UDC 351:004.056.5:004.738.5(477)

V. Sarychev

O. Poplavskyi

O. Cherkaskyi

CYBERSECURITY SYSTEM OF THE PUBLIC SECTOR OF UKRAINE: STRUCTURAL PROBLEMS, GOVERNANCE MODELS, AND STRATEGIC MODERNIZATION DIRECTIONS

The article substantiates the strategic principles for developing the cybersecurity system of Ukraine's public sector in the context of digital transformation, European integration, and military threats. Based on an analysis of national strategic documents and international approaches — the NIS 2 Directive (Network and Information Security Directive 2, an EU legislative act on measures for a high common level of cybersecurity across Member States), NIST CSF 2.0 (Cybersecurity Framework), and Zero Trust (a cybersecurity architectural approach based on the principle of "never trust, always verify") — the study systematizes management tools for the cyber protection of public institutions. Structural problems are identified: regulatory fragmentation, uneven cyber maturity, personnel shortages, insufficient integration of management and technological solutions, and weaknesses in risk-oriented management and security culture. Strategic goals and principles, a conceptual development model, and tools for its implementation, monitoring, and performance evaluation for public administration bodies are proposed.

***Keywords**: cybersecurity, public sector, public administration, NIS 2, NIST CSF 2.0, Zero Trust, cyber maturity, cyber resilience.*

Statement of the problem. The rapid digitalization of Ukraine's public sector (electronic services, registries, interagency platforms) expands the attack surface and increases the dependence of public administration on digital components, which is a typical challenge for digitalized public administration systems and critical infrastructure. In wartime conditions, these risks are intensified by the hybrid nature of threats, where cyber influence is combined with information-psychological operations and pressure on the state's ability to provide public services continuously. Despite the presence of regulatory and organizational elements of cyber defense, systemic barriers persist in the public sector: fragmented regulation, uneven cyber maturity of institutions, personnel shortages, weak integration of management and technical solutions, and insufficiently developed partnerships with the private and civil sectors. In such a situation, modernizing the cybersecurity system requires a transition from predominantly reactive practices to a risk-oriented management model aligned with the European regulatory framework of the NIS 2 standard, as well as modern requirements for cyber risk management technologies (NIST CSF 2.0 and Zero Trust).

Analysis of recent research and publications. The issue of public sector cybersecurity is studied at the intersection of public administration, digital transformation, and national security. A significant body of work is dedicated to critical infrastructure protection, the evolution of threats, and approaches to ensuring cyber resilience , as well as the systemic consequences of the digitalization of infrastructure and management circuits. Certain studies propose instrumental approaches to structuring management knowledge (for example, ontologies/Knowledge Graphs for critical infrastructure), which can be useful for standardizing policies and processes in public bodies.

At the same time, gaps critical specifically for the public sector of Ukraine can be traced in the scientific discourse: (1) the dominance of a technical-legal focus over managerial analysis; (2) insufficient integration of cybersecurity into models of good governance and the full cycle of public policy; (3) a deficit of holistic strategic models adapted to the conditions of full-scale war and European integration obligations.

The purpose of the article is the theoretical substantiation and development of strategic foundations for the evolution of the cybersecurity system in the public sector of Ukraine based on a synthesis of management models and international approaches to cyber defense and cyber resilience. Achieving this goal involves

forming an integrated strategic vision (goals, principles, priorities) aligned with NIS 2 requirements and the logic of NIST CSF 2.0 cyber risk management, as well as oriented toward implementation in state and local government bodies.

Summary of the main material. The logic of the research involves the conceptual clarification of such basic concepts as the cybersecurity system in the public sector and the mechanisms of public administration in the field of cybersecurity, as well as the determination of its effective methodological approaches.

