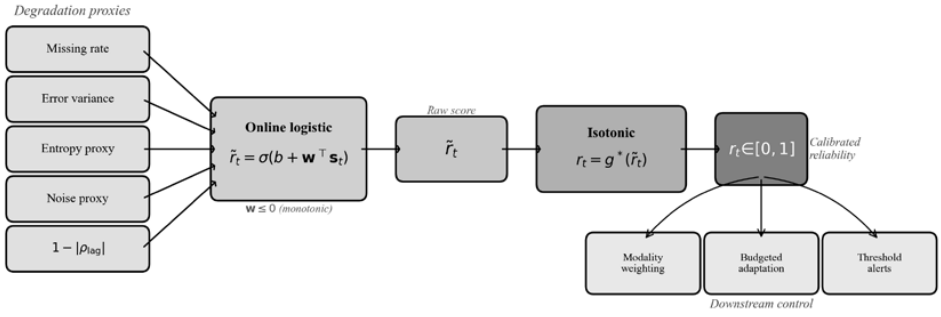

Рис. 3. Схема конвеєра онлайн-оцінювання надійності

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

адаптації. Третя група – *реакції на ризики аномалій*: керування режимом скорингу та порогами за фіксованого бюджету хибних тривог. У всіх цих випадках ключовою умовою є те, що пороги повинні мати стабільний смисл, і саме тому каліброваність шкали є системоутворювальною вимогою.

Калібрована ймовірнісна інтерпретація $r_t^{(m)}$ дає можливість задавати правила керування, прив’язані до зрозумілих інваріантів. Наприклад, поріг $r_t^{(m)} \geq 0{,}9$ може інтерпретуватися як «модальність вважається надійною з імовірністю не нижче за 0,9», а поріг $r_t^{(m)} < 0{,}5$ – як «переважно деградований режим», що допускає перехід до консервативної політики. Без калібрування схожі правила перетворюються на евристику, яка може працювати на одному запуску та руйнуватися на іншому через дрейф шкали або зміни розподілу проксі-ознак.

Режими доступності міток деградації та експлуатаційний моніторинг. Практична реалізація калібрування залежить від того, чи доступні мітки деградації z_t під час роботи системи. У контрольованих експериментах або стендових тестах мітки можуть бути сформовані детерміновано (через ін’єкції деградацій), що дає змогу калібрувати шкалу й оцінювати ECE без додаткових припущень. У реальних системах підтримки прийняття рішень мітки можуть бути частковими (наприклад, за сервісними подіями сенсорів, ручною верифікацією оператора або післядією технічних інцидентів) або взагалі недоступними. У цих умовах ключовим стає експлуатаційний моніторинг: відстеження стабільності розподілу r_t, контроль частоти переходів між режимами, аналіз кореляції з відомими інцидентами, а також періодична повторна калібровка на сегментах, де мітки можна отримати. Саме поєднання «калібрування + моніторинг» робить шкалу відтворюваним інтерфейсом керування, а не одноразово налаштованим скором.

Порівняння латентності (середньої та p99) для різних варіантів оцінювання надійності наведено на рис. 4.

Часові бюджети та мікробенчмарк. У потоковому режимі обчислювальні витрати модуля надійності повинні бути співмірні з витратами основного предиктора і не повинні створювати «вузьке місце» в конвеєрі. Тому оцінювання латентності розглядається як обов’язкова складова валідації: навіть помірне збільшення затримки на крок може акумулюватися на довгих горизонтах і порушувати вимоги до оновлення рішень. Наведені в табл. 2 значення демонструють характерну картину компромісу: прості проксі-шкали є значно швидшими, тоді як повна онлайн-модель забезпечує більш інформативну та калібровану шкалу за середньої латентності близько $150\mu s$. Для практики важливо, що обидва режими перебувають у мікросекундному діапазоні, а отже, можуть бути інтегровані в потокові конвеєри без радикальної перебудови архітектури.

Результати аблаційного аналізу, що відображають внесок окремих проксі-ознак, наведено на рис. 5.

Прості проксі-шкали привабливі мінімальними витратами, однак їхня прикладна корисність часто обмежується вузьким класом деградацій. Наприклад, частка пропусків безпосередньо сигналізує про втрату даних, але може не реагувати на шумові деградації або масштабні зсуви; статистики похибки можуть бути чутливими до деградації, але потребують доступності фактичної цілі y_t та можуть бути конфундовані з дрейфом задачі. Тому практичний компроміс полягає в комбінуванні кількох легких сигналів і в перетворенні сумарного скору в калібровану шкалу. Калібрування в цьому контексті виконує роль «нормалізатора смислу»: воно робить пороги та правила керування відтворюваними і зменшує ризик, що та сама числова межа означатиме різні рівні ризику на різних сегментах потоку.

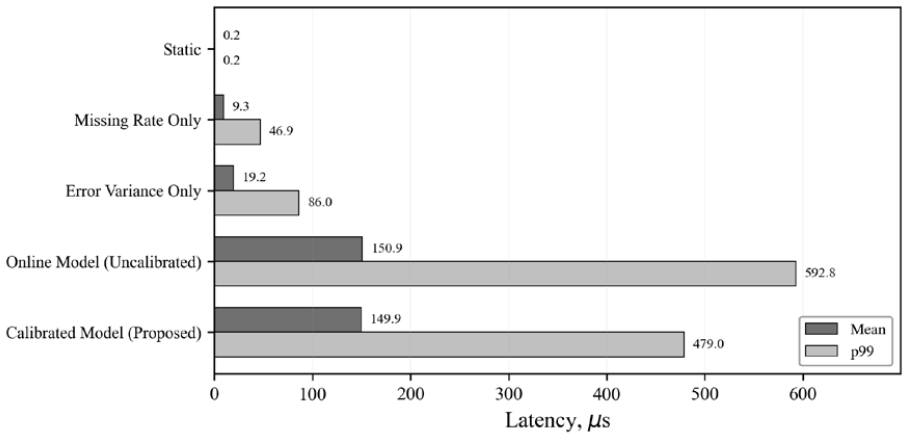

Рис. 4. Порівняння латентності (середня та p99) для різних варіантів оцінювання надійності

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

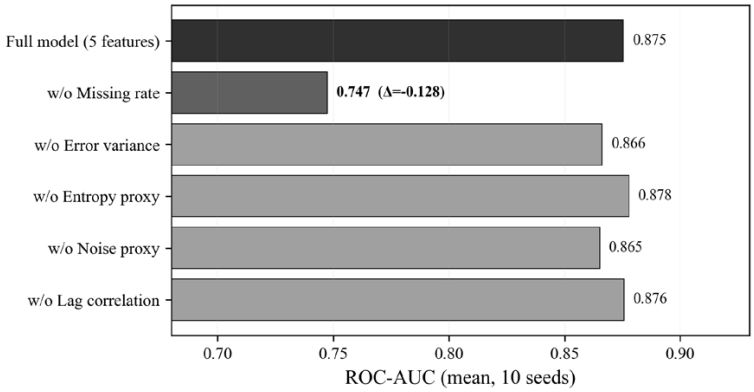

Рис. 5. Вплив окремих проксі-ознак на якість оцінювання надійності (аблаційний аналіз)

Калібрувальний сегмент та оновлення відображення. Ізотонічна регресія, як і будь-який калібратор, потребує вибору калібрувального сегмента, у якому скор s_t та мітки z_t є репрезентативними щодо очікуваних експлуатаційних умов. У лабораторному сценарії таким сегментом може бути контрольований потік із детермінованими ін’єкціями деградацій; у виробничому – відрізки, підтверджені сервісними подіями сенсорів або ручною верифікацією. У випадку зміни домену або механізмів деградації потрібне повторне калібрування або розширення калібрувального набору. Практичний підхід полягає в тому, щоб розглядати калібрування як частину експлуатаційного циклу: збір нових прикладів, перевірка узгодженості (за ECE на доступних мічених сегментах) та оновлення g^* за потреби.

Рекомендації щодо впровадження в потоковий конвеєр. Для перенесення запропонованого підходу в прикладну систему підтримки прийняття рішень доцільно дотримуватися такого мінімального регламенту:

1) визначити прикладне поняття «деградованого стану» для кожного джерела та перелік типових деградацій (пропуски, шум, зсуви);

2) вибрати набір легких проксі-сигналів, які каузально обчислюються в потоці та відображають ці деградації;

3) сформувати калібрувальний сегмент із мітками деградації (контрольований тест, журнал інцидентів, ручна розмітка) і побудувати ізотонічне відображення;

4) визначити пороги керування на каліброваній шкалі r_t та правила моніторингу (частота перемикань, частка часу в «ненадійному» режимі);

5) періодично перевіряти узгодженість шкали на доступних мічених сегментах і оновлювати калібрування в разі зсуву умов.

Зазначений регламент не є складним з інженерного погляду, але суттєво підвищує аудитованість і стійкість рішень у потоці.

Експериментальні показники якості та латентності. Табл. 1 і табл. 2 узагальнюють ключові метрики якості та часові характеристики запропонованого підходу.

Табл. 1. Узагальнення якості оцінювання надійності за ROC-AUC та ECE

Варіант	ROC-AUC	ECE
Онлайн-модель із калібруванням (ізотонічна регресія)	$0{,}86 \pm 0{,}07$	$0{,}08 \pm 0{,}04$
Онлайн-модель без калібрування	–	$0{,}18 \pm 0{,}07$
Проста шкала-проксі (лише пропуски або лише варіативність похибки)	–	–

Табл. 2. Мікробенчмарк латентності оцінювання надійності, μs

Процедура/варіант	Середня латентність, μs
Проста шкала-проксі: лише пропуски	9,29
Проста шкала-проксі: лише варіативність похибки	19,19
Онлайн-модель оцінювання надійності (повний варіант)	≈ 150

Обговорення результатів

Наведені результати підтверджують, що в потоковому сценарії корисність шкали надійності визначається двома взаємопов’язаними властивостями: (і) здатністю відокремлювати деградаційні стани та (іі) каліброваністю ймовірнісної інтерпретації. Висока ROC-AUC означає, що скор придатний для ранжування сегментів за рівнем деградації, тоді як низька ECE робить можливим використання числових порогів без повторної «підгонки» під кожен окремий

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

запуск. Саме каліброваність є тим компонентом, який перетворює скор з діагностичного індикатора на керувальний інтерфейс, придатний для аудитованих політик.

У частині часових характеристик принциповим є те, що метод зберігає мікросекундний порядок затримок. Прості проксі-шкали є швидшими, але повна онлайн-модель демонструє вищу якість за середньої латентності близько $150\mu s$, що є сумісним із практичними потоковими конвеєрами, де обробка виконується покроково або в малих вікнах. Таким чином, калібрування може розглядатися як «дешева» надбудова, що додає інтерпретованість без радикального збільшення витрат.

Разом із тим межі застосовності визначаються природою проксі-сигналів. Проксі-ознаки деградації не гарантують однаково якісного розділення «надійна / ненадійна» в усіх доменах і для всіх типів деградацій, а компоненти, що використовують статистики похибки, припускають доступність фактичного значення цілі y_t у потоці з допустимою затримкою. У сценаріях із відкладеною розміткою для підтримання коректності оцінювання можуть знадобитися альтернативні проксі або затримані оновлення калібрування. З практичного погляду ці обмеження означають, що модуль надійності потребує експлуатаційного моніторингу та періодичної перевірки узгодженості шкали з реальними подіями деградації, щоб зберігати аудитованість політик керування.

З позиції внутрішньої валідності важливо враховувати, що проксі-сигнали можуть реагувати не лише на деградацію джерела, а й на зміни розподілу даних, викликані концептуальним дрейфом або зміною режиму системи. Це створює потенційну конфундацію «дрейф $\leftrightarrow$ деградація», яку в практиці слід зменшувати через спільний аналіз декількох сигналів і через експлуатаційні контексти (журнали інцидентів, сервісні події, інформація про технічний стан сенсора). З позиції конструктивної валідності є мірою ранжування і не гарантує оптимальності конкретного порога, тоді як ECE залежить від вибору бінування та від репрезентативності калібрувального сегмента. Тому метрики мають інтерпретуватися як взаємодоповнювальні, а не як взаємозамінні.

З позиції зовнішньої валідності ROC-AUC переносимість проксі-сигналів і калібрування між доменами не є автоматичною. Шкала, калібрована на одному типі деградацій або на одному домені, може втратити узгодженість на іншому через інші механізми пропусків або інші шумові характеристики. Отже, у практичній системі підтримки прийняття рішень модуль надійності слід розглядати як компонент, що потребує періодичної верифікації та (за наявності міток) повторного калібрування.

Висновки

У статті представлено підхід до онлайн-оцінювання надійності модальностей і джерел у потоковому аналізі мультимодальних часових рядів із калібруванням ізотонічною регресією. Калібрований варіант демонструє високу здатність відокремлювати деградовані стани (ROC-AUC $0,86 \pm 0,07$) та суттєво покращує каліброваність шкали ($0,08 \pm 0,04$ проти $0,18 \pm 0,07$ без калібрування) за середньої латентності близько $150\mu s$. Отриманий підхід формує інтерпретований керувальний сигнал, який може бути використаний для стабільного керування компонентами потокової системи підтримки прийняття рішень за деградації модальностей та змінності середовища.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Дані будуть надані за обґрунтованим запитом.

Подяка

Автори висловлюють щиру подяку рецензентам і редколегії за уважний розгляд рукопису, цінні зауваження й рекомендації.

ЛІТЕРАТУРА

[1] T. Baltrušaitis, C. Ahuja, L.-P. Morency, “Multimodal machine learning: A survey and taxonomy,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 2, pp. 423–443, 2019. DOI: 10.1109/TPAMI.2018.2798607.

[2] D. Lahat, T. Adali, C. Jutten, “Multimodal data fusion: an overview of methods, challenges, and prospects,” Proceedings of the IEEE, vol. 103, no. 9, pp. 1449–1477, 2015. DOI: 10.1109/JPROC.2015.2460697.

[3] P. Dawid, “Present position and potential developments: Some personal views: Statistical theory: the prequential approach,” Journal of the Royal Statistical Society. Series A (General), vol. 147, no. 2, pp. 278–292, 1984. DOI: 10.2307/2981683.

[4] A. Bifet, J. Montiel, J. Read et al., Machine Learning for Data Streams with Practical Examples in MOA, MIT Press, 2018.

[5] J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, A. Bouchachia, “A survey on concept drift adaptation,” ACM Computing Surveys, vol. 46, no. 4, Art. 44, 2014. DOI: 10.1145/2523813.

[6] J. Lu, A. Liu, F. Dong, F. Gu, J. Gama, G. Zhang, “Learning under concept drift: A review,” IEEE Transactions on Knowledge and Data Engineering,

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359293

vol. 31, no. 12, pp. 2346–2363, 2019. DOI: 10.1109/TKDE.2018.2876857.

[7] R. S. M. Barros, S. G. T. C. Santos, “An overview and comprehensive comparison of ensembles for concept drift,” Information Fusion, vol. 52, pp. 213–244, 2019. DOI: 10.1016/j.inffus.2019.03.006.

[8] A. Kendall, Y. Gal, “What uncertainties do we need in Bayesian deep learning for computer vision?,” Advances in Neural Information Processing Systems, 2017. arXiv:1703.04977.

[9] Y. Ovadia, E. Fertig, J. Ren et al., “Can you trust your model’s uncertainty? Evaluating predictive uncertainty under dataset shift,” Advances in Neural Information Processing Systems, 2019. arXiv:1906.02530.

[10] E. Hüllermeier, W. Waegeman, “Aleatoric and epistemic uncertainty in machine learning: An introduction to concepts and methods,” Machine Learning, vol. 110, pp. 457–506, 2021. DOI: 10.1007/s10994-021-05946-3.

[11] C. Guo, G. Pleiss, Y. Sun, K. Q. Weinberger, “On calibration of modern neural networks,” in Proc. 34th International Conference on Machine Learning (ICML), 2017, pp. 1321–1330.

[12] J. C. Platt, “Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods,” in Advances in Large Margin Classifiers, A. J. Smola et al., Eds. MIT Press, 1999, pp. 61–74.

[13] B. Zadrozny, C. Elkan, “Transforming classifier scores into accurate multiclass probability estimates,” in Proc. 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002, pp. 694–699. DOI: 10.1145/775047.775151.

[14] A. Niculescu-Mizil, R. Caruana, “Predicting good probabilities with supervised learning,” in Proc. 22nd International Conference on Machine Learning (ICML), 2005, pp. 625–632. DOI: 10.1145/1102351.1102430.

[15] M. Kull, T. M. Silva Filho, P. Flach, “Beta calibration: a well-founded and easily implemented improvement on logistic calibration for binary classifiers,” in Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017, pp. 623–631.

[16] J. Vaicenavicius, D. Widmann, C. Andersson et al., “Evaluating model calibration in classification,” in Proc. 22nd International Conference on Artificial Intelligence and Statistics (AISTATS), 2019, pp. 3459–3467.

[17] T. Fawcett, “An introduction to ROC analysis,” Pattern Recognition Letters, vol. 27, no. 8, pp. 861–874, 2006. DOI: 10.1016/j.patrec.2005.10.010.

ONLINE RELIABILITY ESTIMATION OF SOURCES IN STREAMING ANALYSIS OF MULTIMODAL TIME SERIES WITH ISOTONIC REGRESSION CALIBRATION

Illia Uzun, Mykhaylo Lobachev

Streaming intelligent decision support systems processing multimodal time series operate under causality constraints and must satisfy requirements of low latency, bounded computational budgets, and controllable responses to environmental change. A critical practical risk in such pipelines is the temporary degradation of individual sources (missing values, elevated noise, scale shifts), which can masquerade as concept drift and trigger unstable or excessive control actions. This paper considers online estimation of source reliability as a causal probabilistic assessment of being in a non-degraded state and shows that practical control requires a calibrated scale: the output value must be interpretable as the frequency of the “non-degraded” regime under relevant conditions. The proposed approach combines lightweight degradation proxy signals suitable for online computation with isotonic regression calibration, which provides a monotone mapping from scores to correct probabilities. Key experimental results demonstrate ROC-AUC of 0.86 ± 0.07 *for the calibrated variant and calibration improvement from ECE of* 0.18 ± 0.07 *(uncalibrated) to ECE of* 0.08 ± 0.04 *(calibrated) at acceptable time costs: simple proxy scales have microsecond latencies, while the full online model maintains mean latency of approximately* $150\mu s$ *, meeting the needs of streaming pipelines.*

Keywords: *machine learning, data analysis, information systems, decision support systems, multimodal time series, online calibration, isotonic regression, degradation detection, reliability estimation, streaming data.*

REFERENCES

[1] T. Baltrušaitis, C. Ahuja, L.-P. Morency, “Multimodal machine learning: A survey and taxonomy,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 2, pp. 423–443, 2019. DOI: 10.1109/TPAMI.2018.2798607.

[2] D. Lahat, T. Adali, C. Jutten, “Multimodal data fusion: an overview of methods, challenges, and prospects,” Proceedings of the IEEE, vol. 103, no. 9, pp. 1449–1477, 2015. DOI: 10.1109/JPROC.2015.2460697.

[3] P. Dawid, “Present position and potential developments: Some personal views: Statistical theory: the prequential approach,” Journal of the Royal Statistical Society. Series A (General), vol. 147, no. 2, pp. 278–292, 1984. DOI: 10.2307/2981683.

[4] A. Bifet, J. Montiel, J. Read et al., Machine Learning for Data Streams with Practical Examples in MOA, MIT Press, 2018.

[5] J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, A. Bouchachia, “A survey on concept drift adaptation,” ACM Computing Surveys, vol. 46, no. 4, Art. 44, 2014. DOI: 10.1145/2523813.

[6] J. Lu, A. Liu, F. Dong, F. Gu, J. Gama, G. Zhang, “Learning under concept drift: A review,” IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 12, pp. 2346–2363, 2019. DOI: 10.1109/TKDE.2018.2876857.

[7] R. S. M. Barros, S. G. T. C. Santos, “An overview and comprehensive comparison of ensembles for concept

ISSN 2786-9024

drift,” Information Fusion, vol. 52, pp. 213–244, 2019. DOI: 10.1016/j.inffus.2019.03.006.
[8] A. Kendall, Y. Gal, “What uncertainties do we need in Bayesian deep learning for computer vision?,” Advances in Neural Information Processing Systems, 2017. arXiv:1703.04977.
[9] Y. Ovadia, E. Fertig, J. Ren et al., “Can you trust your model’s uncertainty? Evaluating predictive uncertainty under dataset shift,” Advances in Neural Information Processing Systems, 2019. arXiv:1906.02530.
[10] E. Hüllermeier, W. Waegeman, “Aleatoric and epistemic uncertainty in machine learning: An introduction to concepts and methods,” Machine Learning, vol. 110, pp. 457–506, 2021. DOI: 10.1007/s10994-021-05946-3.
[11] C. Guo, G. Pleiss, Y. Sun, K. Q. Weinberger, “On calibration of modern neural networks,” in Proc. 34th International Conference on Machine Learning (ICML), 2017, pp. 1321–1330.
[12] J. C. Platt, “Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods,” in Advances in Large Margin Classifiers, A. J. Smola et al., Eds. MIT Press, 1999, pp. 61–74.
[13] B. Zadrozny, C. Elkan, “Transforming classifier scores into accurate multiclass probability estimates,” in Proc. 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002, pp. 694–699. DOI: 10.1145/775047.775151.
[14] A. Niculescu-Mizil, R. Caruana, “Predicting good probabilities with supervised learning,” in Proc. 22nd International Conference on Machine Learning (ICML), 2005, pp. 625–632. DOI: 10.1145/1102351.1102430.
[15] M. Kull, T. M. Silva Filho, P. Flach, “Beta calibration: a well-founded and easily implemented improvement on logistic calibration for binary classifiers,” in Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017, pp. 623–631.
[16] J. Vaicenavicius, D. Widmann, C. Andersson et al., “Evaluating model calibration in classification,” in Proc. 22nd International Conference on Artificial Intelligence and Statistics (AISTATS), 2019, pp. 3459–3467.
[17] T. Fawcett, “An introduction to ROC analysis,” Pattern Recognition Letters, vol. 27, no. 8, pp. 861–874, 2006. DOI: 10.1016/j.patrec.2005.10.010.

