JEL Classification: M15; F63; O33 **DOI**: https://doi.org/10.31521/modecon.V52(2025)-01

Burkovska Anna, PhD (Economics), Associate Professor of the Department of Management, Business and Administration, Mykolayiv National Agrarian University, Mykolayiv, Ukraine

ORCID ID: 0000-0003-0563-6967
e-mail: anna.burkovskaya12@gmail.com

Strategic Prospects for Managing Computer Networks and Information Systems in the Context of Digital Transformation and Global Cyberspace Integration

Abstract. Introduction*. In today's global digital age, the development and integration of computer networks and information systems have become vital strategic priorities. As the global economy becomes more dependent on data-centric operations, secure and scalable IT infrastructures become increasingly important. These infrastructures serve as a foundation for sustainable technological advancement and inclusive digital growth worldwide. This study explores how contemporary digital solutions, such as cloud computing, cybersecurity architectures, and intelligent network management, foster international connectivity, drive digital innovation, and strengthen the resilience of national economies amid ongoing global digital integration.*

Purpose. *This research primarily seeks to evaluate the strategic potential and practical impact of advancing computer networks and information systems within the context of global digital transformation. The study emphasizes identifying critical enablers, challenges, and policy tools that facilitate integration into the global digital ecosystem. Particular focus is given to adherence to international standards, technological interoperability, and robust cybersecurity measures.*

Results. *The findings of this research indicate that advanced digital infrastructure plays a crucial role in enhancing information exchange, fostering innovation ecosystems, and reinforcing economic and administrative resilience. Technologies such as cloud computing, AI-driven systems, and transnational data networks help overcome technological isolation and encourage greater participation in the global digital economy. A comparative review of international best practices, particularly those implemented by leading digital economies, reveals their potential for adaptation in developing and emerging markets.*

Conclusions. *Modernizing computer networks and information systems is a fundamental driver of sustainable global integration and achieving digital sovereignty. Overcoming obstacles such as obsolete infrastructure, regulatory gaps, and limited access to digital competencies requires coordinated action, international collaboration, and alignment with global digital standards. Ultimately, these efforts will lead to improved service efficiency, stronger cybersecurity, and greater inclusion in the global digital economy.*

Keywords: *digital infrastructure management; computer networks; global integration; information systems; cybersecurity; digital development.*

УДК 338:658.012

Бурковська А. І., доктор філософії (економіка), доцент кафедри менеджменту, бізнесу та адміністрування, Миколаївський національний аграрний університет, Миколаїв, Україна

Стратегічні перспективи управління комп'ютерними мережами та інформаційними системами в умовах цифрової трансформації та інтеграції до світового кіберпростору

Анотація. *Розвиток і інтеграція комп'ютерних мереж та інформаційних систем є одним із ключових стратегічних напрямів глобального цифрового прогресу, що суттєво впливає на економічну стабільність, ефективність державного управління та конкурентоспроможність на міжнародному рівні. В умовах, коли світова економіка дедалі більше базується на даних, цифрових технологіях і автоматизованих процесах, критичної ваги набуває створення надійної, безпечної та сумісної ІТ-інфраструктури. У дослідженні розглядається внесок сучасних цифрових рішень - таких як хмарні технології, системи кібербезпеки та інтелектуальне управління мережами - у процес інтеграції до глобального цифрового середовища, зміцнення кіберстійкості держав та розвиток цифрової економіки. Особливу увагу приділено стратегічним можливостям країн, що розвиваються, у впровадженні інноваційних цифрових технологій, а також подоланню ключових викликів, зокрема через застарілу інфраструктуру, нестачу кваліфікованих кадрів із цифровими навичками та фрагментарне правове регулювання. Порівняльний аналіз міжнародного досвіду провідних цифрових держав свідчить, що ефективне управління цифровими системами значно підвищує здатність адаптуватися до глобальних викликів, забезпечує безперервність критично важливих процесів і прискорює цифрову трансформацію суспільства. Формування сучасних інформаційних систем відповідно до міжнародних стандартів і принципів цифрової безпеки розглядається як основа сталого технологічного розвитку, зміцнення міжнародного співробітництва та забезпечення цифрового суверенітету.*

Ключові слова: *управління цифровою інфраструктурою; комп'ютерні мережі; глобальна інтеграція; інформаційні системи; кібербезпека; цифровий розвиток.*

JEL Classification: *M15; F63; O33*

[1]**Стаття надійшла до редакції**: 27.08.2025
Received: 27 August 2025

Formulation of the problem. In today's rapidly digitalizing and interconnected world, computer networks and information systems have become essential components of global infrastructure. They support key operations in finance, international commerce, public administration, and social interaction. The reliability, scalability, and security of these systems directly influence global economic stability, innovation capacity, and societal security [1].