The cybersecurity system in the public sector of Ukraine is proposed to be understood as an organized set of public authority subjects, legal norms, management processes, institutional structures, resources, and technologies aimed at ensuring the confidentiality, integrity, availability, and resilience of information resources and information and communication systems of state authorities, local self-government bodies, and their subordinate organizations. Strategic foundations for the development of the cybersecurity system are a set of long-term goals, principles, priorities, management models, and basic decisions regarding architecture, institutional design, and resource provision that determine the desired state of the system, the trajectory of its evolution, and the rules for making management decisions in the medium and long term.

Along with this, the mechanisms of public administration in the field of cybersecurity should be perceived as institutionally fixed ways of influence of public authority subjects on the object of management (the cybersecurity system), which include legal, organizational, economic, information, technological, personnel, and communication tools, as well as procedures for planning, implementation, monitoring, and evaluation of policy in this field.

Thus, based on such a conceptual clarification, it is possible to determine the leading methodological approaches of the presented research, among which the most productive are as follows:

1) systemic approach, which allows considering the cybersecurity of the public sector as a multi-level system where legal-regulatory, institutional, technological, personnel, organizational-procedural, and cultural-value levels interact;

2) institutional approach, which emphasizes formal and informal rules, organizational structures, competencies of cybersecurity provision subjects, as well as mechanisms of interagency coordination and interaction between the state, business, and civil society;

3) process approach, which is used to analyze the cycle of state policy in the field of cybersecurity – from problem formulation and goal setting to implementation, monitoring, evaluation, and correction of policies and programs;

4) risk-oriented approach, which ensures concentration on the assessment and management of cyber risks, including supply chain risks, the human factor, and the exploitation of vulnerabilities of public sector information systems; it correlates with the requirements of the NIS 2 directive and modern cyber risk management frameworks;

5) comparative approach, which is used to compare national strategic documents and institutional practices with European and international standards (NIS 2, NIST CSF, Zero Trust Architecture), which allows adapting best practices to the conditions of Ukraine.

The research logic is structured as follows: first, the categorical apparatus and methodological foundations are clarified; then, global trends and cybersecurity challenges are analyzed ; after that, structural problems of the national cybersecurity system in the public sector are identified; on this basis, strategic goals, principles, and priorities are formulated, and a conceptual model is proposed; the final block is dedicated to the mechanisms of implementation, monitoring, and performance evaluation.

Figure 1 demonstrates these key methodological approaches, which together form the holistic logic of the research.

