

DOI: <https://doi.org/10.35774/econa2025.02.001>

JEL classification: L86, H56, L86, O33, D83

UDC: 004:338:2

Yaroslav IZMAILOV

DSc (Economics), Professor,
Professor of Department of Tax Administration,
State Tax University, Ukraine
E-mail: izmyar@ukr.net
ORCID iD: 0000-0003-4853-205X

Iryna YEGOROVA

PhD, Associate Professor,
Department of International Relations,
State University of Economics and Technology, Ukraine
E-mail: yegorova_ig@kneu.dp.ua
ORCID iD: 0000-0002-7800-2810

Roman BARYTSKYI

PhD student,
State Tax University, Ukraine
E-mail: r.baritskiy@gmail.com
ORCID iD: 0009-0006-0421-741X

DIGITALIZATION DEVELOPMENT AND CYBER THREAT COUNTERACTION AS DETERMINANTS OF GLOBAL SECURITY

ABSTRACT

Introduction. The theoretical foundations of the digitalization of the economy, its role in ensuring sustainable development, and productivity growth are considered. Special attention is given to cybersecurity issues accompanying digital transformation, particularly in the context of global instability. The peculiarities of forming information security policies in Ukraine and abroad are revealed. Recommendations are proposed to improve the management of digital risks in the public sector and at the enterprise level. Priorities for improving the regulatory framework and developing the institutional infrastructure for cybersecurity are identified. Conclusions are made regarding the necessity of harmonizing digital strategies with the national security system.

Goal. The aim of the article is to substantiate the importance of ensuring the security of the state from internal and external threats through the improvement of cybersecurity and the digitalization of the economy.

Method (methodology). The following methods were used in the research process: dialectical, generalization, comparison, systemic analysis, observation of economic activities, graphical methods, and others.

Results. Under modern conditions, the digital economy has acquired strategic importance, becoming a critically vital component of national security on par with military defence. Effective protection of the state from internal and external threats is impossible without a balanced and secure digital system, which must be based on a well-thought-out policy of protection against cyber threats. Since the onset of the full-scale

© Yaroslav Izmailov, Iryna Yegorova, Roman Barytskyi, 2025

Received: 02.05.2025

Accepted: 17.05.2025

Published: 28.05.2025



This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 license, which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cite as: Izmailov, Y., Yegorova, I., & Barytskyi, R. (2025). Digitalization development and cyber threat counteraction as determinants of global security. *Economic analysis*, 35 (2), 1-11. DOI: <https://doi.org/10.35774/econa2025.02.001>

aggression of the Russian Federation against Ukraine, partner countries have been collecting and analysing not only the advantages and disadvantages of certain types of weapons and tactics but also the resilience to the threats of digitalization in both the public and private sectors of the economy. In addition to military threats, the rapid development of artificial intelligence technologies worldwide is opening up new horizons and risks for increasing efficiency in various fields of the economy and governance. It has been established that the advancement of modern technologies, particularly artificial intelligence, generates new threats to national security that require a prompt adaptation of relevant cyber defence strategies. Emphasis is placed on the necessity of modernizing digital infrastructure and actively implementing digital solutions in strategically important sectors – such as defence, healthcare, and others. Attention is drawn to strengthening the protection of critical infrastructure and citizens' personal data, as well as developing effective regulatory frameworks in the field of digital technologies. It is determined that the combination of digitalization measures and cybersecurity efforts can produce significant synergistic effects: enhancing trust in digital services, stimulating economic growth, and improving the efficiency of public administration and business. It is substantiated that solving digital security issues is critically important for preserving economic stability and national sovereignty, and the proposed initiatives will contribute to increasing Ukraine's innovative potential and international competitiveness.