However, the rapid evolution of digital technologies, explosive data growth, and increasingly complex IT architectures present significant challenges to managing digital infrastructure globally. Escalating cybersecurity threats capable of undermining governments, disrupting essential services, and endangering global safety underscore the urgent need for more sophisticated and coordinated responses. Effective network management today demands automation, cloud-native architectures, AI integration, and robust international cooperation in cybersecurity [2].

Although international standards and regulatory frameworks exist, there are still significant disparities in digital governance. Many nations and institutions struggle with technology adoption, workforce shortages of digital skills, and fragmented cybersecurity strategies [3].

These conditions highlight the critical need for a unified strategic vision in the governance of computer networks and information systems - one that is grounded in globally recognized standards, powered by advanced technologies, and committed to fostering a resilient cybersecurity culture [4]. Only through coordinated global efforts can we safeguard the stability, security, and effectiveness of digital infrastructure in an increasingly complex and vulnerable digital landscape.

Analysis of recent research and publications. Recent academic literature has thoroughly explored the evolution of computer networks and information systems, as well as their growing strategic significance. Once considered primarily technical tools for automating manual tasks, information systems have become core components of organizational strategy. The emergence of networking technologies and the proliferation of the World Wide Web marked a transformative period, repositioning IT from a supporting function to a strategic enabler of interorganizational and international collaboration [2]. This progression reflects a paradigm shift in management - from an emphasis on technical details to aligning IT with broader business goals and global dynamics.

Digital transformation now extends far beyond technological enhancements, fundamentally reshaping organizational structures and operations. It places technology at the heart of strategic planning, encouraging innovation, agility, and operational efficiency [5]. Consequently, network management must evolve in tandem, shifting from a siloed technical activity to a strategic discipline tightly integrated with organizational change. The widely accepted definition of digital transformation as the reconfiguration of business processes through the widespread use of digital technologies [4] further illustrates the inseparable relationship between technology and strategic management in the modern context.

Although integrating computer networks and information systems into the global digital infrastructure offers substantial benefits, it also introduces significant complexities and risks. These issues stem from increasingly sophisticated supply chains, rapid technological changes, and inconsistent global regulations. The increasing number of cyber threats and the constant evolution of attack methods require enhanced international cooperation to secure digital assets and ensure equitable access to the benefits of digitalization [6]. Additionally, the unequal distribution of cyber capabilities among nations and organizations contributes to a widening digital divide that must be addressed through inclusive strategic planning.

Strategic management in the digital era relies on established principles and evolving frameworks. Traditional concepts, such as resource optimization, competitive positioning, and goal alignment, remain relevant but must be adapted to the rapidly changing digital environment. Strategic Information Systems Planning (SISP) is especially valuable in this context, offering a comprehensive methodology to ensure investments in IT infrastructure support long-term organizational goals [7]. The SISP process involves several key phases: developing strategic awareness, analyzing the current state, exploring strategic alternatives, crafting an actionable plan, and effectively implementing it. Models such as Porter's Five Forces and the Value Chain are central to this process, underscoring the importance of integrating IT strategy with the broader business landscape. By aligning technology initiatives with corporate objectives, SISP helps organizations maximize the value of their digital investments - a necessity in an era of continuous transformation.

Formulation of research goals. The primary objective of this research is to identify strategic approaches and practical solutions for developing and integrating computer networks and information systems in Ukraine, in line with global digital progress and integration into the international digital ecosystem.