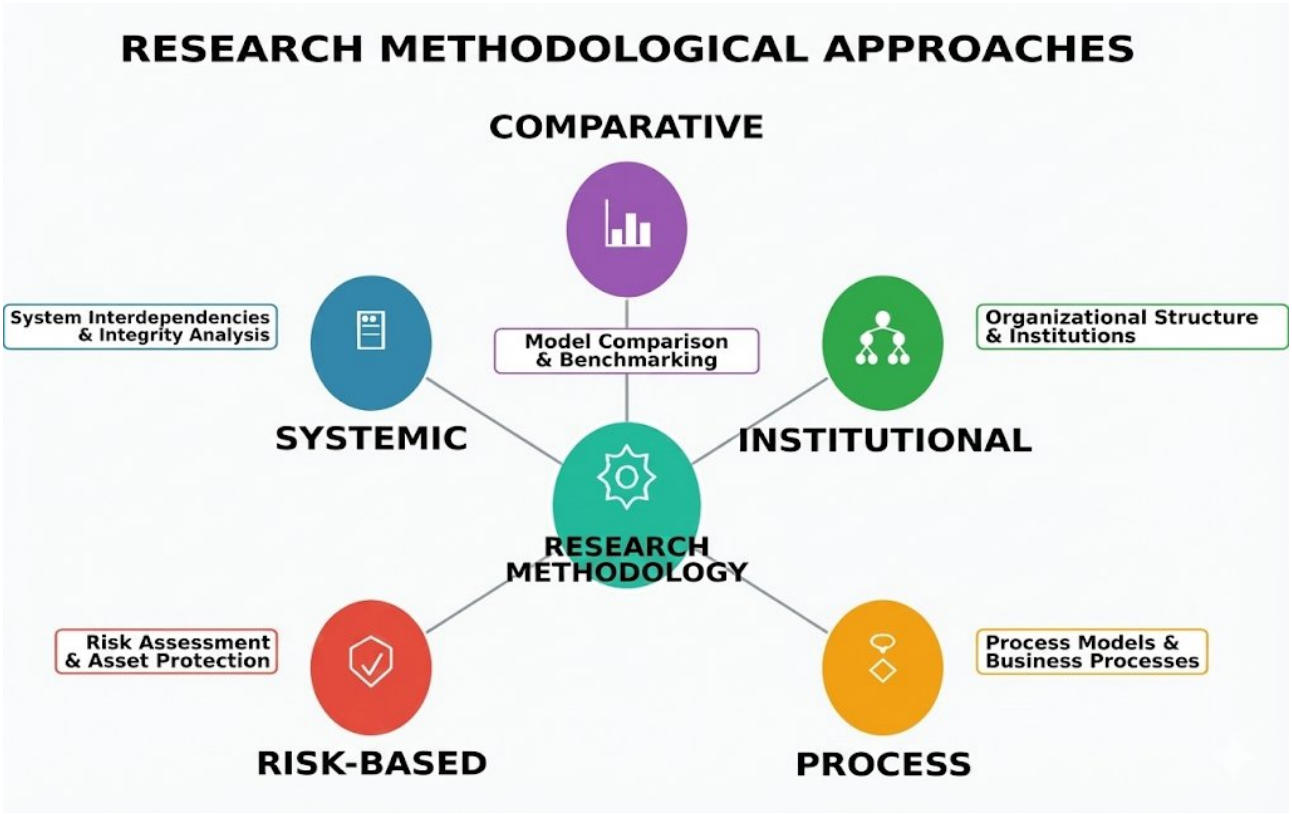

Figure 1 – Key methodological approaches of the research

At the center is a node of methodological approaches, from which the main analytical directions diverge: the systemic approach focuses on the analysis of interconnections between system elements and allows viewing the object as a holistic structure with integrated components; the institutional approach is aimed at assessing the organizational structure, the role of institutions, formal and informal rules, and functioning mechanisms; the process approach emphasizes flows and operations, enabling the study of the sequence of actions, management cycles, and the logic of policy implementation; the risk-oriented approach focuses on identifying and assessing threats, determining vulnerabilities, and forecasting risks, which allows for identifying critical points and forming preventive mechanisms; the comparative approach provides the opportunity to analyze alternatives and compare different models and strategies, helping to choose the most effective solution. In aggregate, these approaches provide a multi-dimensional vision of the research object and allow for obtaining complex balanced conclusions.

An important factor of the presented study is also the consideration that the modern cybersecurity environment is characterized by a number of such powerful trends, critically important for the public sector:

hybridization of threats, the combination of cyberattacks with information-psychological operations, physical impact on infrastructure, and economic pressure;

the growing role of states and non-state actors who carry out targeted cyberattacks on public institutions, the electoral system, and critical infrastructure management bodies;

expansion of the state's digital footprint through e-services, registries, "single window" systems, and open data platforms, which increases the attack surface;

rapid implementation of cloud services, mobile solutions, IoT infrastructure, and intelligent data analysis systems in the public sector;

growing dependence of public management on digital platforms managed by the private sector (cloud providers, telecom operators, IT solution providers).

In parallel, Ukraine aims to harmonize its own cybersecurity system with European approaches, primarily the NIS 2 doctrine, which establishes a unified interpretation of the legal standard for ensuring a high level of cybersecurity in critical sectors, including public administration, and requires Member States to form national strategies, coordination systems, and monitoring (Table 1).