Keywords: digitalization; cybersecurity; digital economy; artificial intelligence; information security; institutional infrastructure; digital risks

Introduction

In the context of the full-scale war with the Russian Federation currently unfolding in Ukraine, there has been a marked deterioration in key macroeconomic indicators. These negative trends are likely to deepen further, presenting the country with the urgent task of adapting swiftly to emerging challenges. At the same time, digitalization and the implementation of digitized services are becoming critically important for ensuring the effective functioning of the economy and the security of the state amid global transformations. The modern world demands digital security on par with military security, as a balanced and resilient digital infrastructure is a crucial component in protecting against both internal and external threats.

Since the onset of Russia's full-scale aggression against Ukraine, partner countries have been actively analysing not only the military aspects of the conflict, but also the resilience of governmental and private digital systems to threats associated with digitalization. Alongside military threats, the rapid development of artificial intelligence technologies brings both new opportunities and emerging risks for improving efficiency across various sectors of the economy and public administration. The use of these technologies is accompanied by a growing number of cyber threats, which is particularly relevant in the context of external aggression and hybrid warfare.

These circumstances necessitate a revision and adaptation of the national strategies for digitalization and cybersecurity in line with the new realities. The integration of artificial intelligence into the field of national cybersecurity has the potential to significantly strengthen the state's ability to respond to cyber threats. However, for such initiatives to be effectively implemented, it is essential to establish an appropriate regulatory and legal framework that ensures the security of digital tools and promotes the responsible use of emerging technologies.

Under these conditions, the digital front becomes no less critical than the military one, as reliable digital infrastructure is indispensable for maintaining robust business activity within the country and for ensuring Ukraine's effective defence. Therefore, prompt and decisive action is required to guarantee digital security and support the stability of the national economy.

Given that the issues of digital and information security in Ukraine during wartime remain underexplored and continue to provoke considerable discussion, this topic is of exceptional relevance for academic investigation.

The issues of economic security, digitalization, and digital transformation have been reflected in the scientific works of Ukrainian scholars such as L. Akimova [1], O. Amosov [2], Z. Varnaliy [3], A. Galchynskyi [4], V. Heiets [5], A. Krysovatyi [6], S. Svirko [7], V. Semynozhenko [8], A. Sukhorukov [9], and A. Chukhno [10]. General aspects of

digitalization and state protection against cyber threats are among the research interests of international scholars such as J. Delmon [11], M. Bromwich [12], L. Bernstein [13], W. Behrens [14], P. M. Havranek [15], E. Nikbakht [16], M. Porter [17], and W. Sharpe [18], among others. A review of the existing literature reveals that the challenges and prospects of digitalization, cybersecurity, and artificial intelligence—and their impact on national security and the sustainable functioning of all sectors of the economy—remain insufficiently addressed.

Purpose and Objectives of the Article

The purpose of this article is to substantiate the importance of safeguarding the state from internal and external threats through the enhancement of cybersecurity and the digitalization of the economy.

In the course of this research, the following methods were employed: dialectical analysis, generalization, comparison, systems analysis, observation of economic activity, graphical modelling, economic and statistical analysis, among others.

Presentation of the Main Research Findings

In most modern states, the implementation of information and communication technologies (ICT) and the development of digital society elements are considered among the highest priorities of national strategy and public policy. The application of digital tools and the social interactions associated with them create a digital environment that now serves as a key factor for economic functioning, unlocking innovation potential, raising educational standards, enhancing public administration efficiency, and promoting democratic development.

Digitalization has gradually evolved from an auxiliary tool into a fundamental component of sustainable development strategies. Its significance and influence on global transformational processes are expected to grow steadily amidst the continuous evolution of technological innovation.

The public policy of digital development in the European Union is marked by a distinct strategic dimension. It is based on the implementation of the comprehensive “Digital Agenda” initiative, which is being executed at both national and

supranational levels with the aim of fostering digital transformation and creating a Single Digital Market within the EU.

Thus, digital evolution serves as an indicator of the deep integration of digital technologies into societal processes. Its impact is evident not only in the economic domain—where it drives productivity and competitiveness – but also across a wide range of sectors, from education and healthcare to public administration and cybersecurity. In this context, digitalization is no longer merely a technological trend but a powerful instrument for strengthening resilience and security on a global scale.