To realize this overarching goal, the study pursues the following specific objectives:

- to analyze the current state, historical development, and strategic significance of computer networks and information systems in Ukraine and globally, emphasizing their role in driving globalization and digital transformation;
- to identify the key technological, economic, organizational, and regulatory factors that shape the development, deployment, and strategic governance of these systems in the context of global digital integration;

- to examine best practices and strategic initiatives from leading digital nations in areas such as digital infrastructure, cybersecurity, and cross-border information system integration, considering their applicability in the Ukrainian context;
- to evaluate the influence of digital transformation and the integration of computer networks and information systems on Ukraine's socioeconomic development, including their effects on public administration, business processes, education, and cybersecurity.

By addressing these objectives, the research aims to provide a scientifically grounded framework for advancing Ukraine's digital infrastructure and promoting its effective integration into the global digital landscape, thereby enhancing national competitiveness and cyber resilience amid ongoing digital transformation.

Outline of the main research material. In the digital era, effectively confronting the growing complexities of cybersecurity threats is a pivotal element in the strategic management of computer networks and information systems. Recent statistics reveal a sharp rise in the financial impact of cybercrime, with global costs projected to reach unprecedented levels in the coming years [8]. Table 1 presents data illustrating this concerning trend as reported by multiple sources. This rapid escalation underscores the critical need for robust cybersecurity frameworks that can protect organizational resources and ensure uninterrupted operations. The evolving threat landscape is further exacerbated by the increasing sophistication of cyberattacks, many of which now exploit artificial intelligence, thereby demanding the deployment of advanced, adaptive security technologies and strategies.

Table 1 **Projected Growth of Cybercrime Costs**

Year	Projected Global Cost (USD Trillion)
2025	10,5
2024	9,2
2028	13,8
2023	8,0
2027	24,0

Джерело: built by the author on the basis of [9]

In the digital era, a core component of strategic management is addressing the escalating risks posed by cybersecurity threats. With the financial toll of cybercrime projected to reach unprecedented levels in the near future, there is an urgent need for robust, proactive cybersecurity frameworks. Table 1 illustrates these trends based on data from multiple sources. As cyberattacks become more sophisticated, including those that use artificial intelligence, organizations must adopt advanced tools and strategies to protect their digital assets and maintain operational resilience.

Adopting established cybersecurity frameworks is critical to building a strong security posture. Frameworks such as the NIST Cybersecurity Framework (version 2.0) and ISO 27001 offer structured methodologies for identifying, protecting against, detecting, responding to, and recovering from cyber threats [10]. NIST CSF 2.0 expands its scope beyond critical infrastructure and emphasizes governance, establishing it as a benchmark for cybersecurity maturity. ISO 27001 provides an internationally recognized standard for evaluating and validating information security management systems. Other frameworks, such as the CIS Critical Security Controls and COBIT, provide prioritized actions and governance structures for comprehensive IT management [11]. Aligning and customizing these frameworks with organizational goals and regulatory contexts is vital for effectively mitigating cyber risk.

In response to AI-enhanced cyber threats, AI-powered technologies are becoming indispensable in cybersecurity operations [10]. AI systems excel at anomaly detection, predictive analytics, identifying the root cause of issues, and providing automated threat alerts. They can process vast volumes of network data, allowing them to uncover subtle patterns that traditional approaches may miss. Furthermore, AI facilitates automated vulnerability detection, patch management, and real-time responses to sophisticated threats, including zero-day exploits and advanced persistent threats. Investing in and integrating AI-driven cybersecurity solutions is essential for sustaining organizational defenses in this dynamic threat environment.

Global cybersecurity management must also consider broader governance issues and the need for international collaboration. Although various frameworks and regulations aim to bolster cyber resilience, a lack of harmonization across jurisdictions creates challenges regarding compliance and coordination [12]. Diverging national approaches – such as those rooted in the concept of cyberspace sovereignty - further complicate cooperation. A secure global cyberspace requires the joint efforts of governments, the private sector, and

individuals, supported by shared norms, legal agreements, and strategies for collective defense and information sharing.

The strategic management of computer networks and information systems must also incorporate emerging technologies that are reshaping how systems are developed, deployed, and maintained. Cloud computing, artificial intelligence, the Internet of Things (IoT), and next-generation networking technologies offer significant advantages in terms of agility, scalability, and innovation. Cloud platforms enable flexible resource allocation, AI enhances automation and analytics, IoT devices collect real-time operational data, and advanced networks support higher data throughput and lower latency [13].