Table 1 – Structural problems of the national cybersecurity system in the public sector

№	**Key Structural Problem**
1	Regulatory fragmentation: bylaws and departmental documents are inconsistent, and there is no unified methodological framework for minimum standards, policies, and procedures
2	Uneven cyber maturity: some government bodies have standards and SOC/CSIRT functions, but many institutions, especially local ones, operate on outdated infrastructure and with informal procedures
3	Limited human resource potential: shortage of specialists, competition with the private sector, weak training and motivation systems, which reduces the ability to maintain the required level of cyber protection
4	Insufficient integration of solutions: technical tools are implemented without changes in processes, powers, and regulations, which reduces the effectiveness of investments in cybersecurity
5	Weak development of risk-oriented management: risk assessment is conducted sporadically, formally, and without a unified methodology, which contradicts modern standards
6	Insufficient interaction with business and the civil sector: mechanisms for information exchange, joint training, and incident reporting operate fragmentarily
7	Low security culture: the human factor is the main source of vulnerabilities, and staff awareness programs are not systemic

Collectively, the results presented in Table 1 demonstrate the complex nature of structural problems and the need for a systemic strategic update of the public sector cybersecurity model – from regulatory support and personnel policy to management processes, partnership, and the development of risk-oriented approaches. The necessity of such an approach is justified by the fact that, as shown in Table 1, the existing problems are complex in nature and simultaneously cover regulatory-legal, organizational-managerial, personnel, technological, and cultural dimensions.

Therefore, the first strategic goal is to ensure the resilience and continuity of the functioning of public authorities and electronic public services under the conditions of destructive influence in cyberspace. The relevance of this goal stems from the unevenness of cyber maturity and the presence of outdated infrastructure, and is confirmed by the growth of hybrid threats, the escalation of cyberattacks, and the increasing dependence of public administration on digital platforms.

The second strategic goal is the formation of unified integrated managerial and regulatory-methodological frameworks for the public sector cybersecurity standard, aligned with their European counterparts and national security priorities.

The third strategic goal is to increase the cyber maturity of government bodies based on standardized assessment and capability development models, which corresponds to international approaches set out in NIST CSF 2.0, ISO/IEC 27001, and relevant European practices.

The fourth strategic goal involves the creation of a sustainable personnel, educational, and scientific-analytical potential for public sector cybersecurity. The necessity of this goal is driven by the shortage of qualified specialists and the weakness of systemic personnel training, as reflected in Table 1, and is also confirmed by national and international analytical data.

The fifth strategic goal is related to the institutionalization of partnerships between the state, business, and civil society in the field of cybersecurity. As shown in Table 1, interaction with business and civil society remains limited and fragmented, which complicates the exchange of information about threats, the conducting of joint exercises, and the development of incident reporting. Mechanisms for such partnership are provided for both in NIS 2 and in national strategic documents and international recommendations of ENISA and NIST.

Based on the defined data, it is possible to form a conceptual model for the strategic development of the cybersecurity system in the public sector.