The evolution of digital approaches necessitates the refinement of mechanisms and forms of communication within economic relations. The active use of ICT promotes the intensification of information exchange, transforms the roles and authority of market participants, and contributes to deeper decentralization in public and corporate governance systems.

As a result, a new socio-economic reality has emerged—one that demands the comprehensive implementation of digital economy policy at the national level. This includes the modernization of legal and regulatory frameworks, the development of strategic policy documents, and the launch of large-scale digital transformation programs, particularly involving the transition of public administration to innovative digital technologies.

Digital development focuses on ensuring broad population access to modern information technologies, while digital transformation involves the integration of digital tools with existing analog processes to achieve functional synergy. In the business sector, digital transformation is realized through the systematic adoption of cutting-edge technologies that alter business models, product and service structures, management paradigms, and the core directions of enterprise activity. At the same time, digital development aims to ensure inclusive access to ICT—including hardware and software – for all segments of the population.

The pathways for strengthening Ukraine’s national security and defence capabilities by improving the level of digital security are illustrated in Figure 1.

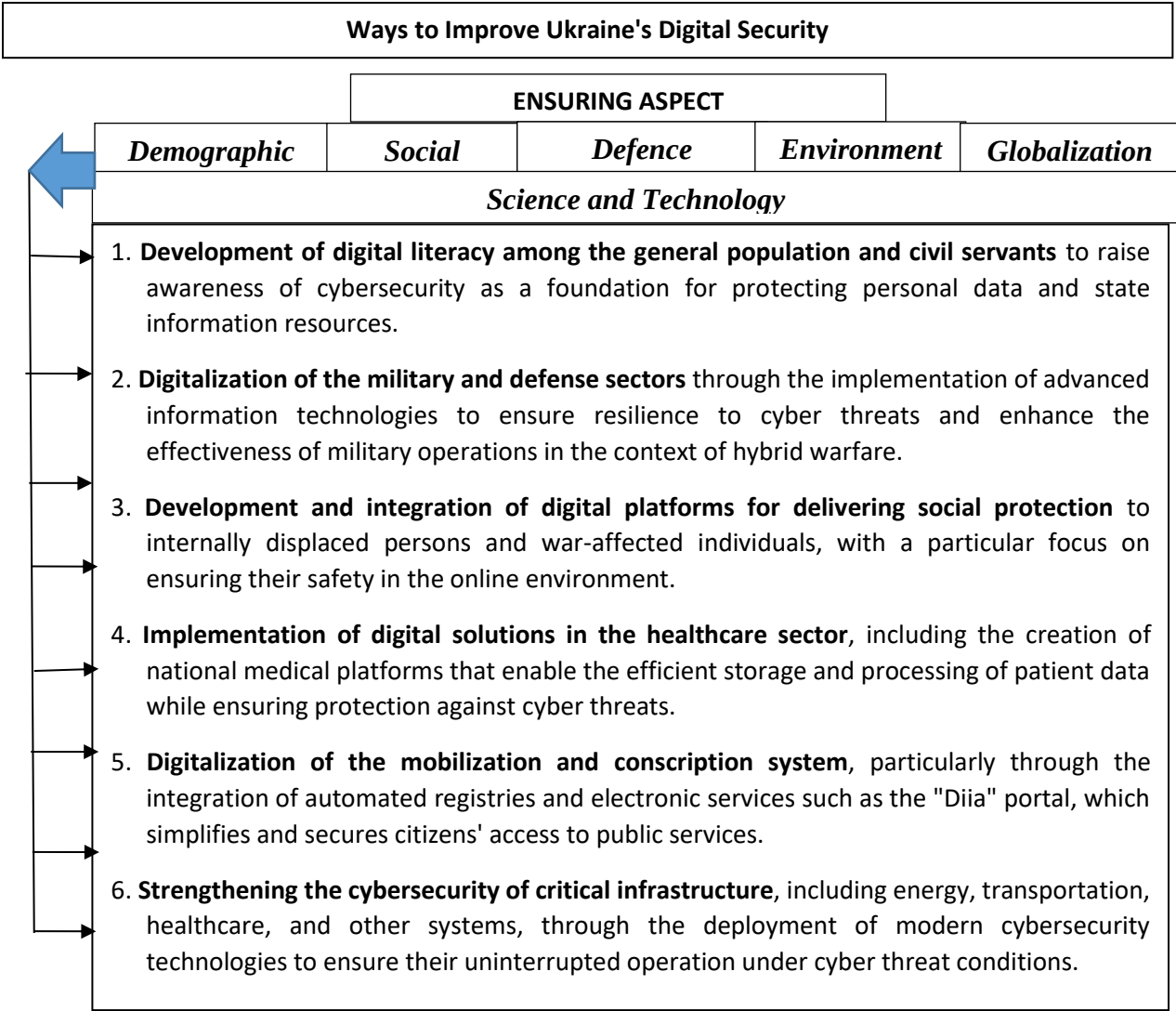


Fig. 1. Pathways for Enhancing Ukraine’s Digital Security

Note: compiled by the authors.

In Figure 1, the proposed elements reflect key pathways for enhancing the level of digital security in Ukraine through the integration of modern technologies across various sectors of society. These elements include both strategic and practical steps to ensure the protection of information systems and personal data in the face of contemporary cyber threats. Among the most important aspects are the development of digital literacy to raise cybersecurity awareness, the digitalization of defence structures and healthcare, and the implementation of innovative platforms for social protection. Particular attention is paid to strengthening the protection of critical infrastructure and developing a national cybersecurity strategy, which will enable the country to respond effectively to cyber threats. All

of these measures aim to ensure the stable functioning of both public and private sectors in the digital age, where cybersecurity is an integral component of national security.

Given the continuous advancement of technologies, digital security will remain one of the most critical challenges for the European Union. Focusing on the protection of information confidentiality, integrity, and availability—along with the development of a comprehensive legal framework, application of risk management practices, organization of incident response, initiation of cybersecurity awareness programs, and promotion of international cooperation—the EU aims to reinforce its information security capacity.