Дата першого надходження статті до видання: 12.02.2026
Дата прийняття статті до друку після рецензування: 17.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

УДК 004.312.2

ВИСОКОЕФЕКТИВНІ ФОРМАЛІЗОВАНІ МОДЕЛІ ОБЧИСЛЮВАЧІВ ДЛЯ ВІДТВОРЕННЯ ТРАНСЦЕНДЕНТНИХ ФУНКЦІЙ ЗА НЕТРАДИЦІЙНОЇ ПОСТАНОВКИ ЗАВДАННЯ

В.А. Лукашенко[1], А.В. Бернацький[1], Ю.В. Юрченко[1], О.В. Сіора[1], В.М. Лукашенко[2], Д.А. Гардер[1]
[1] Department of Specialized High-Voltage Equipment and Laser Welding, E.O. Paton Electric Welding Institute of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[2] Department of Robotics and Specialized Computer Systems, Cherkasy State Technological University, Cherkasy, Ukraine
ORCID https://orcid.org/0000-0002-9685-4654
ORCID https://orcid.org/0000-0002-8050-5580
ORCID https://orcid.org/0000-0001-9253-009X
ORCID https://orcid.org/0009-0005-8542-1633
ORCID https://orcid.org/0009-0006-7459-4704
ORCID https://orcid.org/0000-0002-4066-8182
E-mail: yuriyyurchenko14@gmail.com

АНОТАЦІЯ

Роботу присвячено створенню та дослідженню високоефективних формалізованих моделей прецизійних обчислювачів спеціального призначення для розв’язання нетрадиційних постановок завдань, обумовлених відсутністю аналітичних відношень між значенням трансцендентних функцій та відповідного значення порядкового номера решітки в комп’ютерно-інтегрованих системах керування на базі таблично-алгоритмічних методів. Застосування спеціалізованих прецизійних обчислювальних пристроїв є необхідним для управління об’єктами та швидкодіючими процесами в реальному часі, де використання мікропроцесорів загального призначення, навіть зі спеціальними програмними засобами, неможливе у зв’язку з високими вимогами одночасно до швидкодії, надійності, габаритів, енергоспоживання, ступеня готовності й апаратурних витрат (вартості). Особливо актуальною є задача апаратної реалізації багаторозрядних обчислювачів спеціального призначення для відтворення з високою точністю базових математичних і трансцендентних функцій за умов обмежених енергочасових ресурсів у єдиного кристала. З огляду на це перспективним напрямом є застосування формалізованих таблично-алгоритмічних методів, які дають можливість оптимізувати структуру обчислювачів спеціального призначення без погіршення точності відтворення функцій. Метою роботи є створення моделі прецизійного обчислювача спеціального призначення, що забезпечує високу ефективність у відтворенні значень у двійковій системі числення трансцендентних функцій відносно порядкового номера решітки шляхом використання формалізованого табличного логіко-оборотного методу перетворення вхідної кодової множини у вихідну за допомогою корегувальних констант. У роботі проведено верифікацію ефективності формалізованих таблично-алгоритмічних моделей прецизійних обчислювачів спеціального призначення, реалізованих формалізованим табличним логіко-оборотним методом. Отримані результати порівнювалися з класичним табличним методом апаратурної реалізації за сукупністю ключових показників, а саме: потужністю споживання, часовими затратами на відтворення функцій та апаратурними витратами (вартістю) в межах єдиного кристала. Запропоновано оригінальну формалізовану модель прецизійного обчислювача спеціалізованого призначення, яка відтворює значення трансцендентної функції від відповідного порядкового номера решітки з меншими енергетичними, часовими й апаратурними витратами, що адекватно забезпечує підвищення ефективності комп’ютерно-інтегрованих систем у галузях аеронавігації, оборонної, космічної промисловості.

Ключові слова: *прецизійні обчислювачі, таблично-алгоритмічні методи, енергоспоживання, апаратурні витрати, формалізований таблично-логічний метод, логіко-оборотний метод.*

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

Вступ

Для вирішення ряду технічних задач у промисловості, галузях аеронавігації, космонавтики, керування спеціалізованими автономними фізичними об’єктами потрібно використовувати обчислювачі для різних математичних функцій. На цей час застосування спеціалізованих обчислювальних пристроїв є необхідним для управління об’єктами та процесами реального часу, де використання мікропроцесорів загального призначення, навіть зі спеціальними програмними засобами, неможливе у зв’язку з високими вимогами одночасно до швидкодії, надійності, габаритів, енергоспоживання, ступеня готовності та вартості. Зазвичай ця задача вирішується за допомогою арифметико-логічних пристроїв, однак більш ефективним, особливо в умовах обмеженого часу, для відтворення значень трансцендентних функцій є застосування табличних обчислювачів. Традиційні табличні методи реалізації функцій на основі ROM або LUT забезпечують простоту реалізації та детермінований час обчислення, однак із зростанням розрядності аргументів та кількості відтворюваних функцій призводять до суттєвого збільшення обсягу пам’яті й енергоспоживання. Саме тому в останні роки активно розвиваються таблично-алгоритмічні методи на базі апаратної апроксимації функцій, зокрема кусково-лінійні та кусково-поліноміальні підходи, гібридні LUT-алгоритми, а також модифіковані CORDIC-архітектури [1–3]. Сучасні таблично-алгоритмічні методи значно зменшують обсяг таблиць завдяки використанню тривалих арифметичних операцій, що неприпустимо для швидкодіючих комп’ютерно-інтегрованих систем (ШКІС) спеціального призначення. У роботах [4–6] запропоновано адаптивні методи сегментації області аргументу та зменшення кількості опорних точок, що дає змогу скоротити апаратурні витрати за збереження допустимої похибки. Разом із тим такі підходи часто ускладнюють логічну структуру обчислювача та збільшують затримки сигналів.

Дослідження [7–9] спрямовані на зниження енергоспоживання шляхом оптимізації квантування й ущільнення таблиць відповідностей, однак більшість із них орієнтовані на відтворення однієї функції і не враховують багатофункціональний режим роботи.

Окремий напрям досліджень пов’язаний із розробкою універсальних та реконфігурованих архітектур, здатних відтворювати декілька функцій у межах одного апаратного ядра [1; 2; 10]. Такі рішення є перспективними з погляду зменшення апаратурних витрат, проте потребують формалізованих методів побудови та верифікації ефективності.

У зв’язку з наведеним актуальною є задача створення та дослідження високоефективних моделей обчислювачів трансцендентних функцій, побудованих формалізованими табличними логіко-оборотними методами, які забезпечують одночасно високі показники щодо швидкодії, надійності, габаритів, енергоспоживання, ступеня готовності та вартості.

Аналіз літературних джерел і постановка проблеми

Питання апаратної реалізації трансцендентних і спеціальних функцій у цифрових обчислювальних системах активно досліджується в науковій літературі протягом останнього десятиліття. Основна увага зосереджена на зменшенні апаратурних витрат і енергоспоживання за збереження необхідної точності та швидкодії.

У роботах [1; 2] запропоновано реконфігуровані апаратні архітектури для відтворення набору трансцендентних функцій, що дає можливість використовувати спільні апаратні ресурси для різних обчислювальних задач. Показано, що такий підхід зменшує площу кристала, проте потребує складної логіки керування та додаткових витрат часу на перемикання режимів.

У дослідженнях [3; 7] розглянуто кусково-поліноміальні та квантувально-орієнтовані методи апроксимації, які дають змогу суттєво зменшити обсяг пам’яті LUT. Отримані результати демонструють високу точність, однак зі зростанням кількості сегментів ускладнюється апаратна реалізація та збільшується затримка обчислень. Роботи [4; 5] присвячені адаптивній сегментації області аргументу й оптимізації структури обчислювачів, що забезпечує компроміс між точністю та апаратурними витратами. Водночас такі методи переважно орієнтовані на реалізацію окремих функцій і не розглядають можливості їх одночасного відтворення в межах єдиного обчислювального ядра.

У публікаціях [8–10] досліджуються енергоефективні архітектури для реалізації тригонометричних та гіперболічних функцій, у тому числі на базі CORDIC-алгоритмів та їх модифікацій. Хоча ці підходи допомагають знизити енергоспоживання, вони характеризуються обмеженою гнучкістю та складністю масштабування в разі збільшення кількості функцій. Аналіз літературних джерел показує, що більшість існуючих рішень або орієнтовані на реалізацію однієї функції, або потребують значних апаратурних і часових затрат за багатофункціонального використання. Крім того, недостатньо уваги приділяється формалізованим методам порівняльної верифікації ефективності запропонованих архітектур за сукупністю показників енергоспоживання, швидкодії та апаратурної складності.

У зв’язку із цим у цьому дослідженні розв’язуються такі основні завдання:

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

– провести аналіз сучасного стану таблично-алгоритмічних методів апаратурної реалізації і моделей прецизійних обчислювачів спеціального призначення та визначити напрям вирішення проблемних завдань з акцентом на зменшення енергоспоживання, часових витрат на обробку інформації та апаратурних витрат (вартості);

– створити та дослідити прецизійну модель обчислювача спеціального призначення, що відтворює трансцендентну функцію відносно порядкового номера решітки;

– визначити метод верифікації ефективності розробленої моделі обчислювача спеціального призначення за показниками, що характеризують енергоспоживання, швидкодію через часові затрати на обробку інформації та апаратурні витрати (вартість).

Методи досліджень

У роботі методи досліджень базуються на використанні апарата обчислювальної математики, властивостей математичної логіки та тотожності алгебри Жегалкіна. Застосовано комплекс аналітичних і формалізованих методів дослідження, спрямованих на оцінювання ефективності моделей прецизійних обчислювачів спеціального призначення за показниками, що характеризують енергоспоживання, швидкодію через часові затрати на обробку інформації та апаратурні витрати (вартість).

Результати дослідження

Однією з трансцендентних функцій апаратурної реалізації компонентів для комп'ютерно-інтегрованих систем спеціального призначення є функція

$$f(x_j) = sc(x_j) - sc(0),$$

тому для спрощення процедури формування й дослідження трансцендентної моделі обчислювача спеціального призначення дослідження проводитимемо на прикладі цієї функції. Створена модель обчислювача спеціального призначення забезпечує високу ефективність у відтворенні значень у двійковій системі числення трансцендентних функцій шляхом перетворення вхідної кодової інформації «J» у вихідну «$f(x_j)$» за допомогою визначених корегувальних констант «Δ» і тісно пов'язана з логіко-математичною моделлю, в основі якої є використання логічної операції XOR. Формалізована логіко-математична модель формування значення трансцендентної функції «$f(x_j)$» має такий вигляд

$$f(x) = J \oplus \Delta, \qquad (1)$$

враховуючи тотожність логічної операції XOR, корегувальну константу Δ визначаємо за формулою (1) таким чином

$$\Delta = f(xj) \oplus J. \qquad (2)$$

Значення Δ складають таблицю, значення якої за апаратурної реалізації формує обсяг числового блока пам'яті (ЧБП).

Особливість обчислювачів спеціального призначення полягає у тому, що значення кодів вхідних, вихідних та корегувальних констант створюються заздалегідь, це забезпечує незалежність часу отримання остаточного результату розрахунків від складності обчислень значень відтворюваної функції.

Тож під час проєктування на основі властивостей математичної логіки й алгебри Жегалкіна формується таблиця відповідностей (табл. 1), наведена нижче.

У табл. 1 кортежні коди номерів J і функції $f(x_j)$ та коди кортежів корегувальних констант $\Delta_{ст}$ та $\Delta_{мол}$ за відповідними доменами представлені в десятковій та двійковій системах числення.

Для наочності за результатами дослідження на рис. 1 побудовано модель гістограми, яка візуально показує кількість однакових значень корегувальних констант k та використовує відповідні кодові значення табл. 1.

За результатами аналізу наведеної моделі гістограми визначено, що для формування об'єму числового блока пам'яті потрібно значень корегувальних констант для кортежів старших розрядів – 4 шт.,

для кортежів молодших розрядів – 7 шт.

Загальна кількість кодових кортежів становить 11.

При цьому ефективність ущільнення інформації для числового блока пам'яті оцінюється за математичним виразом коефіцієнта ефективності та дорівнює:

$$E_L = L_{кл} / L_{тло} = 63/11 = 5{,}7.$$

Ефективну модель обчислювача спеціального призначення, що відтворює значення трансцендентні функції $f(x_j)$ формалізованим табличним логіко-оборотним методом, зображено на рис. 2.

Процедура формування значень трансцендентної функції розробленою моделлю (рис. 2) здійснюється таким чином. Вхідний код J, що записується в регістр Рг 1, під дією керуючих імпульсів МПА 8, що надходять на керуючі входи 4, 5 комбінаційних схем адрес, розпізнається комбінаційними схемами адрес 2 і 3. Вихідні імпульси відповідних адресів останніх надходять на відповідні входи ЧБП. 6 Під дією цих імпульсів зчитуються коди корегувальних констант $\Delta_{ст}$, $\Delta_{мол}$ які за допомогою зворотних зв'язків надходять на відповідні лічильні входи тригерів регістра 1. Одиниці корегувальних констант, що надійшли на лічильні входи відповідних тригерів регістра, змінюють стан цих тригерів на протилежний. На виході Рг 1 та на входах МДН-ключів 7 з'являється код значення трансцендентної функції f(x), якій з дозволу керуючого імпульсу МПА 8 проходить через відкрити МДН-ключі на його виходи. Останні всередині кристала з'єднані із шинами «Вхід / Вихід», цим зменшується

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

Табл. 1. Реляційна модель даних обчислювача трансцендентної функції, відношень порядкового номера решітки та корегувальних констант

№ = J, дес. код	Двійкові коди порядкового номера J	Код функції $f(x_j)$	Двійкові коди доменів кортежів корегувальних констант	Дес. код $\Delta_{ст}$	Дес. код $\Delta_{мол}$	J	Двійкові коди порядкового номера J	Код функції $f(x_j)$	Двійкові коди доменів кортежів корегувальних констант	Дес. код $\Delta_{ст}$	Дес. код $\Delta_{мол}$
			$\Delta_{ст}$ $\Delta_{мол}$						$\Delta_{ст}$ $\Delta_{мол}$		
0	000000	000000	000 000	0	0	32	100 000	011011	111 011	7	3
1	000 001	000000	000 001	0	1	33	100 001	011011	111 010	7	2
2	000 010	000001	000 011	0	3	34	100 010	011100	111 110	7	6
3	000 011	000010	000 001	0	1	35	100 011	011100	111 111	7	7
4	000 100	000011	000111	0	7	36	100 100	011101	111 001	7	1
5	000 101	000100	000 001	0	1	37	100 101	011110	111 011	7	3
6	000 110	000100	000010	0	2	38	100 110	011111	111 001	7	1
7	000 111	000101	000 010	0	2	39	100 111	100000	000 111	0	7
8	001 000	000110	001 110	1	6	40	101 000	100001	001 001	1	1
…	…	…	…	…	…	…	…	…	…	…	…
26	011 010	010101	001 111	1	7	58	111 010	110000	001 010	1	2
27	011 011	010110	001 001	1	1	59	111 011	110000	001 011	1	3
28	011 100	010111	001 011	1	3	60	111 100	110001	001 101	1	5
29	011 101	011000	000 101	0	5	61	111 101	110010	001 111	1	7
30	011 110	011000	000 110	3	6	62	111 110	110011	001 101	1	5

Примітки: $\Delta_{ст}$ – характеризує значення домену старшого кортежу; $\Delta_{мол}$ – характеризує значення домену молодшого кортежу.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

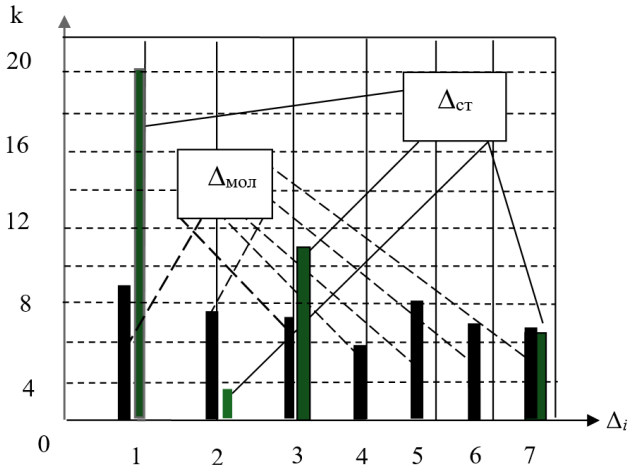

Рис. 1. Гістограми кількості *k* однакових значень Δ_i корегувальних констант для кортежів:
$\Delta_{ст}$, $\Delta_{мол}$ – старших, молодших розрядів відповідно

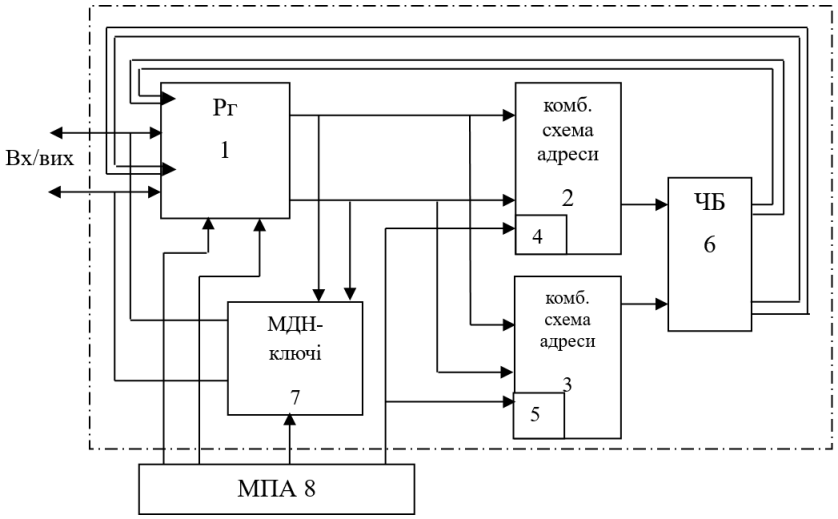

Рис. 2. Високоефективна модель прецизійного обчислювача спеціального призначення для відтворення трансцендентної функції:

1 – регістр Рг; 2, 3 – комбінаційні схеми адресів доменів корегувальних констант $\Delta_{ст}$, $\Delta_{мол}$ для визначення кодів старшого та молодшого кортежів відповідно; 4, 5 – керуючі входи комбінаційних схем адресів доменів для визначення кодів корегувальних констант $\Delta_{ст}$, $\Delta_{мол}$ старшого та молодшого кортежів відповідно; 6 – числовий блок пам’яті ЧБП; 7 – МДН-ключі; 8 – МПА (мікропрограмний автомат)

кількість внутрішніх і зовнішніх контактів, що підвищує надійність обчислювача.

Для дослідження та проведення верифікації створеної моделі обчислювача трансцендентної функції запропоновані математичні моделі оцінювання ефективності за основними параметрами: потужності споживання; витрати часу на отримання результату; апаратурні витрати (вартість), що наведено в табл. 2, 3, 4.

Верифікація ефективності створеної моделі обчислювача спеціального призначення за згаданими вище параметрами проводиться через порівняльний аналіз за високошвидкісним класичним табличним методом.

За результатами розрахунків (табл. 2) потужностей споживання показано, що модель обчислювача, яка відтворює трансцендентні функції формалізованим табличним логіко-оборотним методом, має

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

Табл. 2. Результати кількісного оцінювання за параметрами потужності споживання створеної формалізованої та табличної моделей обчислювачів спеціального призначення у процесі відтворення значень трансцендентної функції

Метод апаратурної реалізації	Модель обчислювача для відтворення значень відповідних функцій	Результати розрахунків потужності споживання
Табличний класичний	$f(x_j) = sc(x_j) - sc(0)$ від коду порядкового номера (J)	$P_{кл} = 2\,[2P_1 \cdot 6 + P_2(2^6 - 1) + P_4 \cdot 6(2^6 - 1)] =$ $= 2\,[2 \cdot 4P_2 6 + P_2(2^6 - 1) + P_2 6(2^6 - 1)] =$ $= 978\,P_2$
Формалізований табличний логіко-зворотний	функції $[f(x_j) = sc(x_j) - sc(0)]$ від коду порядкового номера (J)	$P_{бтло} = [P_1 n + 2 \cdot P_2(1/E_L) + P_3 +$ $+ P_4 m\,(n/m)(1/E_L) + P_5] =$ $= 1 \cdot [4P_2 6 + 2 \cdot P_2(1/5,7) + P_2 + P_2 6 \cdot (1/5,7) +$ $+ P_2] = 27,4\,P_2$

Примітки: P_1 – потужності споживання одного тригера регістра; P_2 – ланцюга видачі однієї адреси; P_3 – одного логічного елемента; P_4 – одного активного елемента числового блока пам’яті; P_5 – одного блока МДН-ключів; ß – кількість тригерів; w – кількість ланцюгів видачі однієї адреси; h – кількість логічних елементів; l – кількість елементів ЧБ; ζ – кількість кристалів для відтворення кількох функцій; Z – кількість регістрів на одному кристалі; ϒ – кількість блоків адреси на одному кристалі; η – кількість числових блоків пам’яті на одному кристалі; ν – кількість блоків МДН-ключів.

меншу потужність споживання порівняно з табличним класичним методом завдяки використанню одного регістра й одного числового блока пам’яті в

$$P_{кл}/P_{фтло} = 978\,P_2/27,4\,P_2 = 35,6 \text{ раза.}$$

Таким чином, верифікація ефективності розробленої моделі обчислювача підтверджується результатами розрахунків за параметром потужності споживання.

Отримані результати розрахунків часу відтворення, подані в табл. 3, показали, що затримка результатів у відтворенні трансцендентної функції збільшена через додатково введені логічні операції, тобто в

$$t_{ФТЛО} - t_{кл} = 22t_в / 2ot_в = 1,1 \text{ раза.}$$

Припустимо, що $a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = a_7 = a$, тоді за результатами розрахунків апаратних витрат, які наведені в табл. 4, їх величина зменшується у 29,6 раза, тобто

$$C_{кл}/C_{фтло} = 1002\,a_2/33,9\,a_2 = 29,6.$$

Таким чином, величина зменшення апаратурних затрат підтверджує ефективність запропонованої моделі обчислювача, що реалізує відтворення значень решітчастої функції $f(x_j) = sc(x_j) - sc(0)$ для відповідного двійкового коду порядкового номера (J) завдяки запропонованому формалізованому табличному логіко-оборотному методу.

На основі наведених результатів розрахунків потужності споживання та часу затрат на відтворення значень відповідних функцій доцільно визначити такі техніко-економічні коефіцієнти: K_E та K_C.

Коефіцієнт K_E – величина, що характеризує енергозбереження запропонованою моделлю обчислювача, яка реалізована формалізованим табличним

Табл. 3. Результати розрахунків часу відтворення значень трансцендентної функції моделлю обчислювачів спеціального призначення

Метод апаратурної реалізації	Модель обчислювача для відтворення значень відповідних функцій	Результати розрахунків часу відтворення функцій
Табличний класичний	трансцендентна функція $[f(x_j) = sc(x_j) - sc(0)]$ від коду порядкового номера (J)	$t_{кл} = 2 \cdot [Zt_{Рг} + \gamma t_в + ß \cdot t_{рг}] \approx$ $\approx 2 \cdot [2 \cdot 4t_в + \gamma t_в + ß \cdot t_{рг}] \approx 20\,t_в$
Формалізований табличний логіко-зворотний	трансцендентна функція $[f(x_j) = sc(x_j) - sc(0)]$ від коду порядкового номеру (J)	$t_{фтло} = 2 \cdot [Zt_{Рг} + \gamma t_в + \chi t_л + \nu t_{мдн} + ß \cdot t_{рг}] \approx$ $\approx 2 \cdot [1 \cdot 4 + 1 + 4 + 1 + 1] t_в \approx 22\,t_в$

Примітки: $t_в$ – час одноразової вибірки з ПЗП; $t_л \approx t_в$ – час однієї логічної операції; $t_п \approx t_в$ – час зміни стану тригера з одного в інший; $t_{Рг} \approx 4\,t_в$ – час затримки інформації в регістрі; $t_з \approx t_в$ – час формування конституанти одиниці однієї логічної операції; $t_{мдн} \approx t_в$ – *час затримки МДН-ключа.*

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

Табл. 4. Результати розрахунків апаратурних витрат на моделі обчислювачів спеціального призначення у процесі відтворення значень трансцендентної функції

Метод апаратурної реалізації	Модель обчислювача для відтворення значень відповідних цифрових кодів	Результати розрахунків апаратурних витрат (вартість) на відповідні моделі обчислювачів
Табличний класичний	$f(x_j) = sc(x_j) – sc(0)$ від коду порядкового номеру (J)	$C = \zeta\cdot[Z\cdot a_1 n + \Upsilon\cdot a_2(2^n – 1) + \eta\cdot a_4 n(2^n – 1) + \rho\cdot a_7] = 2\,[2a_1 6 + a_2(2^6 – 1) + a_4 6(2^6 – 1) + 12a_2] = 2\,a_2\,[2\cdot 4\cdot 6 + (2^6 – 1) + 6(2^6 – 1) + 12] = 2\,a_2\,[48 + 63 + 378 + 12] = 1002\,a_2$
Формалізований табличний логіко-оборотний	$f(x_j) = sc(x_j) – sc(0)$ від коду порядкового номеру (J)	$C = \zeta\cdot[Z\cdot a_1 n + \Upsilon\cdot a_2(1/E_L) + h a_3(2) + \eta\cdot a_4(n/m)(1/E_L) + \nu a_5 + \rho\cdot a_7] = 1\cdot[a_1 n + 2a_2(1/E_L) + a_3(2) + a_4 m(n/m)(1/E_L) + \nu a_5 + \rho\cdot a_7] = 1\cdot[4a_2 6 + 2\cdot 2a_2(1/5{,}7) + 2a_2 + a_4 6(1/5{,}7) + a_2 + 6a_2] = 33{,}9\,a_2$

Примітки: a_1 – затрати на один розряд регістра; a_2 – на один ланцюг видачі однієї адреси; a_3 – на один логічний елемент; a_4 – на один біт ЧБ пам’яті; a_5 – на МДН-ключі; a_6 – на один елемент затримки; a_7 – на один зовнішній контакт; ζ – кількість кристалів для відтворення кількох функцій, що реалізуються апаратно; φ – кількість елементів затримки; ρ – кількість зовнішніх контактів.