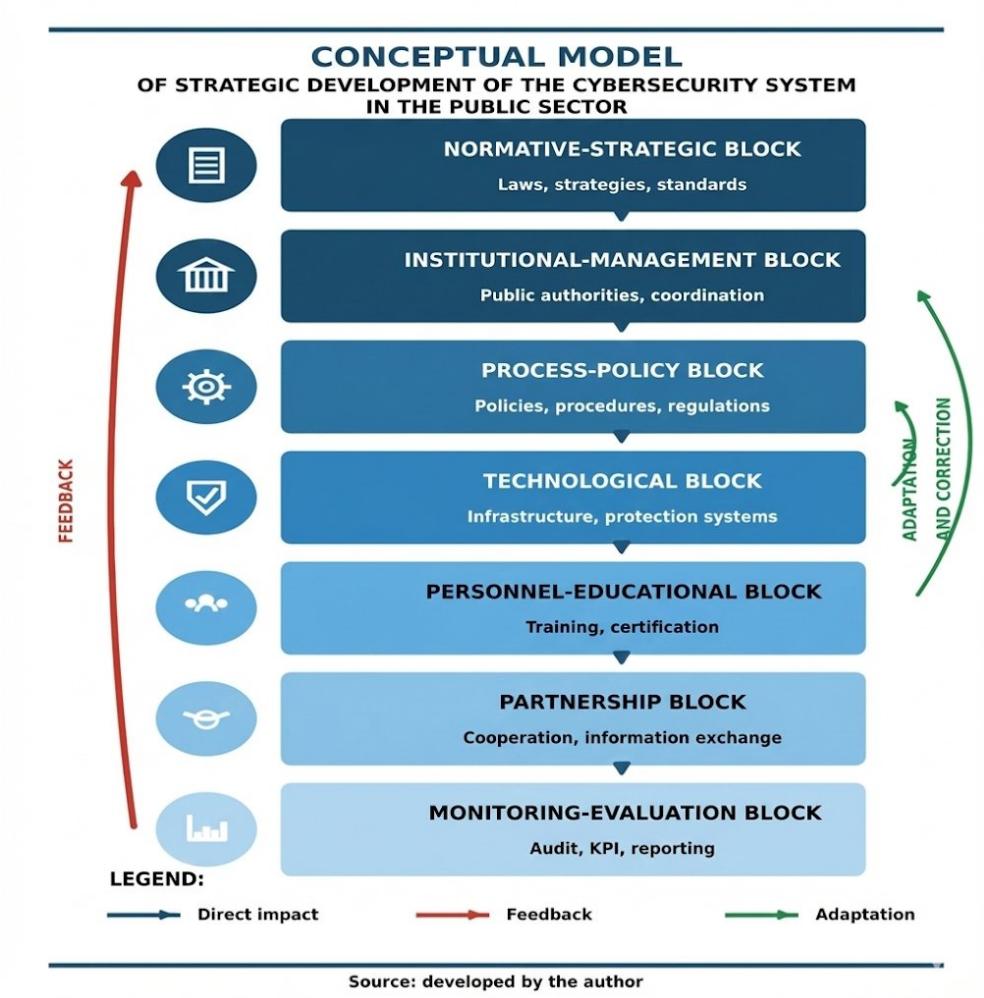

Figure 2 – Structural blocks of the conceptual model

The presented model demonstrates the consistent interaction of seven structural blocks that together form the strategic architecture for the development of the cybersecurity system in the public sector. Its upper normative-strategic block establishes the legal, conceptual, and methodological foundation; the next, institutional-managerial block, ensures the distribution of roles between central and local authorities, defines coordination mechanisms, and forms the institutional infrastructure (SOC, CERT, interagency centers) ; the process-political block regulates the cycle of formation and implementation of state policy: from problem analysis and solution development to implementation, monitoring, and correction.

The technological block rests upon it, covering infrastructure components, protection systems, monitoring tools, and the application of Zero Trust models and international cyber defense standards. Next, the model moves to the personnel-educational block, which forms staff competencies, the system of training and certification, and the security culture. Nearby is the partnership block, which ensures interaction between the state and business, scientific institutions, civil society, and international partners, creating a shared environment of cyber resilience. The final component is the monitoring-evaluative block, responsible for audits, maturity assessment, KPIs (key performance indicators), reporting, and the formation of feedback, which contributes to policy updates and system adaptation to new threats. Direct, feedback, and adaptive links between the blocks ensure the cyclical nature of development, continuous improvement, and the consistency of all model components.

However, the development of the cybersecurity system in the public sector of Ukraine requires not only strategically formulated goals but also effective tools for their practical implementation. In conditions of digital transformation, deepened European integration, and growing hybrid threats, state authorities need a comprehensive, interconnected, and adaptive system of managerial, regulatory, technological, and communication solutions. The strategic foundations for public sector cybersecurity development defined in the study are aimed at increasing the cyber maturity of institutions, ensuring the continuity of public services,

strengthening human resource potential, and forming sustainable partnership interactions between the state, business, and civil society. In this context, an important component is the systematization of public administration tools that ensure the practical realization of strategic guidelines.