A core element of the EU's digital security policy is the Network and Information Security (NIS) Directive, the first pan-European legislative act in the field of cybersecurity. This directive is aimed at ensuring a high level of cybersecurity among member states by requiring them to develop national strategies and capabilities, appoint responsible authorities and contact points, foster cooperation and information sharing at the EU level, and ensure that essential service and digital service providers take the necessary measures to protect their systems and report incidents.

In January 2023, the original NIS Directive was replaced by NIS2, which introduced stricter requirements and expanded its scope to cover additional sectors and organizations deemed vital to the EU's economy and society. NIS2 also addressed supply chain security, simplified reporting obligations, and harmonized penalties across the EU [19].

The European Union also promotes research and innovation to strengthen its capacity in the field of information security and to enhance strategic autonomy. Under the "Digital Europe" programme for 2021–2027, the EU committed to investing €1.6 billion to enhance cybersecurity capabilities and support large-scale implementation of cybersecurity infrastructure and tools across public institutions, businesses, and civil society. Additionally, the EU supports the development of a European network of cybersecurity competence centers and the creation of a coordinating hub that drives research and innovation initiatives, pools expertise and resources, and provides cybersecurity policy advice [20].

Based on the analysis of literature sources [1–18] and practical experience, the primary cyber threats to the digital economy today are identified as follows:

1. Cyberattacks on critical infrastructure – attacks targeting energy, transportation, financial, and other vital sectors that may lead to significant economic and social disruptions.
2. Malware – the use of viruses, trojans, and rootkits to compromise computer systems, steal confidential data, or extort ransom.
3. Phishing and social engineering – manipulation of users to steal personal data, passwords, financial information, or gain access to corporate systems.
4. Supply chain attacks – compromising suppliers or partners to infiltrate organizational networks, potentially causing data breaches or financial losses.
5. Attacks on blockchain and cryptocurrency platforms – threats related to vulnerabilities in cryptocurrency networks and decentralized financial instruments (DeFi), potentially resulting in theft or transaction manipulation.
6. DDoS attacks – large-scale distributed denial-of-service attacks on internet services, platforms, or infrastructure, leading to temporary or permanent unavailability of essential digital services.
7. Data breaches – unauthorized access to personal or financial information, potentially resulting in financial loss and loss of trust in digital services.
8. Unauthorized access to corporate databases – malicious intrusions into business systems to steal intellectual property, financial data, or customer information, seriously affecting organizational competitiveness.