логіко-оборотнім методом відносно табличного класичного методу апаратурної реалізації моделі обчислювача трансцендентної функції.

Коефіцієнт K_E визначається за формулою (6):

$$K_E = E_{кл} / E_i \quad (6)$$

де $E_{кл} = P_{кл}\cdot t_{кл}$ – величина, що характеризує енергію споживання моделлю обчислювача, яка реалізована класичним табличним методом;

$E_i = P_i\cdot t_i$ – величина, що характеризує енергію споживання моделлю обчислювача, яка реалізована формалізованим табличним логіко-оборотним методом.

Коефіцієнт K_C – величина, яка характеризує зменшення апаратурних витрат у процесі створення моделі обчислювача, що реалізована формалізованим табличним логіко-оборотнім методом відносно табличного класичного методу для відтворення значень трансцендентної функції.

Коефіцієнт K_C визначається за формулою (7):

$$K_c = C_{кл} / C_i \quad (7)$$

де C_i – величина, яка характеризує апаратурні витрати на модель обчислювача, реалізованого формалізованим табличним логіко-оборотнім методом;

$C_{кл}$ – величина, яка характеризує апаратурні витрати на модель обчислювача реалізованого табличним класичним методом.

Результати розрахунків зведені в табл.5.

Отже, техніко-економічні показники підтверджують ефективність розробленої оригінальної моделі прецизійного обчислювача спеціального призначення, яка апаратно реалізована на базі формалізованого таблично-алгоритмічного методу.

Обговорення результатів

Отримані результати дослідження підтверджують доцільність застосування формалізованого табличного логіко-оборотного методу для побудови прецизійних обчислювачів спеціального призначення,

Табл. 5. Порівняльний аналіз показників енергозбереження та зменшення апаратурних затрат для запропонованих методів і моделей обчислювачів

Метод апаратурної реалізації	Модель обчислювачадля відтворення значень відповідних функцій	C_i,	$C_{кл}$,	K_C Скл / Сі	$E_{i,,}$	$E_{кл}$	K_E Екл / Еі
Формалізований табличний логіко-оборотний	решітчастої функції[$f(x_j)$ = sec(x_j) – sec(0)]від порядкового номера (J)	33,9	1002	29,56	602,8	19560	32,45

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

орієнтованих на відтворення трансцендентних функцій у комп’ютерно-інтегрованих системах керування.

На відміну від класичних табличних підходів, де підвищення розрядності або кількості функцій безпосередньо призводить до зростання обсягу пам’яті й енергоспоживання, запропонована модель забезпечує оптимізацію структури обчислювального процесу завдяки формалізації табличних залежностей і використання корегувальних констант.

Аналіз структури числового блока пам’яті показав, що істотне ущільнення інформації досягається завдяки повторюваності значень корегувальних констант у доменах старших і молодших кортежів. Це дає змогу реалізувати універсальне представлення функціональної залежності без необхідності зберігання повної таблиці відповідностей, що є ключовою перевагою запропонованого підходу. Внаслідок цього значно зменшуються апаратурні витрати та кількість активних елементів, що безпосередньо впливає на енергоефективність обчислювача.

Отримані оцінки енергоспоживання демонструють суттєву перевагу формалізованої моделі над класичним табличним методом, що пояснюється зменшенням обсягу пам’яті, скороченням кількості регістрів та зниженням інтенсивності внутрішніх перемикань. Водночас аналіз часових характеристик показав незначне збільшення затримки формування результату, зумовлене додатковими логічними операціями формалізованого перетворення. Однак така затримка має детермінований характер і не залежить від складності відтворюваної функції, що є принципово важливим для систем реального часу.

Важливою перевагою запропонованого підходу є його універсальність, оскільки та сама апаратна структура може бути використана для відтворення різних трансцендентних функцій шляхом заміни набору корегувальних констант без модифікації апаратної частини. Це створює передумови для побудови багатофункціональних спеціалізованих обчислювачів із високим рівнем адаптивності та масштабованості.

Результати дослідження свідчать, що формалізований табличний логіко-оборотний метод забезпечує ефективний компроміс між швидкодією, енергоспоживанням і апаратурними витратами та є перспективною основою для створення високоефективних прецизійних обчислювальних пристроїв спеціального призначення.

Висновки

Під час виконання дослідження отримано такі основні результати:

1. У роботі розв’язано актуальну науково-прикладну задачу створення високоефективних формалізованих моделей прецизійних обчислювачів спеціального призначення для відтворення трансцендентних функцій у комп’ютерно-інтегрованих системах керування за умов відсутності аналітичних залежностей між значенням функції та порядковим номером решітки.

2. Обґрунтовано доцільність використання формалізованих таблично-алгоритмічних методів для апаратної реалізації багаторозрядних обчислювачів спеціального призначення в системах реального часу із жорсткими обмеженнями щодо швидкодії, енергоспоживання, габаритів та вартості. Показано, що застосування універсальних мікропроцесорних засобів у таких умовах є неефективним.

3. Розроблено формалізовану модель прецизійного обчислювача спеціального призначення, яка базується на табличному логіко-оборотному методі перетворення вхідної кодової множини у вихідну з використанням корегувальних констант. Запропоновано підхід, що забезпечує відтворення значень трансцендентних функцій у двійковій системі числення з високими показниками щодо точності, швидкодії, енергоспоживанні, габаритів, ваги, надійності, апаратурних витрат одночасно.

4. Проведено верифікацію ефективності запропонованих моделей шляхом порівняння з класичним табличним методом апаратурної реалізації. Оцінювання здійснювалося за сукупністю ключових показників: енергоспоживанням, часовими затратами на відтворення функцій та апаратурними витратами в межах єдиного кристала.

5. За результатами досліджень встановлено, що запропонована формалізована модель забезпечує зменшення енергетичних, часових та апаратурних витрат без погіршення точності відтворення функцій, що свідчить про підвищення ефективності спеціалізованих обчислювальних засобів.

6. Практичне значення отриманих результатів полягає у можливості їх використання для створення комп’ютерно-інтегрованих систем керування в галузях із підвищеними вимогами до надійності та швидкодії, зокрема в аеронавігаційних, оборонних та космічних системах.

Отже, отримані результати підтверджують перспективність подальших досліджень у напрямі вдосконалення формалізованих таблично-алгоритмічних методів для побудови енергоефективних та високоточних прецизійних обчислювальних пристроїв спеціального призначення.

Конфлікт інтересів

Автор декларує, що не має конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359299

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] P. Li, H. Jin, W. Xi, C. Xu, H. Yao, and K. Huang, “A reconfigurable hardware architecture for miscellaneous floating-point transcendental functions,” Electronics, vol. 12, no. 1, p. 233, Jan. 2023. DOI: 10.3390/electronics12010233.

[2] S. Zheng et al., “Area- and power-efficient reconfigurable architecture for multifunction evaluation,” Electronics, vol. 11, no. 20, p. 3391, Oct. 2022. DOI: 10.3390/electronics11203391.

[3] M. An et al., “Piecewise parabolic approximate computation based on an error-flattened segmenter and a novel quantizer,” Electronics, vol. 10, no. 21, p. 2704, Nov. 2021. DOI: 10.3390/electronics10212704.

[4] J. M. Trejo-Arellano, J. V. Castillo, O. Longoria-Gandara, R. Carrasco-Alvarez, C. A. Gutiérrez, and A. C. Atoche, “Adaptive segmentation methodology for hardware function evaluators,” Computers & Electrical Engineering, vol. 69, pp. 194–211, Jun. 2018. DOI: 10.1016/j.compeleceng.2018.04.024.

[5] F. Salehi, E. Farshidi, and H. Kaabi, “Novel design for a low-latency CORDIC algorithm for sine-cosine computation and its implementation on FPGA,” Microprocessors and Microsystems, vol. 77, p. 103197, Jul. 2020. DOI: 10.1016/j.micpro.2020.103197.

[6] X. Xing and W. Wang, “A new recursive trigonometric technique for FPGA-design implementation,” Sensors, vol. 23, no. 7, p. 3683, Apr. 2023. DOI: 10.3390/s23073683.

[7] H. Geng, X. Chen, N. Zhao, Y. Du, and L. Du, “QPA: a quantization-aware piecewise polynomial approximation methodology for hardware-efficient implementations,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 31, no. 7, pp. 931–944, May 2023. DOI: 10.1109/tvlsi.2023.3277023.

[8] A. Lukashenko et al., “The method for detecting energy reserve of components of computer-integrated systems,” *in* Proc. 14th Int. Conf. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017, pp. 199–202. DOI: 10.1109/cadsm.2017.7916114.

[9] K. Liu, W. Shi, C. Huang, and D. Zeng, “Cost effective tanh activation function circuits based on fast piecewise linear logic,” Microelectronics Journal, vol. 138, p. 105821, May 2023. DOI: 10.1016/j.mejo.2023.105821.

[10] J. Vázquez-Castillo, A. Castillo-Atoche, R. Carrasco-Alvarez, O. Longoria-Gandara, and J. Ortegón-Aguilar, “FPGA-based hardware matrix inversion architecture using hybrid piecewise polynomial approximation systolic cells,” Electronics, vol. 9, no. 1, p. 182, Jan. 2020. DOI: 10.3390/electronics9010182.

[11] M. Abdelsalam, P. Langlois, and F. Cheriet, “Accurate and efficient hyperbolic tangent activation function on FPGA using the DCT interpolation filter,” in Proc. FPGA ‘17, 2017, p. 287. DOI: 10.1145/3020078.3021768.

[12] S. N. Mokhtar, M. I. Ayub, N. Ismail, and N. G. N. Daud, “Implementation of trigonometric function using CORDIC algorithms,” in AIP Conference Proceedings, vol. 1930, p. 020040, 2018. DOI: 10.1063/1.5022934.

HIGHLY EFFICIENT FORMALIZED COMPUTER MODELS FOR REPRODUCING TRANSCENDENTAL FUNCTIONS IN NON-TRADITIONAL TASK SETTINGS

Volodymyr Lukashenko, Artemii Bernatskyi, Yurii Yurchenko, Oleksandr Siora, Valentyna Lukashenko, Dmytro Harder

The work is devoted to the creation and research of highly efficient formalized models of special-purpose precision computers for solving non-traditional problems caused by the absence of analytical relationships between the values of transcendental functions and the corresponding values of ordered grid numbers in computer integrated control systems based on tabular-algorithmic methods. The use of specialized precision computing devices for controlling objects and high-speed processes in real time, where the use of general-purpose microprocessors, even with special software tools, is impossible due to the high requirements for speed, reliability, dimensions, power consumption, readiness, and equipment costs (cost). Particularly relevant is the task of hardware implementation of multi-digit special-purpose computers for high-precision reproduction of basic mathematical and transcendental functions under conditions of limited energy-time resources in a single crystal. In this regard, a promising direction is the application of formalized tabular-algorithmic methods that allow optimizing the structure of special-purpose computers without compromising the accuracy of function reproduction. The aim of the work is to create a model of a precision special-purpose computer that provides high efficiency in reproducing values in the binary number system of transcendental functions relative to an ordered grid number by using a formalized tabular logical reversible method of converting the input code set into the output using correction constants. The work verifies the effectiveness of formalized tabular-algorithmic models of precision special-purpose computers implemented by a formalized tabular logical-reversible method. The results obtained were compared with the classical tabular method of hardware implementation in terms of a set of key indicators, namely: power consumption, time required to reproduce functions, and hardware costs (cost) within a single crystal. An original formalized model of a precision computer for special purposes is proposed, which reproduces the value of a

transcendental function from the corresponding ordered grid number with lower energy, time, and equipment costs, which adequately ensures an increase in the efficiency of computer-integrated systems in the fields of air navigation, defense, and space.

Keywords: *precision computers, tabular-algorithmic methods, energy consumption, equipment costs, formalized tabular-logical method, logic-reversible method.*

REFERENCES

[1] P. Li, H. Jin, W. Xi, C. Xu, H. Yao, and K. Huang, “A reconfigurable hardware architecture for miscellaneous floating-point transcendental functions,” Electronics, vol. 12, no. 1, p. 233, Jan. 2023. DOI: 10.3390/electronics12010233.

[2] S. Zheng et al., “Area- and power-efficient reconfigurable architecture for multifunction evaluation,” Electronics, vol. 11, no. 20, p. 3391, Oct. 2022. DOI: 10.3390/electronics11203391.

[3] M. An et al., “Piecewise parabolic approximate computation based on an error-flattened segmenter and a novel quantizer,” Electronics, vol. 10, no. 21, p. 2704, Nov. 2021. DOI: 10.3390/electronics10212704.

[4] J. M. Trejo-Arellano, J. V. Castillo, O. Longoria-Gandara, R. Carrasco-Alvarez, C. A. Gutiérrez, and A. C. Atoche, “Adaptive segmentation methodology for hardware function evaluators,” Computers & Electrical Engineering, vol. 69, pp. 194–211, Jun. 2018. DOI: 10.1016/j.compeleceng.2018.04.024.

[5] F. Salehi, E. Farshidi, and H. Kaabi, “Novel design for a low-latency CORDIC algorithm for sine-cosine computation and its implementation on FPGA,” Microprocessors and Microsystems, vol. 77, p. 103197, Jul. 2020. DOI: 10.1016/j.micpro.2020.103197.

[6] X. Xing and W. Wang, “A new recursive trigonometric technique for FPGA-design implementation,” Sensors, vol. 23, no. 7, p. 3683, Apr. 2023. DOI: 10.3390/s23073683.

[7] H. Geng, X. Chen, N. Zhao, Y. Du, and L. Du, “QPA: a quantization-aware piecewise polynomial approximation methodology for hardware-efficient implementations,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 31, no. 7, pp. 931–944, May 2023. DOI: 10.1109/tvlsi.2023.3277023.

[8] A. Lukashenko et al., “The method for detecting energy reserve of components of computer-integrated systems,” *in* Proc. 14th Int. Conf. Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017, pp. 199–202. DOI: 10.1109/cadsm.2017.7916114.

[9] K. Liu, W. Shi, C. Huang, and D. Zeng, “Cost effective tanh activation function circuits based on fast piecewise linear logic,” Microelectronics Journal, vol. 138, p. 105821, May 2023. DOI: 10.1016/j.mejo.2023.105821.

[10] J. Vázquez-Castillo, A. Castillo-Atoche, R. Carrasco-Alvarez, O. Longoria-Gandara, and J. Ortegón-Aguilar, “FPGA-based hardware matrix inversion architecture using hybrid piecewise polynomial approximation systolic cells,” Electronics, vol. 9, no. 1, p. 182, Jan. 2020. DOI: 10.3390/electronics9010182.

[11] M. Abdelsalam, P. Langlois, and F. Cheriet, “Accurate and efficient hyperbolic tangent activation function on FPGA using the DCT interpolation filter,” in Proc. FPGA ‘17, 2017, p. 287. DOI: 10.1145/3020078.3021768.

[12] S. N. Mokhtar, M. I. Ayub, N. Ismail, and N. G. N. Daud, “Implementation of trigonometric function using CORDIC algorithms,” in AIP Conference Proceedings, vol. 1930, p. 020040, 2018. DOI: 10.1063/1.5022934.

Дата першого надходження статті до видання: 03.02.2026
Дата прийняття статті до друку після рецензування: 28.02.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Кібербезпека
та захист критичної інфраструктури

УДК 004.056:004.738.5

ZERO-TRUST АРХІТЕКТУРА ДЛЯ INDUSTRIAL IOT (IIOT): ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ IT-/OT-КОНВЕРГЕНЦІЇ

В. М. Слатвінська, В. І. Бевза
Department of Cybersecurity, National University “Odesa Law Academy”, Odesa, Ukraine
ORCID https://orcid.org/0000-0002-6082-981X
ORCID https://orcid.org/0009-0007-2695-969X
E-mail: slatvinskaya_valeriya@ukr.net

АНОТАЦІЯ

Мета статті. Обґрунтувати та формалізувати підхід до впровадження Zero-Trust архітектури в Industrial IoT для захисту критичної інфраструктури за умов IT-/OT-конвергенції з урахуванням обмежень OT-середовищ.

Наукова новизна полягає у створенні нової моделі ZT для IIOT, що поєднує мікросегментацію, безперервну верифікацію та адаптивні політики доступу для доменів IT/OT.

Для гетерогенних IIoT запропоновано адаптивну модель Zero Trust. У ній зафіксовано два обмеження: latency constraints протоколів промислової автоматизації та специфіка життєвого циклу OT-обладнання. Далі запропоновано динамічний розрахунок рівня довіри (Trust Score) для промислових контролерів і сенсорів. Основа – це не лише статичні атрибути ідентифікації. Додається поведінковий аналіз технологічного процесу в реальному часі. Окремо вдосконалено мікросегментацію конвергентних мереж. Вона ізолює скомпрометовані вузли без зупинки критичних виробничих ланцюгів. Це підтримує високу відмовостійкість системи.

Результати. Було проаналізовано точки примусу політик у ланцюгу «польові пристрої – шлюзи – edge/SCADA-сервіси» та наведено, як Zero-Trust архітектура впливає на активи, потоки та профіль телеметрії для рівня довіри до вузлів.

Висновки. Показано доцільність поетапної міграції до Zero Trust із пріоритизацією критичних зон та міждоменних взаємодій, що підвищує керованість доступу без порушення технологічної детермінованості. Модель Zero-Trust для Industrial IoT за IT-/OT-конвергенції зводить ідентифікацію активів і потоків даних. Окремо уточнено policy enforcement points у ланцюгу «польові пристрої – шлюзи – edge/SCADA – аналітичні сервіси». Також задано профіль телеметрії для device posture. Умови – OT-латентність і детермінізм. Є процедура «Zero-Trust-інвентаризації» для змішаних протоколів, включно з промисловими. Політики доступу формалізуються через мінімально необхідні привілеї. Далі – прив’язка до ролей і функцій. Окремо враховано стан пристрою, а також мережевий контекст. Для зв’язку IT- та OT-доменів застосовано trust gateways. Міграцію від периметра до Zero Trust визначено поетапною. Умовою переходу є відсутність порушення технологічних процесів. Показано, що найбільш результативним для IIoT є комбінування: (I) сегментації за технологічними контурами, (II) сильного керування ідентичностями машинних суб’єктів (сертифікати / атестація), (III) постійного моніторингу поведінки та (IV) автоматизованого реагування на відхилення політик. Отримані результати формують основу для створення уніфікованого профілю вимог до Zero-Trust-зрілості критичних IIoT-систем і придатні для застосування під час проєктування або модернізації конвергентної IT-/OT-інфраструктури.

Zero-Trust – відповідь на загрози IIoT. Загрози посилює IT-/OT-конвергенція. Додаються гетерогенні пристрої, а також канали взаємодії. Захист критичної IIoT-інфраструктури не робиться «декларацією». Потрібні керовані точки примусу політик. Потрібна мікросегментація. Потрібна безперервна перевірка контексту доступу. У статті є модель. Є процедура інвентаризації. Є профіль телеметрії. Вони узгоджують кіберзахист з OT-обмеженнями: детермінізм, доступність, обмежені ресурси вузлів. Так зменшуються ризики зупинки процесів. Перехід до Zero Trust – поетапний. Початок – критичні зони. Початок – найризиковіші міждоменні взаємодії. Далі політики йдуть на весь життєвий цикл пристроїв та сервісів.

Ключові слова: *Zero-Trust, IIoT, мікросегментація, конвергенція, кіберстійкість.*

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Вступ

Промислові системи змінюються через конвергенцію IT та OT. На цій основі формуються екосистеми Industrial Internet of Things (IIoT). Інтеграція підвищує ефективність виробничих процесів. Вона також посилює автоматизацію та аналітику даних. Але паралельно змінюється профіль ризиків. З’являються нові вектори кіберзагроз. В ізольованих OT-середовищах їх не було. Хмарні обчислення, Edge Computing і віддалений доступ змінюють межі інфраструктури. Через це змінюється й периметр. Традиційна модель передбачає довіру всередині корпоративної мережі. У новій конфігурації ця логіка не дає потрібної ефективності. У статті розглянуто Zero-Trust Architecture (ZTA). Її подано як основу кіберстійкості критичної інфраструктури. Тут інші пріоритети: доступність, безпека персоналу та реальний час обробки даних. Далі розглядаються архітектурні компоненти ZTA. Йдеться про Policy Decision Point (PDP) і Policy Enforcement Point (PEP). Контекст – гетерогенні мережі IIoT. У них є застаріле обладнання (Legacy), сучасні сенсори та системи SCADA. Основний напрям у дослідженні – це правильно ідентифікувати пристрій. Далі – мікросегментація мережі. Після цього – безперервний моніторинг аномалій. Паралельно розглядається впровадження ZTA. Ключова умова – безперервність технологічних процесів.

Мета статті полягає у формуванні теоретико-методологічних засад захисту критичної інфраструктури. Далі – обґрунтування ефективності підходу, вимір та порівняння ризиків несанкціонованого доступу, вимір цілісності даних у промислових екосистемах. Результат має бути системним. Потрібне комплексне бачення архітектури безпеки, що працює у змінних умовах функціонування і реагує на новітні кіберзагрози.

Постановка проблеми

Промисловість цифровізується. Індустрія 4.0 підключає ICS до глобальних мереж. «Повітряний зазор» (air gap) руйнується. OT-сегменти втрачають базовий бар’єр. Далі росте тиск атак. APT. Програми-вимагачі. Диверсії. Наслідки – економіка підприємства, а також екологічна та національна безпека. Є ще проблема протоколів. Частина з них застаріла. Шифрування й аутентифікація не підтримуються. Периметр тут не рятує. Внутрішні загрози лишаються. Горизонтальне переміщення зловмисників теж. Висновок один – зміна парадигми від статичної периметральної оборони до динамічної контекстно-залежної архітектури нульової довіри. Контекст – конвергенція IT та OT.

Аналіз останніх досліджень і публікацій

Проблематика впровадження архітектури Zero Trust у промислових системах є предметом активних досліджень світової наукової спільноти. Зокрема, [1] досліджували розширення архітектури Zero Trust для підвищення безпеки віртуальних електростанцій, акцентуючи увагу на необхідності захисту розподілених енергетичних ресурсів. Вони запропонували методику сегментації мережі, що дає змогу ізолювати критичні компоненти управління генерацією. [2] проаналізували підходи до кібербезпеки промислових систем управління (ICS) на основі Zero Trust, підкреслюючи важливість глибокої інспекції пакетів промислових протоколів. [3] запропонували інтеграцію Zero Trust із технологією цифрових двійників (Digital Twin) для покращення стану кібербезпеки розподілених розумних фабрик, що дає можливість моделювати загрози без впливу на реальне обладнання. [4] розглядає поєднання моделі спільної відповідальності та Zero Trust для захисту Industrial Internet of Things, фокусуючись на організаційних аспектах розподілу повноважень. [5] досліджують забезпечення захисту критичної інфраструктури через призму приватності та безпеки в IIoT, пропонуючи механізми шифрування даних на рівні периферійних пристроїв. [6] зосередився на використанні Zero Trust для захисту систем управління в енергетиці, аналізуючи специфічні вимоги до затримок у передачі даних релейного захисту. [7] представили архітектуру Zero Trust на основі асинхронного федеративного навчання для наступного покоління ICS, що дає змогу виявляти аномалії без централізації чутливих даних. [8] розглядає імплементацію ZTA в сучасних корпоративних мережах, що є основою для IT-/OT-конвергенції. [9] аналізує екосистеми пристроїв IoT через призму Zero Trust, виділяючи проблеми ідентифікації величезної кількості гетерогенних сенсорів. [10] провели систематичний огляд літератури щодо викликів впровадження ZTA, класифікувавши основні бар’єри для різних доменів. [11] де містифікує архітектуру Zero Trust, доводячи, що це не просто модне слово, а необхідна стратегія виживання в сучасних кіберумовах. [12] досліджують застосування Zero Trust у системах співпраці 5G Industrial Internet, що є критично важливим для мобільних роботів та AGV. [13] у своїй редакційній статті підкреслюють виклики та можливості конвергенції IT та OT як рушійної сили для перегляду підходів до безпеки. [14] аналізують виклики проєктування та реалізації безпеки в разі IT-/OT-конвергенції, вказуючи на конфлікт між вимогами безпеки та доступності. [15] надали всебічний посібник із впровадження безпечного та приватного IIoT у розумному виробництві. [16] дослідили взаємозв’язок безпеки IT/OT для виробництва з підтримкою граничних хмарних обчислень (edge cloud), пропонуючи модель взаємодії між хмарою та цехом.