The presented diagram (Figure 3) demonstrates a logically ordered architecture of tools — from the regulatory basis to technological solutions. It illustrates the comprehensive structure of public administration tools that ensure the practical implementation of the strategic foundations for developing public sector cybersecurity. The scheme is constructed on the principle of vertical sequence: each subsequent instrumental block relies on the previous one and complements it.

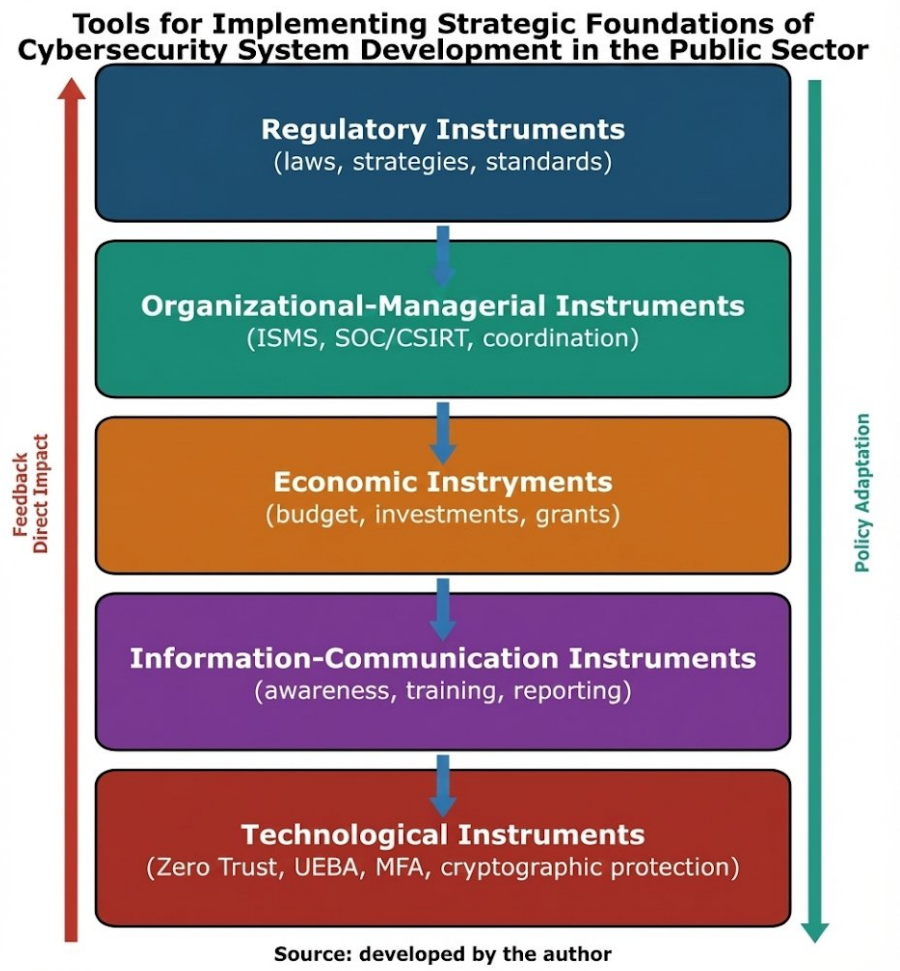

Figure 3 – Tools for the implementation of the strategic foundations for the development of the cybersecurity system in the public sector

The diagram also contains two key systemic loops. Feedback (red outline) goes from the technological block to the regulatory one and ensures policy review, standard updates, and improvement of requirements based on the results obtained, audits, and identified incidents. The adaptive link (green outline) reflects the possibility of dynamic adjustment of management decisions and regulatory provisions based on new threats, technological development, and updates to international requirements. Collectively, the diagram demonstrates that the public sector cybersecurity system is cyclical and self-reinforcing: the results of practical activities constantly return to the strategic loop and ensure the continuous improvement of models, standards, and procedures.