Figure 2 presents the main problems and threats, the necessary steps, and actions required to ensure the country's operational efficiency and security through improvements in cybersecurity and digitalization. It also illustrates the synergistic effects of the proposed measures.

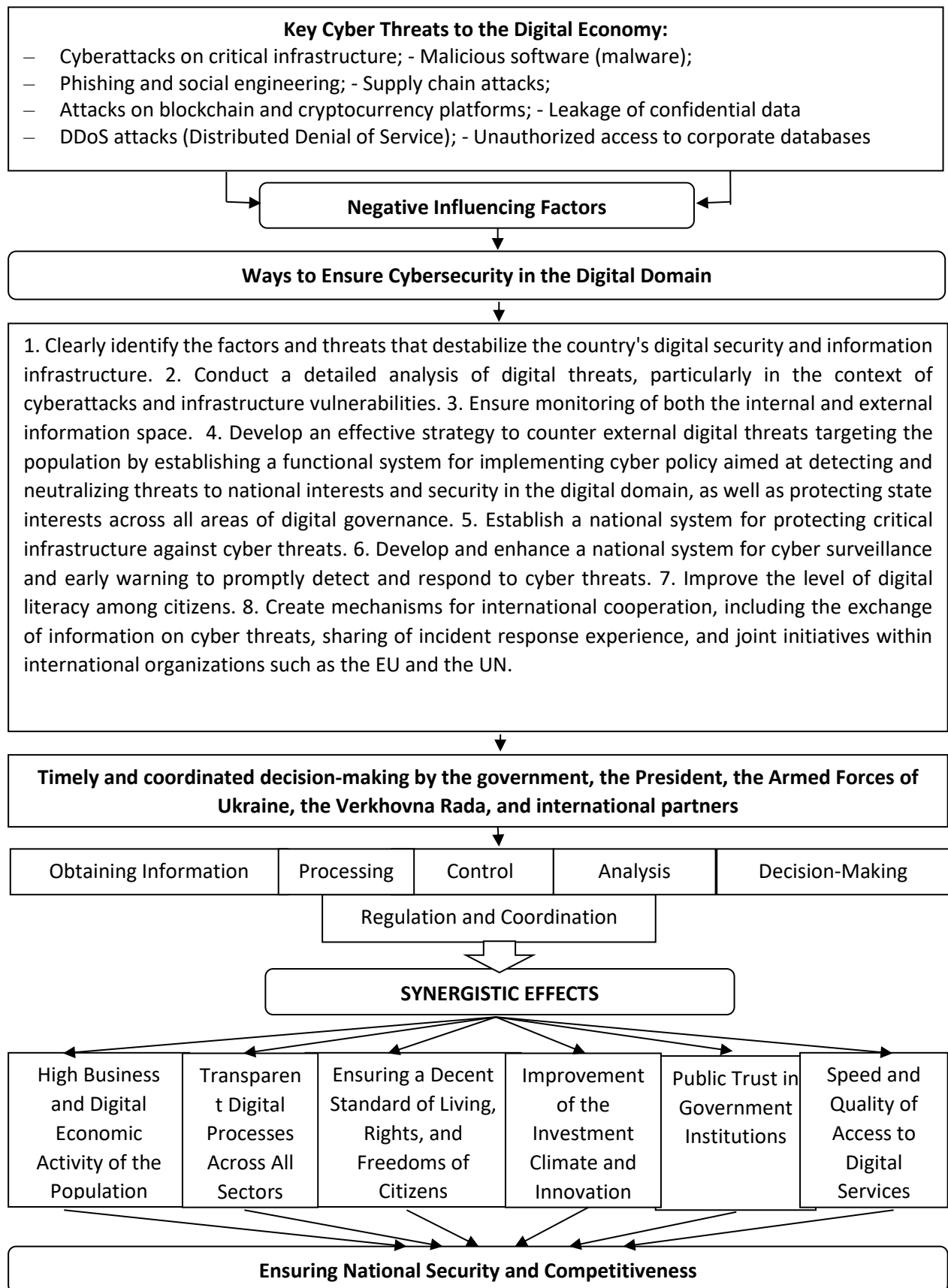


Fig. 2. Synergistic Effects of Enhancing Cybersecurity and Digitalization

Note: Compiled by the authors

The structural framework presented in Figure 2 illustrates the influence of challenges and prospects related to digitalization and cybersecurity enhancement on national functioning, highlighting the synergistic effects that, in turn, positively impact national security and the quality of life of citizens. Enhancing cybersecurity and digitalization can generate significant synergistic effects for the country, contributing to national security development, economic resilience, and increased innovation potential. The key synergistic effects are identified as follows:

1. Increased public trust in digital technologies. Improved cybersecurity fosters greater trust among citizens and businesses in digital platforms and online services. This, in turn, stimulates the digitalization of public and business processes, as a secure environment forms the foundation for widespread technology adoption.

2. Efficiency of economic processes. Digitalization leads to greater automation and efficiency in economic processes, while enhanced cybersecurity ensures the reliable protection of critical infrastructure, increasing the stability of economic systems and reducing cyber-related risks for enterprises and government agencies.

3. High business and digital economic activity among the population. The improvement of digitalization and cybersecurity promotes the development of secure and accessible online platforms for businesses and citizens, enabling faster financial transactions, e-commerce, and entrepreneurial opportunities. This fosters economic activity at all levels—from small enterprises to large corporations—and stimulates the development of new sectors, particularly in the tech and digital economy.

4. Transparent digital processes across all domains. Digitalization and cybersecurity support the creation of transparent and efficient governance systems, where every process stage is traceable and auditable. This enhances accountability and openness in government and business structures, reduces corruption risks, improves public service delivery, and strengthens interaction between the state, enterprises, and citizens.