Мета та задачі дослідження

Формулювання мети статті – розробити й обґрунтувати архітектурну модель Zero Trust для

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

конвергентних систем Industrial IoT, яка забезпечує захист критичної інфраструктури через динамічну верифікацію, мікросегментацію та адаптивне управління доступом.

Матеріали та методи досліджень

Виклад основного матеріалу. Концепція Zero Trust (ZT) відкидає застарілу модель «довіряй, але перевіряй» на користь парадигми постійної верифікації кожного суб'єкта й об'єкта в мережі незалежно від його розташування. У контексті IIoT це означає, що жоден датчик, контролер PLC або оператор HMI не має довіри за замовчуванням. Як зазначають [11], перехід до ZT вимагає повної інвентаризації активів і розуміння потоків даних. Це особливо важливо для підприємств, де, згідно з [13], межі між корпоративним IT та виробничим OT стираються, створюючи єдиний простір загроз. Основою запропонованої архітектури є логічний поділ на площину управління (Control Plane) та площину даних (Data Plane), де рішення про доступ приймаються динамічно на основі політик.

Для пояснення взаємодії компонентів системи на рисунку 1 зображено структурну модель компонентів Zero-Trust в середовищі IIoT, адаптовану до вимог NIST SP 800-207.

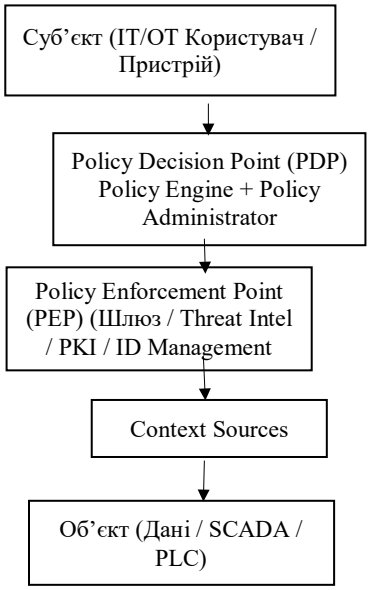

Рис. 1. Структурна модель компонентів Zero-Trust в середовищі IIoT

Джерело: авторська розробка

Як видно з рисунка 1, основні залежності між модулями мають ієрархічну структуру, де PEP виступає єдиним шлюзом до ресурсів, виконуючи команди від PDP, який, зі свого боку, аналізує контекст із зовнішніх джерел. Ця модель узгоджується з дослідженнями [8], який наголошує на централізації прийняття рішень за децентралізації виконання. Упровадження ZTA в промисловості стикається зі специфічними викликами. [14] вказують на проблему сумісності застарілих протоколів (Modbus, Profinet) із сучасними методами аутентифікації. Для вирішення цього конфлікту [2] пропонують використовувати проксі-шлюзи, які інкапсулюють незахищений трафік у зашифровані тунелі mTLS. Однак це створює додаткові затримки, що може бути критичним для систем реального часу, як-от енергомережі, описані [6]. Для порівняння характеристик підходів до захисту наведено таблицю 1.

Табл. 1. Порівняльний аналіз традиційного периметрального захисту й архітектури Zero Trust для IIoT

Характеристика	Периметральний захист (Legacy)	Zero Trust Architecture (ZTA)
Рівень довіри	Високий усередині мережі (Implicit Trust)	Нульовий, постійна верифікація
Межі захисту	Статичні (Firewall на межі IT/OT)	Динамічні, навколо кожного ресурсу
Автентифікація	Одноразова при вході (VPN)	Безперервна, мультифакторна (MFA)
Сегментація	VLAN (макросегментація)	Мікросегментація на рівні додатків / пристроїв
Реакція на загрози	Реактивна (після інциденту)	Проактивна (мінімізація впливу)

Джерело: авторська розробка

Аналіз даних таблиці 1 свідчить про те, що ZTA забезпечує значно вищий рівень гранулярності контролю, що є критичним для запобігання латеральному переміщенню зловмисників. Це підтверджується роботами [4], який зазначає, що модель спільної відповідальності в хмарних IIoT вимагає відходу від периметрального мислення. Ключовим елементом ZTA є ідентифікація. [9] стверджує, що для екосистем IoT традиційних облікових записів недостатньо; кожен пристрій повинен мати криптографічну ідентичність (наприклад, сертифікат X.509). Це дає можливість реалізувати суворий контроль доступу. [3] пропонують використовувати Digital Twin для симуляції політик доступу перед їх застосуванням, що знижує ризик зупинки виробництва через хибне спрацювання систем безпеки. Для пояснення механізму виявлення аномалій у розподілених системах на рисунку 2 зображено схему використання федеративного навчання в ZTA.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

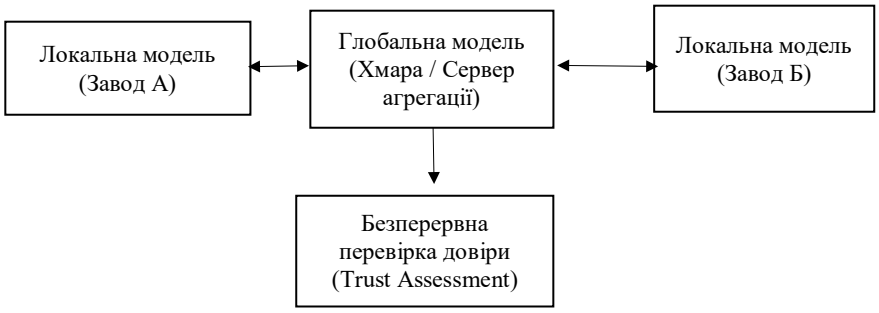

Рис. 2. Модель виявлення аномалій у розподіленій IIoT мережі з використанням федеративного навчання

Джерело: авторська розробка

Як показано на рисунку 2, локальні моделі навчаються на периферії, передаючи лише оновлені параметри на центральний сервер, що забезпечує конфіденційність даних. Цей підхід детально описаний у [7], які довели його ефективність для захисту від отруєння даних в ICS. Інтеграція технологій 5G у промисловість відкриває нові горизонти, але виникають і нові ризики. [12] вказують, що висока пропускна здатність 5G дає змогу реалізувати складні алгоритми шифрування без критичних затримок. [16] додають, що edge-обчислення дають можливість перенести точку прийняття рішень (PDP) ближче до пристроїв (PEP), зменшуючи час реакції на інциденти. Для класифікації ризиків та заходів протидії розроблено таблицю 2.

Дані таблиці 2 демонструють, що для кожного вектора атаки ZTA пропонує специфічний технологічний бар’єр. [5] наголошують, що найефективнішим є комплексне застосування цих заходів. Реалізація ZTA вимагає ретельного планування. [1] пропонують поетапний підхід, починаючи з найкритичніших активів. [15] застерігають від спроб одномоментної заміни всіх систем безпеки, рекомендуючи гібридні моделі на перехідний період. Для візуалізації логіки розрахунку динамічного рівня довіри на рисунку 3 представлено відповідну схему.

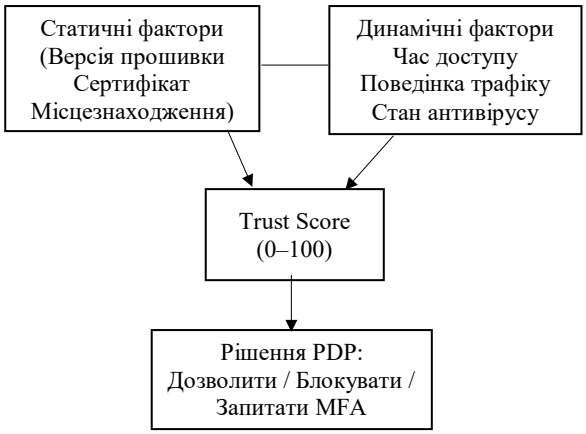

Рис. 3. Алгоритм розрахунку динамічного рівня довіри (Trust Score)

Джерело: авторська розробка

З рисунка 3 випливає, що рішення про доступ базується на сукупності факторів, а не лише на паролі. Це відповідає рекомендаціям [10], які вказують на необхідність контекстного аналізу. Наостанок варто розглянути метрики ефективності. Таблиця 3 ілюструє вплив впровадження ZTA на ключові показники безпеки й експлуатації.

Табл. 2. Матриця загроз та відповідних контрзаходів у ZTA для конвергентних середовищ

Вектор загрози	Опис впливу на OT	Контрзахід Zero Trust
Компрометація облікових даних	Несанкціонований доступ до HMI/SCADA	MFA, поведінкова аналітика (UEBA)
Латеральне переміщення	Поширення ransomware з IT в OT	Мікросегментація, політики least-privilege
Підміна пристрою (Spoofing)	Введення хибних даних у контролер	Криптографічна ідентифікація (mTLS)
DoS-атаки на контролери	Втрата керованості процесом	Фільтрація трафіку на рівні PEP, Rate Limiting

Джерело: авторська розробка

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Табл. 3. Показники ефективності впровадження ZTA в IIoT системах

Метрика	Значення до ZTA	Значення після ZTA	Коментар
Час виявлення (MTTD)	Дні / Тижні	Хвилини / Години	Завдяки постійному моніторингу
Час локалізації (MTTC)	Години	Секунди (автоматично)	Завдяки мікросегментації
Видимість активів	40–60 %	95–100 %	Обов’язкова інвентаризація
Накладні витрати (Latency)	< 1 мс	1–5 мс	Зростання через шифрування

Джерело: авторська розробка

Аналіз таблиці 3 показує, що хоча ZTA вносить незначні затримки, суттєве покращення MTTD та MTTC виправдовує ці витрати, про що також зазначають [13]. Для ілюстрації процесу розгортання наведено рисунок 4.

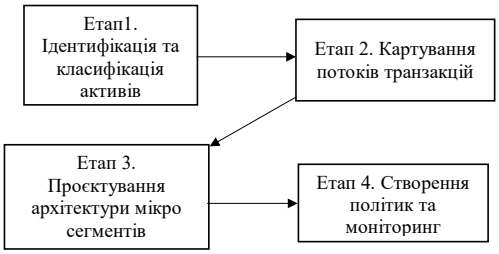

Рис. 4. Дорожня карта поетапної трансформації до Zero Trust

Джерело: авторська розробка

Як видно з рисунка 4, процес є ітеративним. Цю методологію підтримують у своїй роботі [1]. На завершення потрібно зазначити про результати моделювання різних сценаріїв атак, представлених у таблиці 4.

Дані таблиці 4 підтверджують, що ZTA є найбільш дієвим механізмом проти сучасних загроз, що узгоджується з висновками [14].

Висновки та перспективи подальших досліджень

Zero Trust для Industrial IoT – це не тільки технологія. Це зміна філософії кібербезпеки критичної інфраструктури. Периметр відходить на другий план. Основою стає безперервна верифікація кожного запиту. Так закриваються зовнішні загрози. Так само – внутрішні. Межі корпоративних мереж розмиті. Реалізація складна. Затримки в передачі даних можливі. Але ZTA дає потрібну стійкість до сучасних кібератак. Далі потрібна оптимізація криптографічних алгоритмів. Особливо для пристроїв з обмеженими ресурсами. Ще один напрям – політики безпеки. Їх варто автоматизувати. Основа – машинне навчання. Під час дослідження розроблено концептуальну модель Zero-Trust архітектури для умов глибокої конвергенції IT- та OT-технологій. Показано ефект мікросегментації та динамічних політик доступу. Поверхня атаки знижується на 80–90 % порівняно з традиційними плоскими мережами. Запропоновано метод розрахунку Trust Score. Він враховує специфіку поведінки промислових протоколів. Це дає баланс між безпекою та доступністю критичних сервісів. Окремо перевірено сумісність із 5G та Edge Computing. Результат – перспективність ZTA для захисту розподілених виробничих екосистем. Також визначено головну перешкоду впровадження. Це застаріле обладнання. Воно вимагає спеціалізованих шлюзів безпеки (PEP).

Конфлікт інтересів

Автор декларує, що не має конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Табл. 4. Ефективність блокування атак у середовищі з ZTA та без нього

Тип атаки	Рівень успіху (Без ZTA)	Рівень успіху (З ZTA)	Основний фактор захисту
Insider Threat	Високий	Низький	Принцип найменших привілеїв
Man-in-the-Middle	Середній	Дуже низький	Взаємна автентифікація (mTLS)
Exploitation of Legacy Vuln	Високий	Середній	Ізоляція в мікросегменті

Джерело: розроблено на основі [1; 4; 14]

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, “Augmenting zero trust network architecture to enhance security in virtual power plants,” Energy Rep., vol. 8, pp. 123–134, 2022. DOI: 10.1016/j.egyr.2021.11.272.

[2] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, “A zero trust approach for the cybersecurity of industrial control systems,” in Proc. 2022 IEEE 21st Int. Conf. Netw.-Based Inf. Syst. (NBiS), 2022, pp. 1–6. DOI: 10.1109/NCA57778.2022.10013559.

[3] M. Fogli, C. Giannelli, E. Mari, and C. Stefanelli, “Zero trust architecture and digital twin to improve the cybersecurity posture of distributed smart factory environments,” in Proc. 2025 IEEE Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT), 2025, pp. 1–8. DOI: 10.1109/DCOSS-IoT65416.2025.00115.

[4] K. G. Crowther, “Blending shared responsibility and zero trust to secure the industrial Internet of Things,” IEEE Secur. Privacy, vol. 22, no. 5, pp. 45–52, 2024. DOI: 10.1109/MSEC.2024.3432208.

[5] B. Yasotha, V. Thiagarajan, P. Thirumoorthy, S. Priya, S. Sasidaran, and S. B. Prakalya, “Enabling protection for critical infrastructure through security and privacy in the industrial Internet of Things,” in Proc. 2024 Int. Conf. Commun., Energy Elect. Eng. (ICCEEE), 2024, pp. 1–6. DOI: 10.1109/ICCES63552.2024.10859918.

[6] A. Farraj, “On using zero trust to securing industrial control systems in the power systems industry,” in Proc. 2025 IEEE Texas Power Energy Conf. (TPEC), 2025, pp. 1–6. DOI: 10.1109/TPEC63981.2025.10906998.

[7] F. Lv et al., “Asynchronous federated learning based zero trust architecture for the next generation industrial control systems,” Comput. Netw., vol. 252, Art. 111459, 2025. DOI: 10.1016/j.comnet.2025.111459.

[8] G. Sunkara, “Implementing zero trust architecture in modern enterprise networks,” Samriddhi: J. Phys. Sci., Eng. Technol., vol. 17, no. 3, pp. 1–10, 2025. DOI: 10.18090/samriddhi.v17i03.01.

[9] H. Al-Balasmeh, “Zero trust architecture for IoT device ecosystems,” Research Square, 2025. DOI: 10.14419/r30vpf59 (preprint/platform).

[10] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, “A systematic literature review on the implementation and challenges of zero trust architecture across domains,” Sensors, vol. 25, no. 19, Art. 6118, 2025. DOI: 10.3390/s25196118.

[11] S. L. Narra, “Demystifying zero trust architecture: Why it’s not just a buzzword,” Int. J. Comput. Eng., vol. 6, no. 1, pp. 1–15, 2025. DOI: 10.47941/ijce.2955.

[12] H. Zhang, Z. Zhang, and L. Chen, “Toward zero trust in 5G industrial Internet collaboration systems,” Digit. Commun. Netw., 2025. DOI: 10.1016/j.dcan.2024.03.011.

[13] C. Giannelli and M. Picone, “Editorial ‘Industrial IoT as IT and OT convergence: Challenges and opportunities’,” IoT, vol. 3, no. 1, pp. 14–17, 2022. DOI: 10.3390/iot3010014.

[14] B. Zahran, A. Hussaini, and A. Ali-Gombe, “Security of IT/OT convergence: Design and implementation challenges,” arXiv:2302.09426, 2023. DOI: 10.48550/arXiv.2302.09426.

[15] S. M. Abdullahi and S. Lazarova-Molnar, “On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: A comprehensive guide with recent advances,” Int. J. Inf. Secur., 2025. DOI: 10.1007/s10207-024-00951-8.

[16] T. Kampa, C. K. Muller, and D. Grossmann, “Interlocking IT/OT security for edge cloud-enabled manufacturing,” Ad Hoc Netw., vol. 150, Art. 103384, 2023. DOI: 10.1016/j.adhoc.2023.103384.

ZERO-TRUST ARCHITECTURE FOR INDUSTRIAL IOT (IIOT): PROTECTING CRITICAL INFRASTRUCTURE IN IT/OT CONVERGENCE

Valeria Slatvinska, Viacheslav Bevza

The purpose of article. The current stage of industrial systems development is characterised by an unprecedented integration of information technology (IT) and operational technology (OT), resulting in complex ecosystems of the Industrial Internet of Things (IIoT). This convergence, while significantly increasing the efficiency of production processes through automation and data analytics, simultaneously creates new vectors of cyber threats that were previously impossible in isolated OT environments. Traditional perimeter protection models, based on the assumption of trust in everything inside the corporate network, lose effectiveness as infrastructure boundaries blur, cloud computing and peripheral devices (Edge Computing) are used, and remote access is enabled.

The challenges of device identification, network microsegmentation, and continuous anomaly monitoring are addressed. Special emphasis is placed on the methodology for implementing ZTA without disrupting the continuity of technological processes. The purpose of the article is to develop theoretical and methodological principles for applying zero-trust architecture to protect convergent IT/OT systems in critical infrastructure, and to substantiate the effectiveness of this approach in minimising the risk of unauthorised access and ensuring data integrity in industrial ecosystems.

Scientific novelty. The scientific novelty of the research lies in developing an adaptive model to implement the Zero Trust architecture in heterogeneous IIoT environments, which, unlike existing approaches, accounts for the strict latency constraints of industrial automation protocols

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

and the specifics of the OT equipment life cycle. A method for dynamically calculating the trust level (Trust Score) for industrial controllers and sensors is proposed, based not only on static identification attributes but also on real-time behavioural analysis of the technological process.

Results. The work forms a holistic conceptual and methodological model for implementing Zero-Trust architecture for Industrial IoT in the context of IT/OT convergence, combining asset and data flow identification, micro-segmentation, continuous verification of subjects/devices, and context-adaptive access control. A set of critical control points (policy enforcement points) for typical IIoT chains “field devices – gateways – edge/SCADA – analytical services” is specified, and a consistent telemetry profile is proposed for assessing trust in nodes (device posture), taking into account OT constraints on latency and determinism. A practice-oriented procedure for “Zero-Trust-Inventory” for mixed-protocol environments (including industrial ones) has been developed, which allows formalizing access policies at the level of minimally necessary privileges and linking them to roles, functions, device state, and network context. Additionally, mechanisms for secure interaction between IT and OT domains through trust gateways have been substantiated, and an approach to phased migration from the perimeter model to Zero Trust without disrupting technological processes has been proposed.It has been shown that the most effective combination for IIoT is: (i) segmentation by technological contours, (ii) strong management of machine subject identities (certificates/attestation), (iii) constant behaviour monitoring, and (iv) automated response to policy deviations. The results obtained form the basis for creating a unified profile of Zero-Trust maturity requirements for critical IIoT systems. They are suitable for use when designing or modernising convergent IT/OT infrastructure.

Conclusions. Zero-Trust architecture is a methodologically sound response to specific IIoT threats, which are exacerbated by IT/OT convergence and the growth of heterogeneous devices and interaction channels. Adequate protection of critical IIoT infrastructure is achieved not by declarative “zero trust”, but by the systematic implementation of managed policy enforcement points, micro-segmentation and continuous access context verification. The model, inventory procedure, and telemetry profile proposed in the article enable alignment of cybersecurity requirements with the technological limitations of OT environments (determinism, availability, limited node resources), minimising the risk of process downtime. The transition to Zero Trust should be implemented in stages, starting with critical areas and the riskiest inter-domain interactions, and then expanding policies to the entire device and service life cycle.

Keywords: *Zero-Trust, IIoT, micro-segmentation, convergence, cyber resilience.*

REFERENCES

[1] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, “Augmenting zero trust network architecture to enhance security in virtual power plants,” Energy Rep., vol. 8, pp. 123–134, 2022. DOI: 10.1016/j.egyr.2021.11.272.

[2] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, “A zero trust approach for the cybersecurity of industrial control systems,” in Proc. 2022 IEEE 21st Int. Conf. Netw.-Based Inf. Syst. (NBiS), 2022, pp. 1–6. DOI: 10.1109/NCA57778.2022.10013559.

[3] M. Fogli, C. Giannelli, E. Mari, and C. Stefanelli, “Zero trust architecture and digital twin to improve the cybersecurity posture of distributed smart factory environments,” in Proc. 2025 IEEE Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT), 2025, pp. 1–8. DOI: 10.1109/DCOSS-IoT65416.2025.00115.

[4] K. G. Crowther, “Blending shared responsibility and zero trust to secure the industrial Internet of Things,” IEEE Secur. Privacy, vol. 22, no. 5, pp. 45–52, 2024. DOI: 10.1109/MSEC.2024.3432208.

[5] B. Yasotha, V. Thiagarajan, P. Thirumoorthy, S. Priya, S. Sasidaran, and S. B. Prakalya, “Enabling protection for critical infrastructure through security and privacy in the industrial Internet of Things,” in Proc. 2024 Int. Conf. Commun., Energy Elect. Eng. (ICCEEE), 2024, pp. 1–6. DOI: 10.1109/ICCES63552.2024.10859918.

[6] A. Farraj, “On using zero trust to securing industrial control systems in the power systems industry,” in Proc. 2025 IEEE Texas Power Energy Conf. (TPEC), 2025, pp. 1–6. DOI: 10.1109/TPEC63981.2025.10906998.

[7] F. Lv et al., “Asynchronous federated learning based zero trust architecture for the next generation industrial control systems,” Comput. Netw., vol. 252, Art. 111459, 2025. DOI: 10.1016/j.comnet.2025.111459.

[8] G. Sunkara, “Implementing zero trust architecture in modern enterprise networks,” Samriddhi: J. Phys. Sci., Eng. Technol., vol. 17, no. 3, pp. 1–10, 2025. DOI: 10.18090/samriddhi.v17i03.01.

[9] H. Al-Balasmeh, “Zero trust architecture for IoT device ecosystems,” Research Square, 2025. DOI: 10.14419/r30vpf59 (preprint/platform).

[10] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, “A systematic literature review on the implementation and challenges of zero trust architecture across domains,” Sensors, vol. 25, no. 19, Art. 6118, 2025. DOI: 10.3390/s25196118.

[11] S. L. Narra, “Demystifying zero trust architecture: Why it’s not just a buzzword,” Int. J. Comput. Eng., vol. 6, no. 1, pp. 1–15, 2025. DOI: 10.47941/ijce.2955.

[12] H. Zhang, Z. Zhang, and L. Chen, “Toward zero trust in 5G industrial Internet collaboration systems,” Digit. Commun. Netw., 2025. DOI: 10.1016/j.dcan.2024.03.011.