Conclusions

The study identifies key systemic problems in public sector cybersecurity development: fragmentation of regulation and practices, uneven cyber maturity of institutions, shortage of competent personnel, insufficient integration of management and technological solutions, and limited institutionalization of partnership and

incident information exchange. This creates a need for a transition from a predominantly reactive protection model to risk-oriented management, where priorities are determined by the criticality of services and processes, and security measures are integrated into the planning, budgeting, control, and audit cycle.

The formulated strategic foundations for the development of the cybersecurity system should be implemented as a complex of interconnected areas: improvement of regulatory and organizational architecture, implementation of unified requirements and risk management procedures, increasing the resilience and recoverability of digital services, development of monitoring and response capabilities, strengthening the protection of supply chains, and systematic work with the human factor. Practical emphasis should be placed on process standardization (policies, regulations, responsibility roles), deployment of performance and compliance indicators, ensuring training for staff and management, and creating sustainable mechanisms for interdepartmental coordination. Ultimately, a strategic approach allows shifting cybersecurity from a mode of primarily responding to current incidents to a managed system mode, where incidents do not become the norm of management.

The results obtained have applied significance for the formation and actualization of state and departmental cyber defense programs, the preparation of management decisions regarding resource provision, the design of organizational models (functions, powers, responsibility), and for the modernization of educational and advanced training programs focused on the cyber maturity of public institutions. At the same time, it should be considered that the proposed approaches require further empirical verification and detailing at the level of specific institutional cases and types of digital services.

Directions for further research may include: empirical validation of the proposed strategic foundations using examples of government bodies at various levels with a comparison of risk profiles, cyber maturity, and organizational models; development of a formalized methodology for assessing the cyber maturity of public institutions with clear levels, measurable criteria, and compliance profiles, as well as building a system of KPIs and performance metrics, particularly for detection, response, recovery, and for managing vulnerabilities and supply chain risks.

References

1. Angyalos Z., & Szilágyi R. (2025). Cybersecurity risks in critical infrastructures: Insights from CISA and ENISA data. *Journal of Agricultural Informatics.* October, no. 16(2), pp. 1–11. DOI: https://doi.org/10.17700/jai.2025.16.2.759 [in English].

2. Potapovs M., & Kanasta K. E. (Eds.) (2025). Cybersecurity in Latvia: Forging resilience amidst emerging threats. Routledge. DOI: https://doi.org/10.4324/9781003638858 [in English].

3. Frey C. (2024). Future-proofing cybersecurity: Leveraging strategic foresight to enhance resilience. *International Journal of Cyber Diplomacy,* no. 5, pp. 23–40. DOI: https://doi.org/10.54852/ijcd.v5y202402 [in English].

4. Vevera A. V. (2024). The digitalization of critical infrastructures – Systemic considerations, evolutions of governance and elements of a national research agenda. *Romanian Military Thinking*. December, no. (3), pp. 104–125 [in English].

5. Ahokangas P., & Aagaard A. (Eds.) (2024). The changing world of mobile communications: 5G, 6G and the future of digital services. Palgrave Macmillan. DOI: https://doi.org/10.1007/978-3-031-33191-6 [in English].

6. Crowther A., Foulds C., Robison R., & Gladkykh G. (Eds.) (2024). Strengthening European energy policy: Governance recommendations from innovative interdisciplinary collaborations. Palgrave Macmillan. DOI: https://doi.org/10.1007/978-3-031-66481-6 [in English].

7. Daniel S. A., & Victor S. S. (2024). Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review. *Computer Science & IT Research Journal*, no. 5(3), pp. 576–593. DOI: https://doi.org/10.51594/csitrj.v5i3.872 [in English].

8. Simu S. J., & Zaman F. I. (2023). Advanced cybersecurity strategies for protecting critical infrastructure: Strengthening the backbone of national security. *International Journal of Scientific Research and Management,* no. 11(12), pp. 999–1016. DOI: https://doi.org/10.18535/ijsrm/v11i12.ec07 [in English].