5. Ensuring a decent quality of life, rights, and freedoms. The development of cybersecurity

and digitalization aims to protect citizens' rights and freedoms in the digital space, including data privacy, confidentiality, and safety. Access to digital resources and services also enables broader access to education, healthcare, and social services, improving overall living standards and social equity.

6. Public trust in state institutions. When public institutions effectively implement digital technologies with a focus on cybersecurity, this strengthens citizens' trust in governance. Citizens feel their data is secure, and government services are transparent and accessible, encouraging greater participation in digital initiatives and cooperation with authorities.

7. Speed and quality of digital service delivery. Advances in digital technologies and cybersecurity enable faster and more convenient access to public and private services for citizens and businesses. This includes e-health, e-education, social protection, and business services. Enhanced speed and service quality reduce administrative burdens and improve government performance and citizen satisfaction.

8. Improved investment climate. A secure digital environment fosters favourable conditions for domestic and foreign investment in technology and digital innovation. This supports the growth of startups, tech companies, and research initiatives, driving economic development.

9. Growth of innovation potential. A secure digital environment in both public and private sectors facilitates the adoption of advanced technologies such as artificial intelligence, blockchain, the Internet of Things (IoT), and other innovative solutions, enhancing the efficiency of various economic sectors.

10. Strengthening national security. Enhanced cybersecurity protects national information resources and critical infrastructure from cyber threats posed by both state and non-state actors, ensuring the stability of governance and economic and social processes.

11. Reduction of cybercrime and economic losses. Improving cybersecurity effectiveness helps reduce cybercrime and the costs of incident recovery, such as data breaches or attacks. It also mitigates financial losses for businesses and the state.