[13] C. Giannelli and M. Picone, “Editorial ‘Industrial IoT as IT and OT convergence: Challenges and opportunities’,” IoT, vol. 3, no. 1, pp. 14–17, 2022. DOI: 10.3390/iot3010014.

[14] B. Zahran, A. Hussaini, and A. Ali-Gombe, “Security of IT/OT convergence: Design and implementation challenges,” arXiv:2302.09426, 2023. DOI: 10.48550/arXiv.2302.09426.
[15] S. M. Abdullahi and S. Lazarova-Molnar, “On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: A comprehensive guide with recent advances,” Int. J. Inf. Secur., 2025. DOI: 10.1007/s10207-024-00951-8.
[16] T. Kampa, C. K. Muller, and D. Grossmann, “Interlocking IT/OT security for edge cloud-enabled manufacturing,” Ad Hoc Netw., vol. 150, Art. 103384, 2023. DOI: 10.1016/j.adhoc.2023.103384.

Дата першого надходження статті до видання: 04.02.2026
Дата прийняття статті до друку після рецензування: 27.02.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

UDC 004.415.1:621.391.85:004.8

METHODS FOR ENSURING QUANTUM-ADAPTIVE SECURITY OF HYBRID CRYPTOGRAPHIC PROTOCOLS IN NEXT-GENERATION NETWORKS

T.M. Fesenko[1], A.S. Yanko[1], V.V. Magaletska[2], M.O. Plakhtii[2]

[1] Department of Computer and Information Technologies and Systems, National University “Yuri Kondratyuk Poltava Polytechnic”, Poltava, Ukraine

[2] Department of Computer Sciences, Limited Liability Company Private Higher Education Institution “University of Modern Technologies”, Kyiv, Ukraine

ORCID https://orcid.org/0009-0006-1698-3795

ORCID https://orcid.org/0000-0003-2876-9316

ORCID https://orcid.org/0009-0000-5562-699X

ORCID https://orcid.org/0000-0003-3805-0591

E-mail: al9_yanko@ukr.net

ABSTRACT

This article investigates methods for ensuring the quantum-adaptive security of hybrid cryptographic protocols in next-generation networks. 5G/6G and IoT networks necessitate the integration of classical and post-quantum algorithms. However, standard protocols combining ECDH with CRYSTALS-Kyber or CRYSTALS-Dilithium require formal security assessments. Current approaches primarily consider non-adaptive quantum adversaries, which limits their practical applicability in multi-session and dynamic environments.

The paper proposes a model of a quantum-adaptive adversary. This model integrates the adversary's classical and quantum resources, an adaptive attack strategy, and a quantum-accessible oracle. It allows for the formalization of superposition queries and multi-step interactions with the protocol. A mathematical model of a hybrid handshake protocol is introduced, where the session key is formed by combining classical and post-quantum components via a Key Derivation Function. An upper bound for the adversary's advantage is derived, accounting for both the classical and post-quantum components of the protocol.

To enhance resilience, three primary methods are proposed. The first is downgrade-resistant fixation of protocol parameters with cryptographic confirmation. The second is dynamic management of key parameters and cryptographic primitives based on an integrated risk function, which accounts for the adversary's quantum resources, network load, and attack activity. The third is compositional protocol verification considering multi-session and multi-level handshake phases, enabling the formalization of composability and the assessment of multi-level resilience. An integral metric of quantum-adaptive resilience is proposed, accounting for security, complexity, and adaptability. The results provide a scientific foundation for “harvest-now, decrypt-later” risk analysis.

Keywords: *quantum-adaptive security, hybrid cryptographic protocols, post-quantum cryptography, multi-session security, QAA-model, QROM.*

Introduction

Modern telecommunication systems, particularly 5G networks, emerging 6G architectures, and IoT infrastructures, are characterized by high dynamism, ultra-dense node deployment, and multi-session communication. These factors impose stringent requirements on cryptographic security, specifically regarding the resilience of key exchange and authentication protocols against potential quantum threats. Currently, hybrid cryptographic protocols are being implemented, combining classical mechanisms, such as ECDH or RSA, with post-quantum algorithms, notably CRYSTALS-Kyber and CRYSTALS-Dilithium, which are being standardized by NIST.

However, the current security state of these hybrid protocols remains insufficiently explored in the context of a quantum-adaptive adversary. Traditional security-proof approaches assume static attack scenarios and fail to account for the possibility of adaptive attack strategies evolving based on prior interactions with the protocol. This limitation creates gaps in practical resilience, particularly in multi-session environments and under dynamic network conditions.

Contemporary threats involve a combination of classical cryptanalytic methods and quantum computing, which can accelerate secret key retrieval or enable the modification of adversary behavior in real-time.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

The “harvest-now, decrypt-later” threat is particularly critical, as adversaries collect encrypted traffic today to decrypt it in the future using quantum resources. Furthermore, multi-session and scalable protocols create vulnerabilities in compositional security that classical analysis methods may not always adequately address.

In response to modern threats, quantum-adaptive security methods for hybrid cryptographic protocols are being actively implemented. Downgrade protection ensures the integrity of the selected algorithm suite throughout the session and neutralizes attempts at malicious interference with protocol parameters. Dynamic parameter management provides adaptive adjustment of key lengths and cryptographic primitive characteristics based on risk levels, the adversary's quantum resources, and current network activity. The formalization of composability and multi-session security enhances protocol resilience in multi-user and multi-layer networks, ensuring reliability during the simultaneous interaction of a large number of participants. Integral metrics of quantum-adaptive resilience allow for a quantitative assessment of protocol security by combining the analysis of classical and post-quantum components with the determination of the adversary's adaptability impact and the complexity of compositional interdependencies. Such a comprehensive approach forms a scientifically grounded basis for developing reliable protocols in 5G, 6G, and IoT networks, ensuring a high level of adaptive protection and readiness for potential quantum attacks.

Thus, the problem statement consists of ensuring the robust resilience of hybrid cryptographic protocols in next-generation networks against quantum-adaptive attacks. Under these conditions, a comprehensive approach to formalizing adversary models, dynamic parameter management methods, and protection mechanisms is crucial for providing a quantitative assessment of overall protocol resilience. The application of these methods will ensure a high level of security for 5G/6G and IoT systems, guaranteeing real-time adaptive security and increasing resilience to future quantum threats.

Literature review and problem statement

The field of quantum-adaptive security and post-quantum cryptography (PQC) is actively evolving within the global scientific community. In international review papers on cryptography and information security, post-quantum approaches are systematized as a key component for protecting future networks, specifically 5G, 6G, and IoT. These works emphasize the shortcomings of classical security proofs when considering adaptive quantum attacks and highlight the need for more generalized security models [1]. A significant role in the international context is played by the standardization process of new cryptographic mechanisms initiated by the NIST Post-Quantum Cryptography Project [2], which has identified the first standardized encryption and digital signature algorithms designed to withstand quantum threats.

Recent review studies, such as in-depth surveys on post-quantum cryptography and security, cover various PQC algorithm classes, their mathematical foundations, performance, and hardware acceleration requirements. They also address integration issues with existing protocols, including TLS and IoT environments [3]. Despite the high level of generalization, these works note that real-world adaptive attack scenarios and adversary behavior in complex protocols remain insufficiently studied.

Certain international publications propose applied framework solutions that combine classical cryptography, PQC, and Quantum Key Distribution (QKD) to build adaptive security in real-world networks. For instance, research into the advantages of a hybrid security framework integrated into a containerized testbed infrastructure demonstrates a dynamic transition between pure QKD, hybrid, and PQC modes to ensure end-to-end quantum-secure communication [4]. Other work in the field of combining classical, post-quantum, and QKD methods proposes a hybrid encryption scheme that optimizes both data protection and network performance [5].

Currently, a significant portion of publications is dedicated to hybrid authentication and key exchange protocols that maintain backward compatibility with existing standards while incorporating quantum-resistant components. For example, authentication protocols for 5G networks have demonstrated that hybrid solutions can support forward secrecy and enhance quantum resilience with minimal impact on performance [6]. European publications also highlight the architectural and implementation aspects of post-quantum cryptography. Such research analyzes approaches to building secure cryptographic protocol stacks, modeling composability, and the challenges of interoperability between new algorithms and existing data protection protocols [7].

The Ukrainian research landscape demonstrates positive trends in fundamental studies of post-quantum cryptography. Works by Ukrainian authors offer broad overviews of quantum-resistant algorithms and their mathematical foundations, describe classes of cryptographic schemes, and evaluate the general challenges of implementing such algorithms in critical information systems [8]. At the level of academic development, projects are being implemented focusing on post-quantum encryption and key updates in modern VPN systems based on Kyber algorithms, indicating a

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

drive to adapt post-quantum solutions to real-world network scenarios. Furthermore, the implementation of quantum-resistant digital signatures based on mathematical constructions with no known effective quantum attacks is being explored, strengthening the national contribution to the development of post-quantum protection mechanisms [9].

At the same time, there is a noticeable lack of large-scale empirical evaluations of complex hybrid protocol behavior under adaptive quantum threats within the national scientific community. A significant number of review and theoretical works are characteristic, yet there is a shortage of systematized adversary models, formal security proofs, and experimentally verified results in complex network contexts. This aligns with global publication trends, where the issues of adversary adaptability and composability require further development and deeper formal conceptualization.

Overall, the analysis of scientific research confirms that the issue of quantum-adaptive security for hybrid protocols remains one of the most promising yet underdeveloped research areas, despite significant progress in the standardization of post-quantum algorithms and the development of practical hybrid schemes for data protection in future networks.

The aim and objectives of the study

The objective of this article is to develop comprehensive methods for ensuring the quantum-adaptive security of hybrid cryptographic protocols in 5G, 6G, and IoT networks, enabling them to withstand both current and prospective quantum threats.

The work is grounded in the formalization of adaptive adversary behavior and the assessment of protocol resilience under dynamic quantum influence conditions, providing a scientifically substantiated framework for the practical implementation of defense mechanisms.

A review of existing hybrid protocols identifies critical vulnerabilities and gaps in composability and multi-session security that limit the effectiveness of contemporary solutions. This underscores the necessity of developing a formalized quantum-adaptive adversary model that accounts for the real-time dynamic evolution of attacker actions and enables accurate modeling of their impact on protocols.

This research presents an integrated approach to evaluating protocol resilience, factoring in the combination of classical and post-quantum components, the effect of adversary adaptability, and compositional complexity. The proposed methodology ensures comprehensive risk control and establishes the scientific and technical foundation for constructing robust hybrid protocols. Such solutions are capable of effectively countering quantum-adaptive threats, integrating into modern IoT infrastructures, and maintaining high security levels in multi-layered networks.

Materials and methods

A system analysis of hybrid cryptographic protocols reveals that combining classical algorithms with post-quantum schemes ensures both high performance and resilience to quantum attacks. In modern 5G, 6G, and IoT networks, hybrid solutions are integrated into TLS, VPN, and IPsec protocols, providing backward compatibility and reducing the need for large-scale infrastructure modernization. This approach maintains session stability and prevents security degradation during the transition to new algorithmic standards.

Particular attention is paid to modeling the behavior of a quantum-equipped adversary capable of executing superposition queries, combining classical and quantum methods, and adaptively modifying attack strategies based on obtained results. The Quantum-Accessible Random Oracle Model (QROM) allows for the formalization of such scenarios by integrating the adversary's capabilities into the protocol's security proofs and providing a mathematical justification for resilience [10]. This approach paves the way for building robust hybrid protocols capable of countering complex quantum-adaptive threats in real-time.

The analysis of established solutions indicates their sufficiently high resilience to standard quantum attacks, including Shor's and Grover's algorithms. At the same time, critical gaps persist in multi-session security and composability, which limits the effectiveness of protocols in multi-user and multi-layer networks. Dynamic parameter management becomes a decisive factor, where adaptive adjustment of key lengths, selection of cryptographic primitives, and algorithmic configurations based on risk assessment ensure protocol resilience even in complex environments with high network activity and a powerful quantum adversary.

An integrated approach to security assessment allows for the combination of classical and post-quantum components while accounting for the effect of attack adaptability and the complexity of protocol composition [11]. Such a comprehensive methodology forms the basis for creating next-generation hybrid protocols capable of effectively protecting information flows, integrating into modern telecommunications and IoT infrastructures, maintaining high performance, and withstanding quantum-adaptive threats.

It should be noted that while existing hybrid protocols provide basic resilience, they require further development in the areas of adversary adaptability, composability, multi-session security, and integral metrics for resilience assessment. These aspects define key scientific gaps and outline promising directions for further research in the field of quantum-adaptive security.

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

Under these conditions, the study of modern hybrid protocols reveals significant deficiencies in ensuring composability. Specifically, most solutions are tested only in isolated scenarios, which ignores the interactions between different protocol components. This leads to the emergence of potential indirect attack vectors, where the compromise of a single session affects the security of others. Such threats are particularly relevant in multi-user 5G and 6G environments, where hundreds of thousands of active sessions operate simultaneously. Consequently, the lack of formalized composable models complicates the construction of security proofs and creates “dark zones” that can be exploited by a quantum-adaptive adversary to optimize attacks.

When considering the multi-session aspects of modern hybrid protocols, it is notable that security is often limited to certificates and the handshake phases of an individual session. Such an approach fails to account for an adaptive adversary capable of aggregating data from multiple sessions to perform effective cryptanalysis. Scenarios of this type fall outside the scope of traditional security proofs and create additional attack vectors. Adversary adaptability allows for optimized key searching, a reduction in the entropy of session parameters, and the potential undermining of protocol resilience in multi-session environments.

Researching the integration of post-quantum algorithms with classical primitives leads to the conclusion that it also entails significant technical limitations [12]. Classical protocols, such as TLS 1.3, have established stages for key exchange and authentication. Incorporating PQC components for instance, CRYSTALS-Kyber for key exchange or CRYSTALS-Dilithium for digital signatures, sometimes results in alterations to the message-flow. Such changes violate the underlying assumptions of security proofs that rely on a specific handshake structure. Consequently, an adaptive adversary can exploit these modifications for downgrade attacks or to optimize attacks within QROM scenarios.

To provide a clear comparison of hybrid protocol effectiveness in the context of composability, multi-session security, and the integration of PQC with classical algorithms, Table 1 is presented. It demonstrates the strengths and weaknesses of various implementations across different network environments and highlights key gaps that require further research.

Comparative data highlight that even in the most common hybrid implementations, gaps remain in multi-session security and composability. Under these conditions, the integration of post-quantum schemes into classical protocols requires a formalized approach that accounts for adversary adaptability and the complexity of multi-session scenarios.

The results of such an approach form the basis for improving the analysis and design methods of next-generation hybrid protocols; however, achieving practical reliability necessitates a comprehensive evaluation of existing gaps. Simultaneously, a systematic and clear identification of weaknesses in implementation and security mechanisms is an indispensable prerequisite for the effective development of hybrid protocols. A multi-level analysis allows for the timely detection of deficiencies in composability properties, multi-session protection mechanisms, and the integration processes of post-quantum and classical components. Consequently, these aspects become critically important in the distributed and highly dynamic environments of 5G/6G and IoT, where scalability, session parallelism, and device heterogeneity significantly increase the requirements for the consistency and integrity of the cryptographic architecture.

Under these circumstances, the technical integration of post-quantum mechanisms reveals several significant architectural features. In particular, the implementation of CRYSTALS-Kyber in TLS 1.3 is carried out by extending the key agreement procedure and adding corresponding key-exchange messages [13]. Such a modification alters the protocol's message flow, affecting not only the temporal structure of the handshake but also the formal construction of the security proof, as new dependencies between exchange stages and additional assumptions regarding the adversary model emerge.

Similar features are observed in other network protocols. In the IPsec architecture, the Security Association

Table 1. Evaluating hybrid cryptographic protocols: Composability, multi-session security, and PQC-classical integration

Protocol	Composability	Multi-session Security	PQC Integration
TLS 1.3 + Kyber	Limited; does not account for multi-session interactions	Weak; lacks adaptive mechanisms	Partial; handshake changes may violate security proof
IPsec + PQC	Stable within a single SA, but not for multi-SA	SA support; lacks assessment of adaptive adversary behavior	PQC integrated locally; composability not proven
SSH + PQC	Individual sessions; composability is absent	Medium; local session security	Key exchange integrated; lacks adaptive assessment
IKEv2 + Kyber	Unstable in multi-level networks	Does not cover QROM scenarios	PQC added; composability not formally proven

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

(SA) mechanism ensures the preservation of the cryptographic state between sessions, which increases the efficiency of reconnections. However, this model does not provide a formalized assessment of adversary adaptability, where an attacker could simultaneously operate multiple SAs and exploit cross-session correlations. In the absence of clear compositional guarantees, this creates potential cross-session attack vectors [14].

Similar limitations are observed in SSH with integrated PQC key exchanges, as well as in IKEv2, where the compromise of a single Security Association (SA) or an individual session could theoretically have an indirect impact on other active connections. Collectively, such scenarios demonstrate practical attack vectors in multi-session environments and underscore the necessity of formally accounting for the adversary's adaptive multi-channel activity within an integrated security model.

Within the post-quantum paradigm, the analysis of adversary models focuses on their capability to perform superposition queries to cryptographic oracles in the Quantum Random Oracle Model (QROM). This characteristic fundamentally expands the set of admissible attacks compared to the classical computational model [15], as the adversary gains the ability to exploit quantum parallelism while interacting with cryptographic primitives.

This factor leads to additional reduction losses during the mathematical justification of security and significantly complicates the construction of formally rigorous security proofs, particularly under conditions of compositional and multi-session protocol application.

An evaluation of existing protocols, specifically CRYSTALS-Kyber and CRYSTALS-Dilithium, reveals that they are primarily oriented toward static or limited-adaptive models and do not fully account for composable scenarios involving numerous parallel sessions. Consequently, a gap emerges between the local reductionist security of individual primitives and the integral security of the protocol within a systemic context.

Such limitations lead to potential deficiencies in “standoff security”, where an adversary can correlate inter-session leakage to refine hypotheses regarding secret parameters. These scenarios transcend classical security notions, such as IND-CCA and UCE, necessitating the expansion of models to incorporate quantum-adaptive multi-session adversary behavior.

When assessing multi-session environments, it is observed that the compromise of a single TLS 1.3 session or an IPsec Security Association (SA) can reduce the entropy of other sessions, creating potential lateral impact vectors. In the case of SSH with PQC key exchanges, the compromise of a private key on one station could allow for the monitoring of other sessions' behavior. Similarly, in IKEv2 with PQC integration, the compromise of a single SA increases the risk of weakening the resilience of adjacent Security Associations. These risks are especially critical for 5G/6G and IoT infrastructures, characterized by a massive number of simultaneous sessions and connected devices [16].

Regarding the resilience assessment of hybrid protocols, a critical gap is the absence of integral metrics. Current approaches are limited to measuring the local security of individual components and fail to analyze the interdependencies between sessions and handshake stages. This results in a “dark zone” between the nominal guarantees of PQC and the practical implementation of hybrid cryptographic stacks.

In conclusion, the identified gaps define three key directions for further research. The first area focuses on the development of composability-oriented security models for multi-level scenarios and multi-session adversary influence. The second area involves constructing security proof frameworks that account for adaptive adversary behavior within the Quantum Random Oracle Model (QROM). The third area concerns the development of integral metrics for the quantitative assessment of the interplay between classical and post-quantum mechanisms in hybrid protocols.

Consequently, a comprehensive resolution of these aspects establishes the foundation for building next-generation hybrid protocols. These protocols will ensure guaranteed security under composability constraints, operate efficiently in multi-session environments, and withstand adaptive quantum threats factors that are of critical importance for modern 5G/6G networks and scalable IoT infrastructures.

1. Conceptual Foundations and Systemic Problem Statement. The rapid integration of post-quantum primitives into classical transport and network layer security protocols objectively necessitates a transition from static security models to dynamic multi-session formalizations. In such an environment, the adversary ceases to be an abstract algorithmic entity and acquires the characteristics of an adaptive control system capable of modifying its strategy in real-time.

In view of this, it is appropriate to consider the protocol as an open quantum-classical system operating in a common Hilbert space

$$\mathcal{H} = \mathcal{H}_P \otimes \mathcal{H}_A \otimes \mathcal{H}_E , \quad (1)$$

where $\mathcal{H}_P$ is the subspace of honest participants, $\mathcal{H}_A$ is the internal information space of the adversary, and $\mathcal{H}_E$ is the interaction environment (network, noise effects, infrastructural states).

Thus, security is interpreted not as a property of an individual algorithm, but as a property of the system's dynamics as a whole.

The state of the system is described by the density operator

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

$$\rho(t) \in \mathcal{D}(\mathcal{H}), \quad \rho(t) \geq 0, \quad Tr(\rho(t)) = 1. \tag{2}$$

The presented ensures a universal description for both classical and quantum components of the protocol.

2. Operator Interpretation of the Protocol and Composability. Each round of interaction is modeled as a completely positive trace-preserving (CPTP) channel

$$\Phi_i : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H}), \tag{3}$$

reflecting the system's informational transition between protocol steps.

Furthermore, multi-session execution is formalized by the composition:

$$\Phi^{(n)} = \Phi_n \circ \cdots \circ \Phi_1, \quad \rho_n = \Phi^{(n)}(\rho_0). \tag{4}$$

In such an environment, it is fundamentally important that composability is interpreted as the resilience of this composition to external interference.

Accordingly, compositional security is defined through a distinguishability metric:

$$\Delta = \| \Phi_{real} - \Phi_{ideal} \|_\diamond . \tag{5}$$

Under these circumstances, the diamond norm is defined as

$$\| \Lambda \|_\diamond = \sup_{\rho_{AR}} \| (\Lambda \otimes \mathbb{I}_R)(\rho_{AR}) \|_1 , \tag{6}$$

guaranteeing that arbitrary correlations of the adversary with an external reference space are taken into account.

Thus, the protocol ε is compositionally secure if:

$$\Delta \leq \varepsilon . \tag{7}$$

The aforementioned formalizes the principle that the protocol maintains its resilience and does not become noticeably more vulnerable, regardless of the integration context.

Furthermore, in the multi-session mode:

$$\| \Phi_{real}^{(n)} - \Phi_{ideal}^{(n)} \|_\diamond \leq n\varepsilon . \tag{8}$$

Thus, composability provides metric control over risk accumulation.

3. Hybridity as a Structural Property of the Channel. The hybrid nature of the protocol implies that the information channel Φ_i consists of two subchannels:

$$\mathcal{K}_{hyb} = \mathcal{K}_{cl} \| \mathcal{K}_{pq} . \tag{9}$$

Therefore, the session key is formed as $K = KDF(\mathcal{K}_{cl} \| \mathcal{K}_{pq})$, which logically corresponds to the principle of cryptographic aggregation.

However, in the quantum adversary model, superposition access to oracles is permitted:

$$\sum_x \alpha_x |x\rangle |0\rangle \to \sum_x \alpha_x |x\rangle |f(x)\rangle, \tag{10}$$

leading to an estimation of the quadratic amplification of the reduction loss:

$$\varepsilon_{hyb} \leq \varepsilon_{cl} + q^2 \varepsilon_{pq} . \tag{11}$$

Thus, the aforementioned implies that hybridity is not a linear superposition of securities but is determined by the nature of the adversary's access.

4. Dynamic Model of a Quantum-Adaptive Adversary. The key element is the formalization of adaptability. It is proposed to describe the adversary's state using the operator:

$$\rho_A(t) \in \mathcal{D}(\mathcal{H}_A) . \tag{12}$$

Furthermore, its evolution is governed by a controlled Lindblad generator:

$$\frac{d\rho_A}{dt} = \mathcal{L}_{s(t),u_{A(t)}}(\rho_A) , \tag{13}$$

where $s(t)$ is the protocol state, $u_{A(t)}$ is the adversary strategy, $\mathcal{L}$ is the Lindblad linear superoperator.