9. Young D. (2025). Protecting critical infrastructure in Nigeria: A framework for integrated cybersecurity approach. *International Journal of Research and Innovation in Social Science,* no. 9(7), pp. 1151–1167. DOI: https://doi.org/10.47772/IJRISS.2025.90700095 [in English].

10. Chen J., Lu Y., Zhang Y., Huang F., & Qin J. (2023). A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction. *International Journal of Critical Infrastructure Protection,* no. 43, Article 100634. DOI: https://doi.org/10.1016/j.ijcip.2023.100634 [in English].

11. Maglaras L., Janicke H., & Ferrag M. A. (2022). Cybersecurity of critical infrastructures: Challenges and solutions. *Sensors,* no. 22(14), Article 5105. DOI: https://doi.org/10.3390/s22145105 [in English].

12. European Commission. (n.d.). NIS2 Directive: Securing network and information systems. *Shaping Europe's Digital Future*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (accessed 27 November 2025) [in English].

The article was submitted to the editorial office on 29 November 2025

УДК 351:004.056.5:004.738.5(477)

В. І. Саричев, О. О. Поплавський, О. В. Черкаський

СИСТЕМА КІБЕРБЕЗПЕКИ ПУБЛІЧНОГО СЕКТОРУ УКРАЇНИ: СТРУКТУРНІ ПРОБЛЕМИ, УПРАВЛІНСЬКІ МОДЕЛІ ТА СТРАТЕГІЧНІ НАПРЯМКИ МОДЕРНІЗАЦІЇ

У статті здійснено комплексне теоретико-методологічне обґрунтування стратегічних засад розвитку системи кібербезпеки у публічному секторі України в умовах цифрової трансформації, євроінтеграції та повномасштабної збройної агресії. На основі аналізу чинного законодавства, Стратегії кібербезпеки та Стратегії інформаційної безпеки України, а також міжнародних стандартів (NIS 2, NIST CSF 2.0, Zero Trust Architecture) систематизовано сучасні підходи до кіберзахисту публічних інституцій. Уточнено зміст базових категорій теорії державного управління, адаптованих до сфери кібербезпеки публічного сектору, зокрема таких як система кібербезпеки у публічному секторі, стратегічні засади розвитку системи кібербезпеки, механізми державного управління у сфері кібербезпеки. Виявлено ключові глобальні тренди та національні виклики, а також структурні проблеми державної системи кібербезпеки: фрагментарність нормативного регулювання, нерівномірність кіберзрілості органів влади, дефіцит кадрів, слабкий розвиток ризик-орієнтованого управління й культури безпеки, обмеженість партнерської взаємодії з бізнесом і громадянським суспільством.

Запропоновано систему стратегічних цілей і принципів розвитку кібербезпеки публічного сектору, орієнтовану на забезпечення стійкості публічних послуг, інтегрованості управлінського стандарту та інституціоналізацію багаторівневого партнерства. Розроблено концептуальну модель стратегічного розвитку системи кібербезпеки, що включає нормативно-стратегічний, інституційно-управлінський, процесно-політичний, технологічний, кадрово-освітній, партнерський та моніторингово-оцінювальний блоки, а також окреслено комплекс інструментів реалізації, моніторингу та оцінювання ефективності, придатних для практичного використання в органах державної влади та місцевого самоврядування.

Ключові слова: *кібербезпека, публічний сектор, державне управління, стратегічні засади, NIS 2, NIST CSF, Zero Trust, кіберзрілість, державна політика, цифрова трансформація, кіберстійкість.*

Sarychev Volodymyr – Doctor of Economics, Associate Professor, Professor of the Department of Economics and Economic Security, University of Customs and Finance
http://orcid.org/0000-0002-8544-9901

Poplavskyi Oleh – Candidate of Technical Sciences, Associate Professor, Head of the Department of Military Training, University of Customs and Finance
https://orcid.org/0000-0002-9023-9992

Cherkaskyi Oleksandr – Postgraduate student, State University of Information and Communication Technologies
https://orcid.org/0009-0006-3105-5217