When adopted strategically, these technologies can foster operational efficiency, business innovation, and improved network resilience. For instance, AI-powered network management systems offer self-healing capabilities, minimizing downtime and optimizing performance [13]. Digital transformation, driven by these tools, enhances communication across supply chains, supports automated processes, and promotes data-informed decision-making. This improves competitiveness and adaptability.

However, integrating such technologies introduces new security challenges that must be proactively addressed. Expanding cloud adoption necessitates robust security and compliance measures. The proliferation of IoT devices increases the attack surface, making networks more vulnerable [10]. While AI is useful for defense, it also presents risks, such as model exploitation and the weaponization of AI technologies. Addressing these threats requires strategic planning, adopting comprehensive security frameworks, implementing cutting-edge detection systems, and providing regular training to foster an organizational culture that is security-aware [14].

Analyzing the digital transformation strategies of advanced economies provides valuable guidance for other nations. For instance, Ukraine has achieved a global ranking of fifth in digital public service delivery [9], exemplifying its successful digital government initiatives. Similarly, Greece's Digital Transformation Bible 2020-2025 outlines a comprehensive vision supported by targeted interventions and measurable objectives. These cases underscore the importance of political will, coherent national strategies, and sustained investment in digital infrastructure as defining traits of successful digital economies.

Ukraine and other emerging economies are rapidly advancing in their digital transitions by prioritizing public sector innovation and service delivery through digital technologies. Ukraine's Diia platform is an effective model of digital transformation for an emerging market [15]. Table 2 outlines Ukraine's IT sector's key metrics for 2024, emphasizing its growing role in the global digital economy. Despite this progress, however, these economies still face critical challenges, including infrastructure gaps, evolving cybersecurity needs, and the imperative to harmonize national systems with international digital standards.

Table 2 **Ukraine's IT Industry Statistics and Rankings (2024)**

Ranking/Statistic	Value/Rank
Global Ranking in Online Services Index	5th
Global Startup Ecosystem Index Ranking	46th
The Network Readiness Index Ranking	46th
E-Government Development Index Score (out of 1)	0.88
IT Services Export Value (USD Billion)	6,4
Share of IT Services Export in GDP	3,4%
Number of Operating Legal Entities Providing IT Services	9,6k
Number of Active Verified IT Companies	2118
Total Number of IT Specialists	300k

Джерело: built by the author on the basis of [13]

Comparing the experiences of leading digital nations with those of emerging economies like Ukraine makes it possible to identify best practices and transferable models for strategic network management and global integration. Ukraine's digital governance model, for example, has been proposed as a replicable model for other countries to follow. Analyzing the common themes and effective approaches of successful digital economies can provide valuable guidance for organizations and policymakers seeking to navigate digital transformation and global cyberspace integration.

Conclusions. In the context of digital transformation and integration into global cyberspace, the strategic management of computer networks and information systems presents a multifaceted challenge that requires a comprehensive and adaptive approach. In the global digital era, these systems are becoming increasingly strategic priorities, necessitating a shift from purely technical management to a more holistic perspective that aligns with broader business objectives and addresses the complexities of a globally interconnected and threat-prone environment. Robust cybersecurity measures informed by established frameworks and increasingly leveraging AI-powered systems are paramount to safeguarding digital infrastructure and data. While the strategic adoption of emerging technologies, such as

cloud computing, AI, and the Internet of Things (IoT), offers significant opportunities for innovation, efficiency gains, and enhanced resilience, it also introduces new security considerations that must be proactively managed.

A comparative analysis of digital transformation strategies and infrastructure development across leading and emerging economies – particularly Ukraine's notable progress in digital public services – provides valuable insights into best practices and transferable models. Organizations and policymakers must consider the need for continuous investment in cybersecurity, strategic alignment of IT initiatives with business goals, fostering a culture of digital literacy and innovation, and engaging in international cooperation to address global cyberspace challenges.

Future research in this rapidly evolving field could explore several promising avenues. The long-term impact of artificial intelligence (AI) on network security and management, particularly the development of autonomous security systems and the mitigation of AI-powered cyber threats, warrants further investigation. The evolution of global cyber governance, including harmonizing international regulations and establishing shared norms, is also a critical area for scholarly inquiry. Additionally, the role of digital infrastructure in promoting sustainable development and fostering digital inclusion across diverse economies is a significant and timely research direction. Continued exploration of these areas will be essential for navigating the future of computer networks and information systems in an increasingly digital and interconnected world.