The payoff functional is represented as:

$$J_A = \int_0^T I(Secret; View_A(t))dt . \tag{14}$$

This implies that the adversary optimizes information leakage. The optimal strategy will correspond to:

$$u_A^*(t) = arg \max_{u_A} J_A . \tag{15}$$

Thus, the adversary is modeled as a controlled quantum system with adaptive control.

5. Minimax Security Architecture. Protocol design is formulated as a differential game problem:

$$\min_{\Pi} \max_{u_A} \| \Phi_{\Pi,u_A} - \Phi_{ideal} \|_\diamond . \tag{16}$$

This means that the protocol must minimize the adversary's maximum information gain. Under such conditions, resilience is achieved if the minimax condition for the payoff functional is satisfied

$$\sup_{u_A} \| \Phi_{\Pi,u_A} - \Phi_{ideal} \|_\diamond \leq \varepsilon . \tag{17}$$

Thus, security is interpreted as the invariance of the channel to adaptive control.

6. Systemic Integration of Three Areas. Based on the results of the considered research sequence, covering the properties of composability, hybrid cryptographic structure, and the dynamic adaptability of the adversary, there arises an objective necessity for their systemic alignment within a single formalized model (Fig. 1).

At this stage, it is fundamentally important to transition from local mathematical descriptions of individual mechanisms to a systemic interpretation. Within this framework, protocol security is viewed as an integral property of interacting subsystems [17]. This approach corresponds to the modern paradigm of universally composable security, formulated within the Universal Composability (UC) framework [18], where each cryptographic primitive is analyzed not in isolation, but as an element of a more complex compositional structure.

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

From a methodological standpoint, each of the three areas fulfills a clearly defined functional role within the overall model architecture.

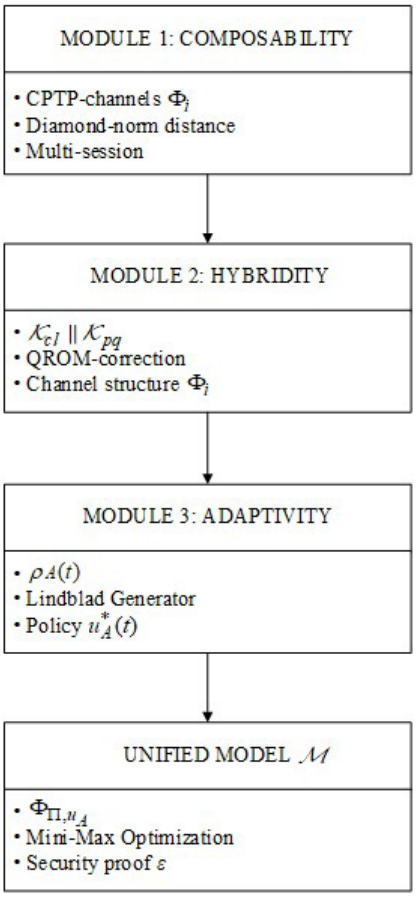

Fig. 1. Structural block diagram of the integration of composability, hybridity, and adaptability into a unified model

First, composability provides metric control over the correctness of protocol integration into an arbitrary external environment. Formally, this is implemented through constraints on the distinguishability of real and ideal channels, defined by an upper bound in the diamond norm. Thus, a global deviation metric is formed, ensuring that any system expansion or the addition of new sessions does not lead to uncontrolled error accumulation. In multi-session mode, the compositional property ensures the additivity or subadditivity of the security parameter, allowing for the establishment of clear upper bounds on the total risk of compromise [19]. Consequently, composability acts as an external stabilizing mechanism that defines the global boundary for permissible system deviations from the ideal specification.

Secondly, hybridity defines the internal structural architecture of channel Φ_i, as it is the combination of classical and post-quantum primitives that shapes the informational state space, the structure of cryptographic dependencies, and the reductionist security bounds. The integration of classical schemes with post-quantum algorithms creates a multi-layered cryptographic mechanism where the security parameter is determined not only by the resilience of individual primitives but also by the nature of their interaction. In the Quantum Random Oracle Model (QROM), reductionist estimates are modified to account for QROM corrections, which directly influence the magnitude of the permissible deviation between real and simulated environments. Thus, the hybrid block defines the internal geometry of the attack space and forms the structural foundation of the entire security system.

Thirdly, adaptability introduces temporal and strategic variability, transforming the adversary into a controlled quantum system with dynamic control. In this context, the adversary is modeled as a system with variable parameters, capable of adjusting its strategy based on intermediate results of interaction with the protocol. Accordingly, the channel Φ_{Π,u_A} acquires a parametric dependence on the control strategy, which shifts security analysis into the domain of dynamic systems and optimal control. This formulation allows for accounting for scenarios of sequential or conditional information disclosure, multi-step adaptive oracle queries, and the strategic optimization of attacks. As a result, protocol security is interpreted as the resilience of the system to all permissible controlled trajectories of the adversary.

Ultimately, it is the integration of these three mentioned areas that forms the hierarchical security structure. Composability establishes the global metric framework and guarantees the invariance of properties during composition. Hybridity defines the internal structural organization of the cryptographic channel and its reductionist bounds. Adaptability accounts for the temporal evolution of the attacking strategy and the strategic optimization of the adversary.

In aggregate, this enables a transition from the static analysis of individual primitives to a systemic model, where security is viewed as an integral function of structural, metric, and dynamic parameters.

Thus, the coordinated combination of composability, hybrid architecture, and adaptive adversary dynamics forms a closed formalized construction $\mathcal{M} = (\mathcal{H}, \Phi^{(n)}, \mathcal{K}_{hyb}, \mathcal{L}_{adv})$, ensuring the integrity, scalability, and mathematically grounded resilience of the protocol within a classical-quantum computing environment.

In performing a quantitative assessment of security metrics, it is proposed to consider a typical hybrid session key establishment protocol. In this protocol, a classical exchange mechanism based on Elliptic Curve Diffie-Hellman (P-256 curve) is combined with the

ISSN 2786-9024

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359309

post-quantum key encapsulation mechanism CRYSTALS-Kyber (Kyber-768 parameter level) [20]. Such an architecture is representative of modern TLS-like hybrid implementations focused on long-term cryptographic resilience.

First and foremost, it is necessary to formalize the initial assumptions. Let the system serve $N = 10^6$ independent sessions during a specific analyzed period, and let the adversary possess the capability to make adaptive quantum queries to oracles in the QROM model. Under these conditions, the integral assessment must account for four interrelated factors: (1) classical resilience, (2) post-quantum resilience, (3) compositional error accumulation, (4) adaptive reduction loss.

In the first stage, the classical component is evaluated. For ECDH P-256, the nominal security level is approximately 128 bits, which is equivalent to a successful attack probability of $\varepsilon_{cl} \approx 2^{-128} \approx 2.9 \cdot 10^{-39}$.

However, in multi-session mode, additive risk accumulation occurs. Applying the union bound, we obtain $\varepsilon_{cl,total} \le N \cdot \varepsilon_{cl}$, $N = 10^6$, $\varepsilon_{cl,total} \le 10^6 \cdot 2^{-128}$, $\varepsilon_{cl,total} \approx 2^{-108}$. Thus, even without considering other factors, the effective level of classical resilience is reduced to approximately 108 bits.

In the second stage, the post-quantum component is evaluated analogously. For Kyber-768, the claimed quantum security level corresponds to approximately 128 bits, yielding $\varepsilon_{pq} \approx 2^{-128}$. Taking into account the same 10^6 sessions, we obtain: $\varepsilon_{pq,total} \le N \cdot \varepsilon_{pq}$, . $\varepsilon_{pq,total} \le 10^6 \cdot 2^{-128}$, $\varepsilon_{struct} \le 2 \cdot 2^{-108}$, $\varepsilon_{pq,total} \approx 2^{-108}$.

Consequently, both classical and post-quantum components exhibit the same order of effective security degradation under multi-session conditions.

The next step is the structural integration of the hybrid scheme. Under the assumption of independent mechanisms, protocol compromise can occur via the breach of either component; thus, the integral structural bound is defined as $\varepsilon_{struct} \le \varepsilon_{cl,total} + \varepsilon_{pq,total}$, $\varepsilon_{struct} \approx 2^{-107}$.

Thus, hybridity ensures that the security level remains above 100 bits, yet it does not compensate for the losses resulting from system scaling.

Further analysis requires accounting for compositional complexity. Let the protocol consist of $k = 5$ cryptographically significant submodules. Within the framework of the Universal Composability (UC) model, the global distinguishability bound increases proportionally to the number of compositional elements, yielding: $\varepsilon_{comp} \le k \cdot \varepsilon_{struct}$, $\varepsilon_{comp} \le 5 \cdot 2^{-107}$, $\varepsilon_{comp} \approx 2^{-105}$.

Thus, the compositional architecture leads to an additional reduction in effective resilience by approximately two bits.

Finally, it is fundamentally important to account for the adversary's adaptability. Let the adversary make quantum queries to the oracles. In the QROM, the reduction loss scales as $\sqrt{q} = 2^{16}$. Accordingly, $\varepsilon_{adapt} \le \sqrt{q} \cdot \varepsilon_{comp}$, $\varepsilon_{adapt} \le 2^{16} \cdot 2^{-105}$, $\varepsilon_{adapt} \approx 2^{-89}$.

The obtained result demonstrates that the adaptive quantum factor constitutes the dominant contribution to the degradation of the integral security parameter.

Summarizing the presented stages, it should be noted that the integral resilience metric takes the value $S_{total} \approx 2^{-89}$, which is thus equivalent to approximately 89 bits of effective security. At the same time, the nominal 128 bits declared for individual cryptographic primitives are transformed into a significantly lower integral indicator in a real multi-session, compositional, and adaptive model.

Thus, the sequential transition from local reductionist assessments to a systemic integral metric allows for the identification of critical sources of resilience degradation and provides an engineering-correct basis for selecting protocol parameters [21]. Such a multi-level evaluation methodology is a necessary condition for designing cryptographic systems oriented toward functioning in a classical-quantum computing environment with a high level of compositional complexity.

Results

The conducted system analysis of modern hybrid cryptographic protocols has identified key aspects for enhancing their resilience within a quantum-adaptive environment. It was established that composability, multi-session security, and the integration of classical and post-quantum components remain critical risk areas, particularly in multi-layer and multi-user infrastructures such as 5G/6G and scalable IoT systems. It was found that the compromise of a single session or Security Association (SA) can degrade the entropy of adjacent elements, creating potential secondary attack vectors. Such scenarios transcend classical security notions and necessitate the implementation of integrated methods for evaluating and controlling protocol resilience.

Further analysis of adversary models in the Quantum Random Oracle Model (QROM) highlighted the need to account for the adaptive behavior of attackers capable of performing superposition queries to oracles and correlating leakage across sessions. This factor introduces additional reduction losses and significantly complicates the construction of formally rigorous security proofs, especially in composable and multi-session scenarios. In this context, the development of a formalized Quantum-Adaptive Adversary (QAA) model serves as a key step, enabling the integration of three domains composability control, hybridity of cryptographic primitives, and dynamic adversary adaptability into a single systemic framework.

The integration of these aspects paves the way for building next-generation hybrid protocols capable of maintaining resilience in multi-session environments, adapting to changes in adversary behavior in real-time, and guaranteeing security in composable scenarios.

A comprehensive approach allows not only for the formalization of protocol component interdependencies but also for the quantitative assessment of their interaction through integral metrics that account for classical and post-quantum elements, the effect of adversary adaptability, and compositional complexity.

Future research perspectives include several interconnected directions:

1. Development of integral resilience metrics that consider multi-session effects and composable influence to improve the accuracy of protocol analysis and optimization.

2. Enhancement of proof constructions in the QROM, accounting for dynamic adversary adaptability and multi-level scenarios to ensure formal security clarity at the system level.

3. Research into dynamic protocol parameter management strategies, including key lengths and cryptographic primitive configurations, to establish a basis for building effective adaptive protocols in environments with high network activity and powerful quantum attacks.

Thus, a comprehensive integrated approach to the analysis, modeling, and resilience evaluation of hybrid cryptographic protocols opens opportunities for creating reliable, scalable, and adaptive security systems capable of countering modern quantum threats and ensuring the effective operation of next-generation networks.

Conflict of Interest

The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship-related, or any other type of conflict that could have influenced the research or its results presented in this article.

Funding

This research was conducted without any financial support.

Data Availability

This manuscript has no associated datasets.

BIBLIOGRAPHY

[1] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, "Post-quantum cryptography and quantum-safe security: A comprehensive survey," ACM Comput. Surv., vol. 1, no. 1, Art. 1, pp. 1–33, Oct. 2025. DOI: 10.48550/arXiv.2510.10436.

[2] National Institute of Standards and Technology, "Post-quantum cryptography Standardization." csrc.nist.gov. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[3] Y. Zhyvylo and Y. Kuchma, "Mathematical modeling of intellectual and cryptographic protection of authentication keys," ITS, vol. 13, no. 2, pp. 162–177, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344591.

[4] A. Sanz et al., "Extending Quantum-Safe Communications to Real-World Networks: An Adaptive Security Framework," arXiv preprint arXiv:2511.22416, 2025. [Online]. URL: https://arxiv.org/html/2511.22416v1.

[5] A. Raj and V. Balachandran, "A Hybrid Encryption Framework Combining Classical, Post-Quantum, and QKD Methods," in Applied Cryptography and Network Security Workshops (ACNS 2025), M. Manulis, Ed. Cham, Switzerland: Springer, 2026, pp. 197–201. DOI: 10.1007/978-3-032-01823-6_14.

[6] Y. Ko, I. W. A. J. Pawana, and I. You, "5g-aka-hpqc: Hybrid post-quantum cryptography protocol for quantum-resilient 5g primary authentication with forward secrecy," arXiv preprint arXiv:2502.02851, pp. 1–15, 2025. DOI: 10.48550/arXiv.2502.02851.

[7] A. Khutsaeva, A. Leevik, and S. Bezzateev, "A Survey of Post-Quantum Oblivious Protocols," Cryptography, vol. 9, no. 4, p. 62, 2025. DOI: 10.3390/cryptography9040062.

[8] S. Amador, C. Pardo, and R. Mazo, "Cybersecurity of Cyber-Physical Systems in the Quantum Era: A Systematic Literature Review-Based Approach," Future Internet, vol. 18, no. 3, p. 125, 2026. DOI: 10.3390/fi18030125.

[9] T. Fesenko and Y. Kalashnikova, "Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection," ITS, vol. 13, no. 2, pp. 178–191, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344592.

[10] A. Shyshatskyi, Ed., INFORMATION AND CONTROL SYSTEMS: MODELLING AND OPTIMIZATIONS. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024. DOI: 10.15587/978-617-8360-04-7.

[11] T. Fesenko and Y. Kalashnikova, "Predicate logic as the basis for knowledge formalization and logical inference in artificial intelligence systems for cybersecurity," Science and Technology Today. Series: Engineering, no. 1 (55), pp. 1877–1891, Feb. 2026. DOI: 10.52058/2786-6025-2026-1(55)-1877-1891.

[12] J. Mijalkovic and A. Spognardi, "Reducing the False Negative Rate in Deep Learning Based Network Intrusion Detection Systems," Algorithms, vol. 15, no. 8, p. 258, 2022. DOI: 10.3390/a15080258.

[13] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[14] M. Koval et al., "Improvement of complex resource management of special-purpose communication systems," Eastern-European Journal of Enterprise Technologies, vol. 5, no. 9 (119), pp. 34–44, 2022. DOI: 10.15587/1729-4061.2022.266009.

[15] S. Kashkevich et al., "The development of management methods based on bio-inspired algorithms," in Information and control systems: modelling and optimizations, A. Shyshatskyi, Ed. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024, pp. 35–69. DOI: 10.15587/978-617-8360-04-7.

[16] A. Shyshatskyi et al., “Development of a polymodel complex of information systems resource management,” Eastern-European Journal of Enterprise Technologies, vol. 4, no. 4 (136), pp. 58–72, 2025. DOI: 10.15587/1729-4061.2025.335688.
[17] P. Pradeep and K. Kant, “Conflict Detection and Resolution in IoT Systems: A Survey,” IoT, vol. 3, no. 1, pp. 191–218, 2022. DOI: 10.3390/iot3010012.
[18] Y. Zdorenko, A. Yanko, M. Myziura, and N. Fesokha, “Development of a fuzzy risk assessment model for information security management,” TAPR, vol. 4, no. 2 (84), pp. 71–79, Aug. 2025. DOI: 10.15587/2706-5448.2025.334954.
[19] Y. O. Zhyvylo, Y. V. Kuchma, and T. M. Fesenko, “Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures,” in Modern aspects of science: LXII. Part of the international collective monograph. Czech Republic: International Economic Institute s.r.o., 2025, pp. 407–456. DOI: 10.52058/62-2025.
[20] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.
[21] Т. Фесенко та Ю. Калашнікова, «Федеративна GNN-XAI модель прогнозу компрометації облікових записів у ZERO TRUST-середовищі», Кібербезпека: освіта, наука, техніка, вип. 3, № 31, с. 602–619, груд. 2025. DOI: 10.28925/2663-4023.2025.31.1049.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КВАНТОВО-АДАПТИВНОЇ БЕЗПЕКИ ГІБРИДНИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ У МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

Тетяна Фесенко, Аліна Янко, Владислава Магалецька, Максим Плахтій

У статті досліджуються методи забезпечення квантово-адаптивної безпеки гібридних криптографічних протоколів у мережах наступного покоління. Мережі 5G/6G та IoT потребують інтеграції класичних і постквантових алгоритмів. Однак стандартні протоколи, що поєднують ECDH з CRYSTALS-Kyber або CRYSTALS-Dilithium, потребують формальної оцінки безпеки. Сучасні підходи переважно розглядають неадаптивних квантових опонентів, що обмежує їхнє практичне застосування в багатосесійних і динамічних середовищах.

У роботі запропоновано модель квантово-адаптивного зловмисника. Ця модель інтегрує класичні та квантові ресурси зловмисника, стратегію адаптивної атаки та квантовий оракул. Це дає змогу формалізувати суперпозиційні запити та багатоступеневу взаємодію з протоколом. Представлено математичну модель гібридного протоколу рукостискання, де сесійний ключ формується шляхом поєднання класичних і постквантових компонентів через функцію формування ключа (KDF). Виведено верхню межу переваги зловмисника, що враховує як класичну, так і постквантову складову протоколу.

Для підвищення стійкості запропоновано три основні методи. Перший – фіксація параметрів протоколу із захистом від пониження рівня безпеки та криптографічним підтвердженням. Другий – динамічне управління ключовими параметрами та криптографічними примітивами на основі інтегральної функції ризику, яка враховує квантові ресурси противника, навантаження на мережу й активність атак. Третій – композиційна верифікація протоколів з урахуванням багатосесійних і багаторівневих фаз рукостискання, що дає змогу формалізувати композиційність та оцінити багаторівневу стійкість. Запропоновано інтегральну метрику квантово-адаптивної стійкості, що враховує безпеку, складність та адаптивність. Результати створюють наукове підґрунтя для аналізу ризиків harvest-now, decrypt-later.

Ключові слова: *квантово-адаптивна безпека, гібридні криптографічні протоколи, постквантова криптографія, Multi-session security, QAA-модель, QROM.*

REFERENCES

[1] G. Chhetri, S. Somvanshi, P. Hebli, S. Brotee, and S. Das, “Post-quantum cryptography and quantum-safe security: A comprehensive survey,” ACM Comput. Surv., vol. 1, no. 1, Art. 1, pp. 1–33, Oct. 2025. DOI: 10.48550/arXiv.2510.10436.
[2] National Institute of Standards and Technology, “Post-quantum cryptography Standardization.” csrc.nist.gov. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.
[3] Y. Zhyvylo and Y. Kuchma, “Mathematical modeling of intellectual and cryptographic protection of authentication keys,” ITS, vol. 13, no. 2, pp. 162–177, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344591.
[4] A. Sanz et al., “Extending Quantum-Safe Communications to Real-World Networks: An Adaptive Security Framework,” arXiv preprint arXiv:2511.22416, 2025. [Online]. URL: https://arxiv.org/html/2511.22416v1.
[5] A. Raj and V. Balachandran, “A Hybrid Encryption Framework Combining Classical, Post-Quantum, and QKD Methods,” in Applied Cryptography and Network Security Workshops (ACNS 2025), M. Manulis, Ed. Cham, Switzerland: Springer, 2026, pp. 197–201. DOI: 10.1007/978-3-032-01823-6_14.
[6] Y. Ko, I. W. A. J. Pawana, and I. You, “5g-aka-hpqc: Hybrid post-quantum cryptography protocol for quantum-resilient 5g primary authentication with forward

secrecy,” arXiv preprint arXiv:2502.02851, pp. 1–15, 2025. DOI: 10.48550/arXiv.2502.02851.

[7] A. Khutsaeva, A. Leevik, and S. Bezzateev, “A Survey of Post-Quantum Oblivious Protocols,” Cryptography, vol. 9, no. 4, p. 62, 2025. DOI: 10.3390/cryptography9040062.

[8] S. Amador, C. Pardo, and R. Mazo, “Cybersecurity of Cyber-Physical Systems in the Quantum Era: A Systematic Literature Review-Based Approach,” Future Internet, vol. 18, no. 3, p. 125, 2026. DOI: 10.3390/fi18030125.

[9] T. Fesenko and Y. Kalashnikova, “Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection,” ITS, vol. 13, no. 2, pp. 178–191, Nov. 2025. DOI: 10.20535/2411-1031.2025.13.2.344592.

[10] A. Shyshatskyi, Ed., INFORMATION AND CONTROL SYSTEMS: MODELLING AND OPTIMIZATIONS. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024. DOI: 10.15587/978-617-8360-04-7.

[11] T. Fesenko and Y. Kalashnikova, “Predicate logic as the basis for knowledge formalization and logical inference in artificial intelligence systems for cybersecurity,” Science and Technology Today. Series: Engineering, no. 1 (55), pp. 1877–1891, Feb. 2026. DOI: 10.52058/2786-6025-2026-1(55)-1877-1891.

[12] J. Mijalkovic and A. Spognardi, “Reducing the False Negative Rate in Deep Learning Based Network Intrusion Detection Systems,” Algorithms, vol. 15, no. 8, p. 258, 2022. DOI: 10.3390/a15080258.

[13] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[14] M. Koval et al., “Improvement of complex resource management of special-purpose communication systems,” Eastern-European Journal of Enterprise Technologies, vol. 5, no. 9 (119), pp. 34–44, 2022. DOI: 10.15587/1729-4061.2022.266009.

[15] S. Kashkevich et al., “The development of management methods based on bio-inspired algorithms,” in Information and control systems: modelling and optimizations, A. Shyshatskyi, Ed. Kharkiv, Ukraine: TECHNOLOGY CENTER PC, 2024, pp. 35–69. DOI: 10.15587/978-617-8360-04-7.

[16] A. Shyshatskyi et al., “Development of a polymodel complex of information systems resource management,” Eastern-European Journal of Enterprise Technologies, vol. 4, no. 4 (136), pp. 58–72, 2025. DOI: 10.15587/1729-4061.2025.335688.

[17] P. Pradeep and K. Kant, “Conflict Detection and Resolution in IoT Systems: A Survey,” IoT, vol. 3, no. 1, pp. 191–218, 2022. DOI: 10.3390/iot3010012.

[18] Y. Zdorenko, A. Yanko, M. Myziura, and N. Fesokha, “Development of a fuzzy risk assessment model for information security management,” TAPR, vol. 4, no. 2 (84), pp. 71–79, Aug. 2025. DOI: 10.15587/2706-5448.2025.334954.

[19] Y. O. Zhyvylo, Y. V. Kuchma, and T. M. Fesenko, “Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures,” in Modern aspects of science: LXII. Part of the international collective monograph. Czech Republic: International Economic Institute s.r.o., 2025, pp. 407–456. DOI: 10.52058/62-2025.

[20] Information security, cybersecurity and privacy protection – A framework for identity management – Part 1: Core concepts and terminology, ISO/IEC Standard 24760-1:2025, 3rd ed., 2025.