12. Development of a skilled workforce. The growing digitalization requires new competencies across fields—from programming to cybersecurity. This promotes education and workforce development, positively impacting the overall level of technological literacy in the country.

13. Enhancing the country's international competitiveness. A country that successfully integrates cybersecurity and digitalization into its national strategies becomes more competitive globally, particularly in international trade, global supply chains, investment, and technological expansion.

These effects are mutually reinforcing, creating the conditions for a more resilient, innovative, and secure digital economy – one that forms the basis for sustainable development and socio-economic growth.

Conclusions and Prospects for Further Research

As a result of the conducted study, key aspects of ensuring the country's digital security under conditions of external aggression were analysed. It was established that digital threats associated with technological advancement – particularly the development of artificial intelligence – pose new challenges to national security. Alongside traditional military threats, Ukraine must actively improve its digital infrastructure and adapt its cybersecurity strategy to new realities.

The main measures and pathways for enhancing digital security in Ukraine were examined. A strategic priority is the integration of modern technologies into key sectors, notably defence and healthcare. Special attention is given

to strengthening the protection of critical infrastructure and ensuring the reliable safeguarding of citizens' personal data. The study emphasizes the need to develop a legal and regulatory framework to guarantee the security of digital platforms and promote the responsible use of emerging technologies.

The principal synergistic effects stemming from the advancement of digitalization and cybersecurity in Ukraine were highlighted. Specifically, improved cybersecurity will foster increased public trust in digital technologies, stimulate economic processes, and enhance the efficiency of governance and business operations. Strengthening the digital infrastructure will also ensure broader access to high-quality digital services for the population, thereby positively influencing quality of life and the level of social services.

The study demonstrates that solving the issue of digital security is essential for maintaining economic stability and national security amid contemporary cyber threats. The proposed measures for improving digital infrastructure and cybersecurity form a solid foundation for developing the country's innovation potential, ensuring economic resilience, and enhancing its international competitiveness.

The outlined proposals and recommendations in the digital sphere provide a framework for further academic research and practical solutions aimed at strengthening national security and promoting sustainable development across nations.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акімова Л. М. Діджиталізація як фактор розвитку економіки України. *Економічні студії*. 2024. С. 25-30.
2. Амоша О. М. Кібербезпека у цифрову еру: проблеми та перспективи. *Кібернетика та інформаційні технології*. 2024. Т. 5, № 3. С. 12-18.
3. Варналій З. І. Цифрова трансформація в Україні: економічний та соціальний вимір. *Інноваційний розвиток України*. 2023. Т. 2, № 4. С. 9-13.
4. Гальчинський А. В. Вплив цифровізації на державне управління. *Управління та інновації*. 2023. Т. 1, № 2. С. 30-35.
5. Геєць В. П. Діджиталізація економіки України: теорія і практика. *Науковий вісник*. 2024. Т. 7, № 4. С. 18-22.
6. Крисоватий А. І. Стратегії цифрової трансформації в Україні. *Інноваційні економічні системи*. 2024. Т. 1, № 3. С. 10-14.