References:

1. Sahid, A., Maleh, Y., & Belaissaoui, M. (2020). Information System Evolution. *Strategic Information System Agility: From Theory to Practices*, 29-66. DOI: https://doi.org/10.1108/978-1-80043-810-120211004.
2. Mihu, C., Pitic, A. G., & Bayraktar D. (2023). Drivers of Digital Transformation and their Impact on Organizational Management. *Studies in Business and Economics*, 18(1), 149-170. https://doi.org/10.2478/sbe-2023-0009.
3. Zybareva, O., Kravchuk, I., Pushak, Y., Verbivska, L., & Makeieva, O. (2021). Economic and Legal Aspects of the Network Readiness of the Enterprises in Ukraine in the Context of Business Improving. *Studies of Applied Economics*, 39(5). https://doi.org/10.25115/eea.v39i5.4972.
4. Grynko, T., Hviniashvili, T., & Filippova, V. (2023). Change management in business structures under the conditions of digitalization. *Efektyvna ekonomika*, 5. http://doi.org/10.32702/2307-2105.2023.5.22.
5. Poltorak, A., Sukhorukova, A., & Burkovska, A. (2021). Cybersecurity in the business organization management transformation system. *Transformation of business organization management: current trends and challenges*, 158-176. https://drive.google.com/file/d/1FaGdRZPIgQRhVjPXSeYenmY45UYOD5Js/view.
6. Granville, L. Z., da Rosa, D. M., Panisson, A., Melchiors, C., Almeida, M. J. B., & Tarouco, L. M. R. (2007). Managing computer networks using peer-to-peer technologies. *Computers & Electrical Engineering*, 33(6), 444-461. https://doi.org/10.1016/j.compeleceng.2007.07.003.
7. Priyadarsini, M., & Bera, P. (2021). Software defined networking architecture, traffic management, security, and placement: A survey. *Computer Networks*, 192, 108047. https://doi.org/10.1016/j.comnet.2021.108047.
8. Wan, H., Liu, G., & Zhang, L. (2021, October 22-24). *Research on the application of artificial intelligence in computer network technology* [Conference presentation abstract]. Proceedings of the 2021 5th International Conference on Electronic Information Technology and Computer Engineering, Xiamen University, Xiamen, China, 704-707.
9. Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering cybercrime risks in financial institutions: Forecasting information trends. *Journal of Risk and Financial Management*, 15(12), 613. https://doi.org/10.3390/jrfm15120613.
10. Aboubakar, M., Kellil, M., & Roux, P. (2022). A review of IoT network management: Current status and perspectives. *Journal of King Saud University – Computer and Information Sciences*, 34(7), 4163-4176. https://doi.org/10.1016/j.jksuci.2021.03.006.
11. Dhanya, V. G., Subeesh, A., Kushwaha, N. L., Vishwakarma, D. K., Kumar, T., Ritika, G., & Singh, A. N. (2022). Deep learning based computer vision approaches for smart agricultural applications. *Artificial Intelligence in Agriculture*, 6, 211-229. https://doi.org/10.1016/j.aiia.2022.09.007.
12. Logeshwaran, J., Ramkumar, M., Kiruthiga, T., & Sharanpravin, R. (2022). The role of integrated structured cabling system (ISCS) for reliable bandwidth optimization in high-speed communication network. *ICTACT Journal on Communication Technology*, 13(1), 2635-2639. https://doi.org/10.21917/ijct.2022.0389.
13. Pandey, P., & Kapoor, A. (2025). Cybercrime in the digital era: Impacts, awareness, and strategic solutions for a secure future. *Sachetas*, 4(1), 32-37. https://doi.org/10.55955/410004.
14. Exarchou, V., Aspridis, G., & Savvas, I. (2022). The digital transformation of human resource management in Greece. A critical review. *The Poprad Economic and Management*, 10, 372.
15. Shtal, T. V., & Plekhanov, K. V. (2023). Ukraine's position in international rankings assessing the level of digital development of countries. *Digital Economy and Economic Security*, 8(08), 22-28. https://doi.org/10.32782/dees.8-5.