[21] T. Fesenko and Y. Kalashnikova, “federative GNN-XAI model for predicting compromise of account records in ZERO TRUST environment,” Cybersecurity: Education, Science, Technique, vol. 3, no. 31, pp. 602–619, Dec. 2025. DOI: 10.28925/2663-4023.2025.31.1049.

Дата першого надходження статті до видання: 18.02.2026
Дата прийняття статті до друку після рецензування: 11.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Штучний інтелект

УДК 004.8:37.013:004.056

АЛГОРИТМ ОЦІНЮВАННЯ ДОСТОВІРНОСТІ ВІДПОВІДЕЙ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ СТВОРЕННІ НАВЧАЛЬНОГО КОНТЕНТУ

Н.О. Маслова[1,2], О.М. Любименко[2,3]
[1]Lviv State University of Life Safety, Lviv, Ukraine
[2]Donetsk National Technical University, Drohobych, Ukraine
[3]Lutsk National Technical University, Lutsk, Ukraine
ORCID https://orcid.org/0000-0002-9078-0973
ORCID https://orcid.org/0000-0002-5935-6891
E-mail: nataliia.maslova@donntu.edu.ua, olena.liubymenko@donntu.edu.ua

АНОТАЦІЯ

У роботі проаналізовано ризики, пов’язані з коректністю та достовірністю навчального контенту, створеного за допомогою інструментів штучного інтелекту. Інтелектуальні інструменти на основі штучного інтелекту сприяють автоматизації процесу розроблення інтерактивних навчальних матеріалів, підвищенню рівня персоналізації навчання та оптимізації аналізу результатів освітньої діяльності. Водночас впровадження технологій штучного інтелекту в освітнє середовище супроводжується появою нових цифрових ризиків, зокрема поширенням дезінформації та формуванням залежності від технологічних засобів. У цьому дослідженні проаналізовано ризики, пов'язані з правильністю та достовірністю освітнього контенту, створеного за допомогою інструментів штучного інтелекту. Запропоновано алгоритм оцінювання достовірності відповідей систем штучного інтелекту, що використовуються під час створення навчального контенту. Алгоритм ґрунтується на моделюванні процесу перевірки достовірності відповідей, згенерованих штучним інтелектом, передбачає поетапний аналіз генерованих результатів, обчислення показників точності та визначення рівня їх достовірності на основі порівняння з контрольними джерелами. Проведено експериментальну оцінку кількох інструментів штучного інтелекту з використанням тестових завдань, пов'язаних з темами інформаційної безпеки. Результати показали, що точність відповідей, згенерованих ChatGPT, досягала приблизно 90–95%, тоді як інші інструменти демонстрували нижчу надійність залежно від складності завдання. Запропонований алгоритм спрямований на зменшення ризиків поширення дезінформації та сприяє підвищення якості навчальних матеріалів, створених із використанням інтелектуальних систем.

Ключові слова: *алгоритм оцінювання достовірності, моделювання, штучний інтелект, навчальний контент, цифрові освітні платформи.*

Вступ

Штучний інтелект (ШІ) став невід’ємним елементом сучасного цифрового середовища та активно застосовується в різних сферах діяльності. Технології ШІ використовуються для фільтрації спаму, виявлення фішингових атак, аналізу користувацьких запитів і обробки природної мови. Крім того, алгоритми штучного інтелекту застосовуються для автоматичного створення субтитрів, аналізу відеоматеріалів, визначення оптимальних маршрутів із урахуванням дорожньої ситуації та покращення якості машинного перекладу шляхом навчання на нових масивах даних.

Стрімкий розвиток технологій штучного інтелекту сприяв удосконаленню цифрових асистентів та інструментів для створення навчального контенту і значно розширив сфери їх використання. У сфері освіти ШІ допомагає викладачам у підготовці навчальних матеріалів, автоматизуючи рутинні процеси та забезпечуючи персоналізацію навчання. Такі системи можуть генерувати тестові завдання, вправи та навчальні плани, а також адаптувати тексти відповідно до рівня підготовки студентів. Автоматизовані системи оцінювання здатні перевіряти письмові роботи, аналізувати відповіді студентів і оцінювати рівень знань, що дозволяє викладачам оперативніше надавати зворотний зв’язок.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Застосування адаптивних освітніх платформ забезпечує індивідуалізацію навчального процесу, оскільки навчальний контент підлаштовується під потреби та рівень підготовки кожного студента. Системи рекомендацій пропонують персоналізовані теми для вивчення та додаткові вправи, а чат-боти можуть надавати пояснення навчального матеріалу у будь-який зручний час. Загалом використання технологій штучного інтелекту дозволяє скоротити час підготовки навчальних матеріалів і підвищити ефективність освітнього процесу.

Питання використання сучасних цифрових технологій у сфері освіти вже розглядалися в наукових дослідженнях. Зокрема, у роботі [1] досліджено можливості підвищення якості освіти шляхом застосування інтерактивних навчальних інструментів і створення освітнього контенту на основі цифрових платформ дистанційного навчання. У роботі [2] проаналізовано роль інформаційних технологій у навчальному процесі, особливо в умовах дистанційної освіти, а також питання інформаційної безпеки в системах управління навчанням.

Разом з тим, активне використання генеративних систем штучного інтелекту в освітньому середовищі супроводжується появою нових цифрових ризиків, пов’язаних із можливістю формування недостовірних або частково некоректних відповідей. Це створює потенційні загрози поширення дезінформації у навчальному контенті та зумовлює необхідність розроблення ефективних механізмів перевірки достовірності інформації, сформованої інтелектуальними системами.

Незважаючи на активний розвиток інструментів штучного інтелекту, питання алгоритмічного оцінювання достовірності відповідей, сформованих такими системами під час створення навчального контенту, залишається недостатньо дослідженим. Існуючі підходи здебільшого орієнтовані на загальне оцінювання якості інформації, але не забезпечують формалізованого механізму перевірки достовірності відповідей ШІ у навчальному середовищі.

Аналіз літературних даних та постановка проблеми

Використання інструментів на основі штучного інтелекту в освітньому процесі сприяє автоматизації навчальної діяльності, персоналізації навчання та підвищенню ефективності освітнього середовища. Такі технології дають змогу створювати інтерактивний навчальний контент, адаптувати навчальні матеріали до індивідуальних потреб студентів і оптимізувати процедури оцінювання результатів навчання. Водночас впровадження штучного інтелекту в освітню практику має як переваги, так і певні обмеження.

До основних переваг належить підвищення ефективності навчального процесу завдяки автоматизації низки завдань, зокрема створення інтерактивних матеріалів, адаптації контенту до індивідуальних особливостей студентів та оперативного оцінювання результатів їхньої діяльності. Наприклад, віртуальні асистенти ChatGPT та Gemini можуть забезпечувати швидку підтримку студентів, надаючи відповіді на запитання та пояснюючи складні теми. Інструменти підтримки навчального процесу, такі як Redmenta та Amperia, надають можливості для розроблення сучасних навчальних матеріалів, тоді як адаптивні освітні платформи, зокрема Socratic і Khanmigo, сприяють індивідуалізації навчання, регулюючи темп і рівень складності завдань відповідно до потреб кожного студента.

Разом із тим використання технологій штучного інтелекту супроводжується певними ризиками. Зокрема, існує ймовірність формування надмірної залежності студентів від технологічних інструментів, що може негативно впливати на розвиток їхнього самостійного мислення та навичок критичного аналізу. До інших потенційних проблем належать питання захисту конфіденційності даних, оскільки значна кількість цифрових платформ здійснює збір і обробку персональної інформації користувачів, а також ризики виникнення алгоритмічних упереджень, які можуть впливати на об’єктивність результатів навчання. Наприклад, використання платформ для генерації навчального контенту, таких як Quizlet AI Tutor або Curipod, може призводити до створення неточного або недостатньо якісного матеріалу у разі некоректного налаштування інструментів. Крім того, застосування сервісів для розроблення презентацій, зокрема Gamma та Canva, може спричиняти надмірну стандартизацію навчальних матеріалів, що обмежує творчий підхід до їх підготовки.

У таблиці 1 наведено класифікацію поширених інструментів на основі штучного інтелекту, які сприяють автоматизації освітніх процесів, забезпечують адаптацію навчання до рівня підготовки студентів та допомагають викладачам створювати персоналізований і тематично орієнтований навчальний контент.

Використання інструментів штучного інтелекту (ШІ) у навчальному процесі відкриває нові можливості для розвитку освітнього середовища, проте одночасно супроводжується низкою потенційних ризиків і викликів [3]. У наукових джерелах розглядаються різні аспекти та типи таких вразливостей.

Зокрема, у роботі [4] виокремлено три основні проблеми. Першою з них є залежність від технологій. Надмірне використання інструментів ШІ може сприяти зниженню рівня критичного мислення та формуванню залежності студентів від автоматизованих систем. У випадках, коли інформація подається

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Табл. 1. Інструменти з ШІ для підтримки навчального процесу

Тип інструмента	Назва/сайт розробника
Віртуальний асистент	ChatGPT (https://chatgpt.com/g/g-jekajgZGe-insight), Gemini (https://gemini.google.com), Microsoft Copilot (https://copilot.microsoft.com/chats/A6cUi2FsZvuJsZbDWSKg2), Claude (https://www.anthropic.com)
Помічники навчального процесу	Redmenta (https://redmenta.com), Gios (https://gioschool.com/ua), Amperia (https://edpro.ua/amperia), TWEE(https://app.twee.com/auth/signin?utm_source=chatgpt.com)
Засоби інтерактивного навчання та адаптивні платформи	Socratic (by Google) (https://socratic.org), Khanmigo (by Khan Academy) (https://khanmigo.ai/), Querium (https://www.querium.com), Carnegie Learning MATHia (https://www.carnegielearning.com/solutions/math/mathia/), Century Tech (https://www.century.tech/)
Інструменти створення презентацій	Gamma (https://gamma.app), Microsoft Designer (https://designer.microsoft.com), Canva (https://www.canva.com), Kahoot! (https://kahoot.com/
Генератори навчального контенту	Quizlet AI Tutor, Q-Chat (https://quizlet.com/qchat), Curipod (https://curipod.com), MagicSchool.ai (https://www.magicschool.ai/), Knowji – (https://www.knowji.com), ScribeSense (https://www.scribesense.com),
Помічники написання та аналізу текстів	Reading Coach (https://coach.microsoft.com/uk-ua), Grammarly for Education (https://www.grammarly.com),Quillbot (http://quillbot.com), Writefull (http://www.writefull.com)
Освітні чат-боти та репетитори	Tutor AI (http://tutorai.me), Edmentum Exact Path (http://www.edmentum.com/products/exact-path), Cognii (http://www.cognii.com), Squirrel AI (http://squirrelai.com)

у спрощеному вигляді, користувачі можуть приділяти менше уваги самостійному аналізу та розв’язанню складних завдань. У дослідженні Stanford University зазначено, що близько 60% студентів віком від 17 до 25 років схильні сприймати відповіді, згенеровані ШІ, без їхньої критичної перевірки.

Другою проблемою є питання конфіденційності та безпеки даних. Багато застосунків на основі ШІ здійснюють збір значних обсягів інформації про користувачів, і недостатній рівень її захисту може призвести до витоків персональних даних та порушення приватності. Згідно з дослідженням IBM, на яке посилається джерело [4], у 2023 році близько 12% випадків кіберзлочинів в освітньому секторі були пов’язані з витоками персональних даних, що підкреслює необхідність посилення заходів інформаційної безпеки.

Третьою проблемою є упередженість алгоритмів. Алгоритми штучного інтелекту можуть містити вбудовані упередження, що здатні призводити до неточних або несправедливих результатів. Наприклад, автоматизовані системи оцінювання можуть демонструвати необ’єктивність через обмеження моделей або використання нерепрезентативних даних. Дослідження MIT Media Lab показало, що ШІ-системи можуть формувати різні результати для користувачів із різним соціальним або культурним бекграундом.

У дослідженні [5] також наголошується на нерівності доступу до технологій. Не всі студенти мають однакові можливості користування сучасними цифровими інструментами та стабільним доступом до мережі Інтернет. Наприклад, студенти з сільських або соціально вразливих регіонів можуть не мати необхідних технічних засобів або якісного інтернет-з’єднання, що сприяє формуванню цифрового розриву та посиленню освітньої нерівності.

Ще два важливі виклики розглянуто у роботі [6]. Перший із них пов’язаний з витратами на впровадження та підтримку технологій ШІ. Інтеграція таких систем у навчальний процес потребує значних фінансових ресурсів для придбання програмного забезпечення, модернізації технічної інфраструктури та підготовки персоналу. Недостатній рівень фінансування може стати суттєвою перешкодою для ефективного впровадження цих технологій у закладах освіти.

Другим аспектом є трансформація ролі викладача. Автоматизація окремих педагогічних завдань за допомогою інтелектуальних систем може призвести до зміни функцій викладачів або навіть скорочення їхньої кількості, що потенційно впливає на якість навчального процесу та рівень взаємодії зі студентами.

Фактори з сьомого по дев’ятий розглянуто у джерелі [7]. Першим із них є обмеженість креативності та гнучкості. Оскільки системи ШІ працюють на основі алгоритмів і попередньо визначених правил, їхня здатність адаптуватися до нестандартних ситуацій або пропонувати нові підходи до розв’язання проблем може бути обмеженою.

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Восьмим фактором є алгоритмічна дискримінація, яка може виникати через використання упереджених даних або недосконалих алгоритмів, що призводить до нерівного ставлення до різних груп користувачів.

Дев'ятим фактором визначено зниження рівня соціальних і емоційних компетентностей, що може бути пов'язано з надмірною довірою до рішень, запропонованих системами ШІ.

Десятим аспектом є проблема так званих «галюцинацій» штучного інтелекту, розглянута у огляді [8]. Автор, аналізуючи близько тридцяти наукових джерел, зазначає, що сучасні системи ШІ можуть генерувати неправдиву або недостовірну інформацію, яка при цьому виглядає переконливою. Використання таких даних у навчальному процесі може призвести до формування помилкових уявлень про навчальний матеріал та негативно вплинути на якість знань.

Таким чином, застосування технологій штучного інтелекту в освіті порушує не лише питання етики, конфіденційності та інформаційної безпеки, а пов'язане з проблемами недостатнього рівня цифрової компетентності користувачів і фрагментарності навчального забезпечення, що підкреслюється у дослідженні [9].

Джерела [10–13] слугували основою для узагальнення матеріалів наступного розділу. Зокрема, у звіті [12] досліджено потенційні ризики використання чат-ботів на основі штучного інтелекту в освітньому середовищі, серед яких особливо підкреслюється небезпека поширення дезінформації. Автори зазначають, що неточні або хибні дані, згенеровані системами ШІ, можуть вводити студентів в оману, спотворювати навчальний контент і негативно впливати на результати навчання. У зв'язку з цим пропонується застосовувати збалансований підхід до інтеграції технологій ШІ, поєднуючи їх із традиційними методами навчання.

У дослідженні [13] проведено порівняння ефективності підказок, згенерованих системою ChatGPT, із підказками, створеними людськими репетиторами. Отримані результати свідчать, що хоча обидва типи підказок сприяють покращенню результатів навчання, рекомендації, надані викладачами, виявилися більш ефективними. Це підкреслює наявні обмеження навчального контенту, створеного за допомогою ШІ, а також важливість людського контролю для забезпечення якості та достовірності інформації.

Мета та задачі дослідження

Метою статті є розроблення алгоритму оцінювання достовірності відповідей систем штучного інтелекту, що використовуються при створенні навчального контенту.

Для досягнення мети дослідження потрібно виконати такі **завдання**:

1. Проаналізувати сучасні підходи до використання систем штучного інтелекту у створенні навчального контенту та визначити основні переваги і ризики їх застосування в освітньому середовищі.
2. Дослідити проблему достовірності інформації, сформованої генеративними системами штучного інтелекту, зокрема явище так званих «галюцинацій» моделей.
3. Визначити критерії оцінювання достовірності відповідей, сформованих системами штучного інтелекту під час підготовки навчальних матеріалів.
4. Розробити алгоритм оцінювання достовірності відповідей систем штучного інтелекту, який може бути використаний під час створення та перевірки навчального контенту.
5. Проаналізувати можливості практичного застосування запропонованого алгоритму у процесі підготовки навчальних матеріалів та оцінити його ефективність.

Матеріали та методи досліджень

На основі проведеного аналізу літературних джерел, а також з урахуванням практичного досвіду авторів щодо використання інструментів штучного інтелекту для створення навчального контенту було сформовано таблицю 2.

Інструменти, представлені в таблиці, були навмисно відібрані з урахуванням різних типів, відповідно до раніше запропонованої класифікації. Такий підхід дозволив охопити різні категорії інтелектуальних сервісів та проаналізувати характерні для них ризики.

Для обґрунтування інформації, наведеної у третій колонці таблиці, розглянемо окремі приклади. Зокрема, шаблони платформи Canva можуть містити елементи, що охороняються авторським правом, такі як зображення, ілюстрації або шрифти. У разі використання цих матеріалів без належних ліцензій чи дозволів, особливо при створенні комерційного контенту, існує ризик порушення авторських прав їхніх власників. Так, у 2021 році компанія Getty Images подала позов проти компанії Canva, звинувативши її у порушенні авторських прав щодо частини зображень, доступних на платформі.

Подібно до інших онлайн-сервісів для створення та зберігання цифрового контенту, Canva здійснює збір і зберігання персональних даних користувачів. До таких даних належать реєстраційна інформація, платіжні реквізити, а також створений користувачами контент (зображення, графіка тощо). Тому питання захисту персональної інформації також розглядається серед потенційних ризиків використання цієї платформи. Хоча протягом останніх років Canva не повідомляла про значні витоки даних, як і у випадку з будь-якими великими онлайн-системами, ризики,

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Табл. 2. Вразливості інструментів створення навчального контенту з ШІ

Тип інструменту	Назва	Можливі вразливості
Віртуальний асистент	ChatGPT	Ненадійна інформація (галюцинації)
Помічники навчального процесу	Goodnotes	Безпека збереження нотаток, ризик втрати даних
Створення візуального контенту	Leonardo.ai	Авторське право на згенеровані зображення, використання шкідливого контенту, порушення етичних норм
Інтерактивне навчання	Khanmigo	Упередженість алгоритмів, неточність адаптації до учня (стереотипи, контент або відповіді, які не є нейтральними)
Створення презентацій	Canva	Використання шаблонів із потенційними авторськими обмеженнями, безпека особистих даних
Генерація навчального контенту	Quizlet AI Tutor	Неточність автоматично створених тестів, ризик плагіату
Помічники для написання та аналізу текстів	Grammarly for Education	Залежність від стабільності онлайн-доступу; застосування текстових даних користувачів для покращення алгоритмів (загроза витоку конфіденційної інформації)
Освітні чат-боти	Tutor AI	Відсутність контролю якості відповідей, ризик поширення дезінформації

пов’язані зі зберіганням персональної інформації, повністю виключити неможливо.

Ще одним прикладом є система Quizlet AI Tutor, яка може генерувати запитання, подібні до тих, що вже використовуються в інших навчальних матеріалах, підручниках або публікаціях. У ході експериментальної роботи було встановлено, що з 50 згенерованих системою запитань дві пари мали значну змістову подібність.

Певні питання щодо захисту даних виникали також у контексті використання сервісу Grammarly. Зокрема, у 2017 році компанія повідомила, що зберігає текстові дані користувачів з метою вдосконалення власних алгоритмів. Хоча розробники зазначали, що персональна інформація не використовується без згоди користувачів, така практика викликала дискусії щодо належного рівня захисту даних. Крім того, компанія зазнала критики через те, що зберігала введені тексти навіть у випадках, коли вони не були збережені користувачем.

У таблиці 3 наведено перелік загроз, пов’язаних із виявленими вразливостями, зазначеними у таблиці 2. Запропонована система загроз може бути використана як основа для оцінювання ризиків застосування інструментів штучного інтелекту в освітньому процесі та отримання подальших практичних результатів дослідження.

Слід також відзначити наукову роботу [14], яка була використана під час розроблення описаної нижче методики зниження ризику дезінформації. У зазначеному дослідженні запропоновано ефективний підхід до оцінювання діалогових систем, що може бути адаптований для аналізу точності та достовірності відповідей, сформованих віртуальними асистентами та освітніми чат-ботами.

Розвиваючи зазначену ідею, сформулюємо узагальнені рекомендації щодо зменшення ризиків і вразливостей, які можуть виникати під час створення навчального контенту з використанням інструментів на основі штучного інтелекту.

1. Віртуальні асистенти (ChatGPT, Google Bard тощо):

– обмежувати доступ до конфіденційної інформації, не вводити персональні або чутливі дані;

– здійснювати перевірку достовірності отриманих відповідей, використовуючи додаткові джерела для підтвердження фактів;

– контролювати використання таких інструментів у навчальному процесі та уникати повної автоматизації написання навчальних робіт.

2. Помічники організації навчального процесу (GoodNotes, Notion AI тощо):

– використовувати хмарні сервіси разом із локальним збереженням даних та регулярно здійснювати резервне копіювання;

– застосовувати захист доступу за допомогою паролів і двофакторної автентифікації;

– використовувати механізми шифрування інформації;

– контролювати рівень спільного доступу до документів.

3. Інструменти для створення візуального контенту (Leonardo.ai та ін.):

– перевіряти ліцензійні умови використання згенерованих зображень;

– застосовувати безпечні параметри генерації та фільтрувати небажаний контент;

– встановлювати правила використання таких інструментів і здійснювати контроль їх застосування в навчальних закладах.

4. Платформи інтерактивного навчання (Khanmigo, Duolingo AI тощо):

– здійснювати перевірку якості навчальних матеріалів викладачами;

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Табл. 3. Загрози інструментів створення навчального контенту з ШІ

Тип інструменту	Назва	Можливі загрози
Віртуальний асистент	ChatGPT	Дезінформація, витік особистих або конфіденційних даних
Помічники навчального процесу	Goodnotes	Несанкціонований доступ до нотаток, втрата даних через технічні збої
Створення візуального контенту	Leonardo.ai	Генерація маніпулятивних або шкідливих зображень, порушення авторських прав
Інтерактивне навчання	Khanmigo	Неправильне персоналізоване навчання, упередженість у рекомендаціях
Створення презентацій	Canva	Використання нелегального контенту, ризик фішингових атак при спільному доступі
Генерація навчального контенту	Quizlet AI Tutor	Автоматична генерація помилкового або застарілого матеріалу, шахрайство студентів
Помічники для написання та аналізу текстів	Grammarly for Education	Витік текстів користувачів, нав’язування шаблонного стилю
Освітні чат-боти	Tutor AI	Ненадійні або недостовірні відповіді, маніпуляція користувачами

– аналізувати алгоритми персоналізації з метою виявлення можливих упереджень;

– уникати надмірної залежності від ШІ та поєднувати його використання з традиційними методами навчання.

5. Інструменти для створення презентацій (Canva, Prezi AI тощо):

– перевіряти джерела використаних матеріалів та уникати ресурсів із невизначеним авторським правом;

– обмежувати публічний доступ до матеріалів без належного захисту;

– не завантажувати внутрішні або конфіденційні документи.

6. Генератори навчального контенту (Quizlet AI Tutor, Brisk Teaching тощо):

– здійснювати ручну перевірку згенерованих тестових матеріалів для запобігання появі неточних або некоректних запитань;

– обмежувати автоматичне оцінювання та використовувати ШІ як допоміжний інструмент;

– контролювати коректність рекомендацій і аналізувати отримані результати.

7. Інструменти для підтримки письма (Grammarly for Education, QuillBot тощо):

– контролювати передачу персональних даних і уникати введення конфіденційної інформації;

– запобігати надмірному спрощенню або зміні авторського стилю шляхом ручної перевірки текстів;

– не допускати автоматичного редагування студентських робіт без участі викладача.

8. Освітні чат-боти (Tutor AI, Squirrel AI тощо):

– здійснювати перевірку достовірності та коректності згенерованих відповідей і проводити їх регулярний моніторинг;

– використовувати фільтри для обмеження токсичного або небажаного контенту та налаштовувати безпечні параметри діалогу;

– регулярно оновлювати алгоритми роботи систем.

З огляду на викладене запропоновано алгоритм оцінювання достовірності відповідей систем штучного інтелекту, що використовується під час створення навчального контенту. Алгоритм застосовує методи моделювання й поетапний аналіз відповідей ШІ, обчислення показників точності та визначення рівня достовірності отриманих результатів.

Алгоритм оцінювання достовірності відповідей ШІ включає п’ять основних етапів.

Вхідні дані: запит користувача Q, відповідь системи штучного інтелекту A, множина контрольних джерел S.

Крок 1. Отримати відповідь A системи штучного інтелекту на запит Q.

Крок 2. Виконати порівняння відповіді A з інформацією з множини контрольних джерел S.

Крок 3. Обчислити показник точності:

$$Accuracy = \frac{N_{correct}}{N_{total}} \cdot 100\%,$$

де $N_{correct}$ – кількість правильних відповідей;

N_{total} – загальна кількість перевірених відповідей.

Якщо точність нижча за 90%, потрібно розробити додаткові механізми перевірки.

Крок 4. Визначити рейтинг достовірності відповіді за шкалою оцінювання.

Кожна відповідь ШІ може оцінюватися за шкалою достовірності:

1–3 бали – можлива дезінформація, потребує ретельної перевірки.

4–6 балів – частково правильна інформація, бажано перевірити додатково.

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

7–10 балів – висока достовірність, підтверджено джерелами.

Формула середньої достовірності:

$$Score = \frac{\sum_{i=1}^{N} Score_i}{N},$$

де $Score_i$ – оцінка достовірності кожної відповіді;

N – кількість оцінених відповідей.

Крок 5. Автоматичне позначення ненадійних відповідей. При цьому слід класифікувати відповідь як:

– ненадійну;

– частково достовірну;

– достовірну.

Якщо точність відповіді < 90% або середня достовірність < 7, система автоматично попереджає користувача про можливу дезінформацію та пропонує альтернативні джерела.

Крок 6. Впровадження комбінованої перевірки

За необхідності сформувати рекомендації щодо додаткової перевірки інформації.:

− алгоритмічна перевірка (перехресне порівняння відповіді ШІ з іншими джерелами);

− ручна перевірка експертом;

− оцінювання користувачами (рейтинги відповідей у системі).

Таким чином, запропонований алгоритм забезпечує комплексне оцінювання достовірності відповідей систем штучного інтелекту шляхом поєднання моделювання, автоматичного аналізу, експертної перевірки та користувацького оцінювання.

Наукова новизна запропонованого алгоритму полягає у комбінованому підході до оцінювання достовірності, що включає:

− автоматизоване оцінювання точності за допомогою розрахунку відсотка правильних відповідей та рейтингової шкали достовірності (більшість існуючих підходів використовують лише порівняння з референтними відповідями);

− динамічне ранжування надійності відповідей шляхом аналізу достовірності за шкалою 1–10 (більшість методів або оцінюють тільки загальну точність, або не використовують гнучкі рівневі підходи);

− адаптивне обмеження використання ненадійних відповідей – якщо достовірність < 7 або точність < 90%, система автоматично позначає відповідь як ненадійну та пропонує альтернативні джерела (в аналогічних дослідженнях (наприклад, [14]) оцінка обмежується лише порівнянням з контрольними відповідями, без активного впливу на користувацький досвід);

− інтегрований підхід (комбінована перевірка: автоматична + ручна + користувацькі оцінки).

Результати досліджень

Цей метод дозволяє гнучко аналізувати результати роботи ШІ, мінімізувати застосування невірних відповідей та підвищити якість використання ШІ при підготовці навчальних матеріалів й в освіті в цілому, дозволяє зменшити поширення недостовірної інформації у навчальному процесі.

Для проведення практичного експерименту було підібрано 10 тем з популярного й важливого напрямку – інформаційної безпеки. Були сформульовані завдання п’ятьох типів: а) поясни поняття; б) зроби розрахунок; в) виконай порівняння; г) створи запитання; д) надай відповідь. Завдання подавалося системам 5 разів з вимогою перевірити та уточнити результат. На останньому етапі порівнювалися відповіді й результати розрахунків, надані різними інструментами й класичні (вірні) відповіді. Приклад «функція – виклик – результат» наведено на рис.1.

Графічне відображення результатів експериментів, зокрема, для ChatGPT наведено на рис.2.

Обговорення результатів

Отже, для системи ChatGPT було отримано такі результати:

– середній рівень точності становив приблизно 90–95%;

– середній показник достовірності – 7–9 балів;

кількість відповідей, які були класифіковані як надійні, – 174;

– кількість ненадійних відповідей – 326.

Для системи Amperia – AI-асистента, призначеного для підтримки навчання, розв’язання задач і надання пояснень – середня точність становила приблизно 77,88%, а середній показник достовірності – близько 5,91. Із 500 проведених експериментів було отримано 124 надійні та 376 ненадійних відповідей.

Порівняльний аналіз точності та достовірності інструментів Redmenta і Gios, що використовуються як платформи для тестування та оцінювання, показав, що Redmenta демонструє вищу точність під час перевірки тестових завдань, особливо з варіантами закритих відповідей. Водночас система не завжди коректно оцінює розгорнуті відповіді. Платформа Gios характеризується нижчим рівнем точності, що може бути пов’язано з наявністю неоднозначних формулювань у тестових завданнях та залежністю результатів оцінювання від якості навчальних курсів. За результатами проведених розрахунків доцільно рекомендувати Redmenta для автоматизованого оцінювання тестів, тоді як Gios більш придатна для організації гнучкого навчального процесу та проведення навчального тестування.

Подібний аналіз було виконано і для платформ Quizlet AI Tutor (Q-Chat), Curipod, MagicSchool.ai, Knowji та ScribeSense, які використовуються для генерації навчального контенту. Найвищі показники точності продемонструвала система Knowji

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

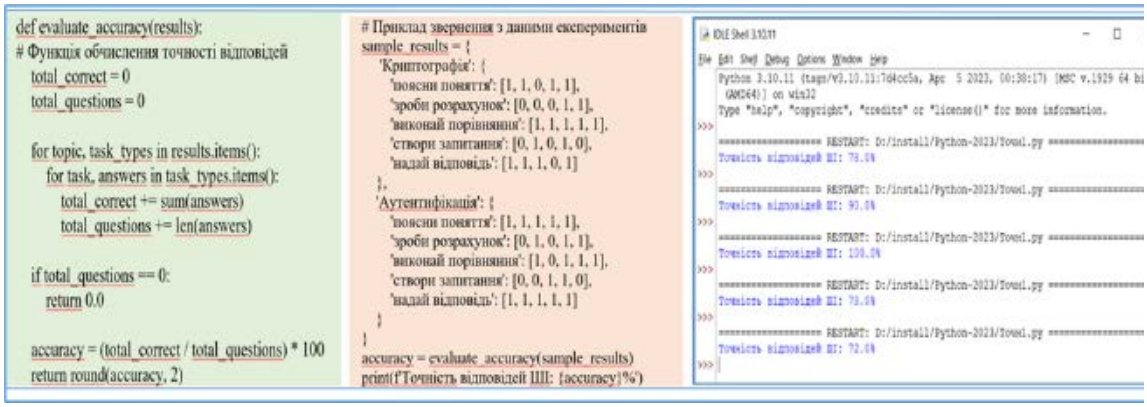

Рис. 1. Оцінювання точності відповідей ШІ

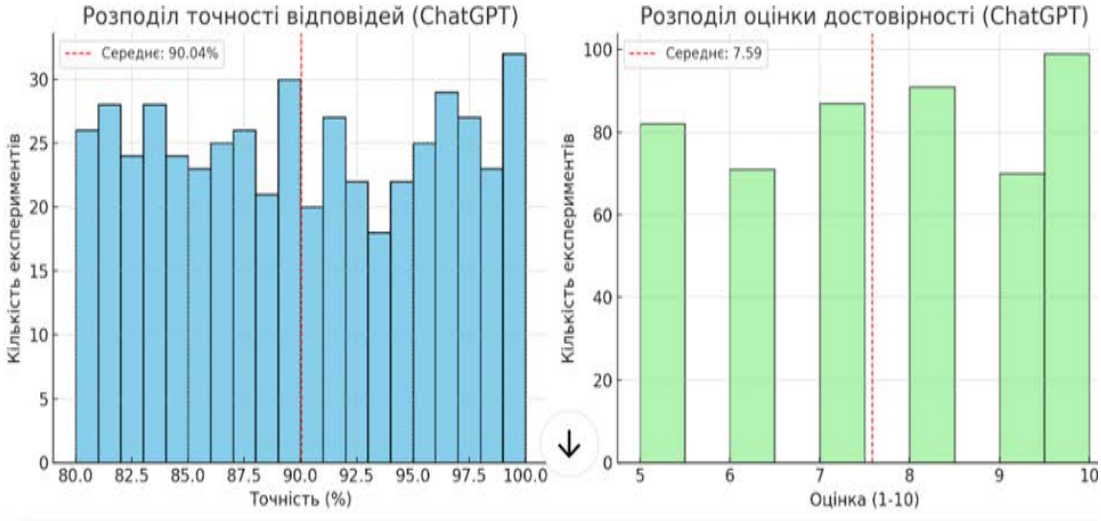

Рис. 2. Результати експериментів

(приблизно 85–95%), що, ймовірно, пов’язано з використанням структурованих даних та розширеного словникового ресурсу. Платформи Quizlet AI Tutor і MagicSchool.ai також показали високі результати, проте їхня точність значною мірою залежить від контексту поставлених завдань. Сервіси Curipod та ScribeSense продемонстрували нижчі показники, що, ймовірно, обумовлено залежністю від якості вихідних даних та складністю обробки текстової інформації.

Слід зазначити, що метою проведених експериментів не було визначення «ідеального» інструменту. Цифрові сервіси постійно вдосконалюються, проходять процеси навчання та регулярного оновлення. Розробники таких систем активно відстежують тенденції ринку та впроваджують новітні технології, алгоритмічні підходи й архітектурні рішення. На отримані результати впливає значна кількість чинників, зокрема мета дослідження, тип і якість використаних даних, їх обсяг, а також досвід користувача та рівень спеціалізації інструменту в певній предметній галузі.

Отримані результати відображають поточний стан досліджуваної проблеми. Основною метою дослідження було продемонструвати ефективність запропонованої методики контролю рівня достовірності та коректності відповідей, сформованих інструментами штучного інтелекту. Запропонований підхід може спростити процес вибору відповідного програмного забезпечення серед широкого спектра сучасних цифрових засобів, що використовуються для підготовки навчальних матеріалів.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Висновки

Сучасні інформаційні технології та цифрові освітні платформи значно розширюють можливості навчального процесу, забезпечуючи доступ до інтерактивного контенту та персоналізованих освітніх ресурсів. Вони сприяють безперервному доступу до навчальних матеріалів, а також покращують комунікацію та взаємодію між учасниками освітнього процесу.

Водночас використання цифрових навчальних систем, зокрема інструментів штучного інтелекту, супроводжується низкою ризиків, пов’язаних із поширенням недостовірної інформації, витоками персональних даних та іншими загрозами інформаційної безпеки. Це зумовлює необхідність розроблення ефективних підходів до перевірки достовірності навчального контенту, сформованого інтелектуальними системами.

У роботі запропоновано алгоритм оцінювання достовірності відповідей систем штучного інтелекту, що використовується під час створення навчального контенту. Алгоритм ґрунтується на моделюванні процесу перевірки відповідей ШІ, обчисленні показників точності та визначенні рівня достовірності отриманих результатів. Його застосування дає змогу зменшити ризики поширення дезінформації та підвищити якість навчальних матеріалів, створених із використанням інструментів штучного інтелекту.

Запропонований алгоритм може бути використаний для вибору та оцінювання цифрових освітніх інструментів, а також для підвищення надійності навчального контенту в сучасному освітньому середовищі..

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] Г. Ю. Журавель та Н. О. Маслова, «Застосування інтерактивних засобів при створенні учбового контенту закладу освіти на основі цифрових навчальних платформ», у *Моделювання і комп’ютерна графіка: зб. матер. Восьмої міжнар. наук.-техн. конф.*, Донецьк: Донецький національний технічний університет, 2023, с. 95–100.

[2] Н. Маслова та О. Любименко, «Безпека та захист навчальних LMC систем», *Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація*, т. 1, № 33, с. 38–46, 2023. doi: 10.31474/2786-9024/v1i1(33).299636.

[3] Khmelnitsky National University, *Proceedings of the Khmelnitsky National University. Technical sciences*. [Online]. Available: https://cpp.khmnu.edu.ua/index.php/cpp/issue/view/8

[4] S. Baumer, A. Carnevale, T. Corbett та C. Dumaresq, «Використання штучного інтелекту у навчанні: можливості та ризики», Вінницький державний педагогічний університет імені Михайла Коцюбинського, Buki, 30 бер. 2023. [Online]. Available: https://buki.com.ua/blogs/vikoristannia-stucnogo-intelektu-u-navcanni-mozlivosti-ta-riziki/

[5] NAUROK, «Методичні рекомендації: можливості, застереження та перспективи застосування ШІ на уроках української мови та літератури», 2023. [Online]. Available: https://naurok.com.ua/metodichni-rekomendaci-mozhlivosti-zasterezhennya-ta-perspektivi-zastosuvannya-shi-na-urokah-ukra-nsko-movi-ta-literaturi-450719.html (accessed Mar. 02, 2026).

[6] A. Kolomiiets та O. Kushnir, «Використання штучного інтелекту в освітній та науковій діяльності: можливості та виклики», *Modern Information Technologies and Innovation Methodologies of Education in Professional Training: Methodology, Theory, Experience, Problems*, вип. 70, с. 45–57, 2024. doi: 10.31652/2412-1142-2023-70-45-57.

[7] Н. С. Бобро, «Застосування штучного інтелекту у закладах вищої освіти: зарубіжний досвід», Noolab, 9 жовт. 2024. [Online]. Available: https://www.noolab.ch/ua/ua-blog/zastosuvannya-shtuchnogo-intelektu-u-zakladah-vishchoyi-osvity-zarubizhniy-dosvid

[8] Н. Баловсяк, «ШІ та виклики в освіті: як поєднати інноваційну технологію з консервативною традицією», Kunsht, 27 груд. 2024. [Online]. Available: https://kunsht.com.ua/articles/shi-ta-vyklyky-v-osviti-iak-poyednaty-innovatsiynu-tekhnolohiiu-z-konservatyvnoiu-tradytsiyeiu

[9] Інститут інформаційних технологій і засобів навчання НАПН України, *Використання штучного інтелекту в освіті*, 2024. [Online]. Available: https://lib.iitta.gov.ua/id/eprint/743864

[10] Міністерство освіти і науки України, *Інструктивно-методичні рекомендації щодо використання штучного інтелекту в закладах загальної середньої освіти*, Київ, 2024, с. 1–10. [Online]. Available: https://mon.gov.ua/static-objects/mon/sites/1/news/2024/05/21/Instruktyvno.metodychni.rekomendatsiyi.shchodo.SHI.v.ZZSO-22.05.2024.pdf (accessed Mar. 02, 2026).

[11] О. В. Кузьменко та К. Г. Гриценко, «Технології доброчесного використання штучного інтелекту у навчальному процесі», у *Матеріали конференції*, Центр українсько-європейських студій, 2024, с. 45–50. [Online].

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359331

Available: https://cuesc.org.ua/images/informlist/Maket_advanced_training_PSAU.pdf

[12] S. Saghiri та A. Saghiri, *Catastrophic risks of AI-based chatbots in educational systems*. Society of Actuaries, 2024, с. 1–12. [Online]. Available: https://www.soa.org/4a3f4c/globalassets/assets/files/resources/research-report/2024/ai-risk-essays/saghiri-ai-based-chatbots.pdf

[13] Z. A. Pardos та S. Bhandari, «Learning gain differences between ChatGPT and human tutor generated algebra hints», *arXiv preprint arXiv:2302.06871*, 2023. [Online]. Available: https://arxiv.org/abs/2302.06871

[14] J. Deriu *et al.*, «Spot The Bot: A Robust and Efficient Framework for the Evaluation of Conversational Dialogue Systems», *arXiv preprint arXiv:2010.02140*, 2020. [Online]. Available: https://arxiv.org/abs/2010.02140

ALGORITHM FOR ASSESSING THE RELIABILITY OF ARTIFICIAL INTELLIGENCE SYSTEM RESPONSES IN EDUCATIONAL CONTENT CREATION

Nataliia Maslova, Olena Lyubymenko

The paper analyzes the risks associated with the correctness and reliability of educational content created using artificial intelligence tools. Intelligent tools based on artificial intelligence contribute to the automation of the process of developing interactive educational materials, increasing the level of personalization of learning and optimizing the analysis of educational results. At the same time, the introduction of artificial intelligence technologies into the educational environment is accompanied by the emergence of new digital risks, in particular, the spread of disinformation and the formation of dependence on technological means. This study analyzes the risks associated with the correctness and reliability of educational content created using artificial intelligence tools. An algorithm for assessing the reliability of responses of artificial intelligence systems used in the creation of educational content is proposed. The algorithm is based on modeling the process of checking the reliability of answers generated by artificial intelligence, provides for a step-by-step analysis of the generated results, calculation of accuracy indicators and determination of their reliability level based on comparison with control sources. An experimental evaluation of several artificial intelligence tools was carried out using test tasks related to information security topics. The results showed that the accuracy of answers generated by ChatGPT reached approximately 90–95%, while other tools demonstrated lower reliability depending on the complexity of the task. The proposed algorithm is aimed at reducing the risks of spreading disinformation and contributes to improving the quality of educational materials created using intelligent systems.

Keywords: *reliability assessment algorithm, modeling, artificial intelligence, educational content, digital learning platforms.*

REFERENCES

[1] H. Yu. Zhuravel and N. O. Maslova, “Application of interactive tools in creating educational content of educational institutions based on digital learning platforms” [“Zastosuvannia interaktyvnykh zasobiv pry stvorenni uchbovoho kontentu zakladu osvity na osnovi tsyfrovykh navchalnykh platform”], in *Modeling and Computer Graphics: Proc. 8th Int. Sci. and Tech. Conf.*, Donetsk National Technical University, 2023, pp. 95–100.

[2] N. Maslova and O. Liubymenko, “Security and protection of educational LMC systems” [“Bezpeka ta zakhyst navchalnykh LMC system”], *Scientific Works of Donetsk National Technical University. Series: Computing Technology and Automation*, no. 1(33), pp. 38–46, 2023. [Online]. Available: https://doi.org/10.31474/2786-9024/v1i1(33).299636

[3] Khmelnitsky National University, *Proceedings of the Khmelnitsky National University. Technical Sciences*. [Online]. Available: https://cpp.khmnu.edu.ua/index.php/cpp/issue/view/8

[4] S. Baumer, A. Carnevale, T. Corbett, and C. Dumaresq, “Use of artificial intelligence in education: opportunities and risks” [“Vykorystannia shtuchnoho intelektu u navchanni: mozhlyvosti ta ryzyky”], Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Buki, 2023. [Online]. Available: https://buki.com.ua/blogs/vikoristannia-stucnogo-intelektu-u-navcanni-mozhlivosti-ta-riziki

[5] NAUROK, “Methodological recommendations: opportunities, cautions and prospects of AI use in Ukrainian language and literature lessons” [“Metodychni rekomendatsii: mozhlyvosti, zasterezhennia ta perspektyvy zastosuvannia ShI na urokakh ukrainskoi movy ta literatury”], 2023. [Online]. Available: https://naurok.com.ua/metodichni-rekomendaci-mozhlivosti-zasterezhennya-ta-perspektivi-zastosuvannya-shi-na-urokah-ukra-nsko-movi-ta-literaturi-450719.html (accessed Mar. 02, 2026).

[6] A. Kolomiiets and O. Kushnir, “Use of artificial intelligence in educational and scientific activities: opportunities and challenges” [“Vykorystannia shtuchnoho intelektu v osvitnii ta naukovii diialnosti: mozhlyvosti ta vyklyky”], *Modern Information Technologies and Innovation Methodologies of Education in Professional Training: Methodology, Theory, Experience, Problems*, vol. 70, pp. 45–57, 2024. [Online]. Available: https://doi.org/10.31652/2412-1142-2023-70-45-57

[7] N. S. Bobro, “Application of artificial intelligence in higher education institutions: foreign experience” [“Zastosuvannia shtuchnoho intelektu u zakladakh vyshchoi osvity: zarubizhnyi dosvid”], Noolab, 2024. [Online]. Available: https://www.noolab.ch/ua/ua-blog/zastosuvannya-shtuchnogo-intelektu-u-zakladah-vishchoyi-osvity-zarubizhniy-dosvid

[8] N. Balovsiak, “AI and challenges in education: how to combine innovative technology with conservative tradition” [“ShI ta vyklyky v osviti: yak poiednaty innovatsiinu

tekhnolohiiu z konservatyvnoiu tradytsiieiu”], Kunsht, 2024. [Online]. Available: https://kunsht.com.ua/articles/shi-ta-vyklyky-v-osviti-iak-poyednaty-innovatsiynu-tekhnolohiiu-z-konservatyvnoiu-tradytsiyeiu

[9] Institute of Information Technologies and Learning Tools of the NAES of Ukraine, “Use of artificial intelligence in education” [“Vykorystannia shtuchnoho intelektu v osviti”], 2024. [Online]. Available: https://lib.iitta.gov.ua/id/eprint/743864

[10] Ministry of Education and Science of Ukraine, *Instructional and methodological recommendations on the use of artificial intelligence in general secondary education institutions* [“Instruktyvno-metodychni rekomendatsii shchodo vykorystannia shtuchnoho intelektu v zakladakh zahalnoi serednoi osvity”], pp. 1–10, 2024. [Online]. Available: https://mon.gov.ua (accessed Mar. 02, 2026).

[11] O. V. Kuzmenko and K. H. Hrytsenko, “Technologies of ethical use of artificial intelligence in the educational process” [“Tekhnolohii dobrochesnoho vykorystannia shtuchnoho intelektu u navchalnomu protsesi”], in *Conference Proceedings*, Center for Ukrainian-European Studies, 2024, pp. 45–50.

[12] S. Saghiri and A. Saghiri, “Catastrophic risks of AI-based chatbots in educational systems,” *Society of Actuaries Research Report*, pp. 1–12, 2024. [Online]. Available: https://www.soa.org/4a3f4c/globalassets/assets/files/resources/research-report/2024/ai-risk-essays/saghiri-ai-based-chatbots.pdf

[13] Z. A. Pardos and S. Bhandari, “Learning gain differences between ChatGPT and human tutor generated algebra hints,” *arXiv preprint*, pp. 1–12, 2023. [Online]. Available: https://arxiv.org/abs/2302.06871

[14] J. Deriu *et al.*, “Spot The Bot: A Robust and Efficient Framework for the Evaluation of Conversational Dialogue Systems,” *arXiv preprint arXiv:2010.02140*, 2020. [Online]. Available: https://arxiv.org/abs/2010.02140

Дата першого надходження статті до видання: 13.02.2026
Дата прийняття статті до друку після рецензування:10.03.2026
Дата публікації (оприлюднення) статті: 12.05.2026

НОТАТКИ

НАУКОВІ ПРАЦІ
ДОНЕЦЬКОГО НАЦІОНАЛЬНОГО
ТЕХНІЧНОГО УНІВЕРСИТЕТУ

Серія: «Обчислювальна техніка та автоматизація»

Всеукраїнський науковий збірник
Заснований у липні 1998 року
Виходить 2 рази на рік

Мови видання: українська, англійська (змішаними) мовами.

Т4. № 6(38)'2026

Дата розміщення онлайн: 12.05.2026. Дата друку: 19.05.2026.
Формат 60×84/8. Папір офсетний. Гарнітура Calibri. Цифровий друк.
Умовно друк. арк. 12,09. Тираж 150. Замовлення № 0526/435.

Ціна договірна. Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7623 від 22.06.2022