7. Свірко С. А. Кібербезпека: міжнародний досвід і проблеми України. *Інформаційна безпека*. 2023. Т. 4, № 2. С. 45-50.
8. Семиноженко В. М. Діджиталізація як стратегічний інструмент розвитку економіки. *Науковий журнал «Інновації»*. 2024. Т. 2, № 5. С. 35-40.
9. Сухоруков А. Ю. Кіберзахист як основа цифрової безпеки. *Кібернетика*. 2024. Т. 5, № 4. С. 15-19.
10. Чухно А. П. Кібербезпека в умовах глобальних цифрових змін. *Наукові дослідження в економіці*. 2023. Т. 3, № 7. С. 35-39.
11. Delmon J. Digital Economy Models in the Context of Globalization. *Journal of Global Digital Economics*. 2024. Vol. 5, No. 2. P. 40-45.
12. Bromwich M. Information Security in the Age of Digital Change. *Cybersecurity & Digital Transformation*. 2024. Vol. 3, No. 4. P. 15-20.
13. Bernstein L. Digitalization in Public Administration. *Digital Governance Review*. 2023. Vol. 6, No. 1. P. 20-25.
14. Berens V. A. Cybersecurity in the Context of Digital Technology Development. *International Cybersecurity Journal*. 2024. Vol. 8, No. 2. P. 30-35.
15. Havranek P. M. Cyber Protection Issues in the Global Digital Economy. *Global Cybersecurity Challenges*. 2023. Vol. 10, No. 4. P. 50-55.
16. Nikbaht E. Business Process Transformation through Digital Technologies. *Digital Business Innovation*. 2024. Vol. 7, No. 3. P. 10-15.
17. Porter M. Strategic Aspects of the Digital Economy. *Harvard Business Review*. 2023. Vol. 102, No. 5. P. 25-30.
18. Sharp U. Innovations in Cybersecurity to Ensure the Digital Economy. *International Journal of Cybersecurity*. 2024. Vol. 11, No. 3. P. 19-24.
19. Proposal for directive on measures for high common level of cybersecurity across the Union. *The Commission has adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive)*. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
20. Integration of Ukraine into the single digital market of the European Union: challenges, opportunities and obstacles. URL: <http://eu-ua-csp.org.ua>

REFERENCES

1. Akimova, L. (2024). Digitalization as a factor of Ukraine's economic development. *Economic Studies*, (2024), 25-30.
2. Amosha, O. (2024). Cybersecurity in the digital age: Problems and prospects. *Cybernetics and Information Technologies*, 5(3), 12-18.
3. Varnaliy, Z. (2023). Digital transformation in Ukraine: Economic and social dimensions. *Innovative Development of Ukraine*, 2(4), 9-13.
4. Halchynskyi, A. (2023). The impact of digitalization on public administration. *Management and Innovation*, 1(2), 30-35.
5. Heiets, V. (2024). Digitalization of Ukraine's economy: Theory and practice. *Scientific Bulletin*, 7(4), 18-22.
6. Krysovatiy, A. (2024). Strategies for digital transformation in Ukraine. *Innovative Economic Systems*, 1(3), 10-14.
7. Svirko, S. (2023). Cybersecurity: International experience and challenges in Ukraine. *Information Security*, 4(2), 45-50.
8. Semynozhenko, V. (2024). Digitalization as a strategic tool for economic development. *Innovation Scientific Journal*, 2(5), 35-40.
9. Sukhorukov, A. (2024). Cyber protection as the basis of digital security. *Cybernetics*, 5(4), 15-19.
10. Chukhno, A. (2023). Cybersecurity under global digital change. *Scientific Research in Economics*, 3 (7), 35-39.

11. Delmon, J. (2024). Digital economy models in the context of globalization. *Journal of Global Digital Economics*, 5 (2), 40-45.
12. Bromwich, M. (2024). Information security in the age of digital change. *Cybersecurity & Digital Transformation*, 3 (4), 15-20.
13. Bernstein, L. (2023). Digitalization in public administration. *Digital Governance Review*, 6(1), 20-25.
14. Berens, V. (2024). Cybersecurity in the context of digital technology development. *International Cybersecurity Journal*, 8 (2), 30-35.
15. Havranek, P. (2023). Cyber protection issues in the global digital economy. *Global Cybersecurity Challenges*, 10 (4), 50-55.
16. Nikbaht, E. (2024). Business process transformation through digital technologies. *Digital Business Innovation*, 7 (3), 10-15.
17. Porter, M. (2023). Strategic aspects of the digital economy. *Harvard Business Review*, 102 (5), 25-30.
18. Sharp, U. (2024). Innovations in cybersecurity to ensure the digital economy. *International Journal of Cybersecurity*, 11(3), 19-24.
19. European Commission. (2025). *Proposal for directive on measures for high common level of cybersecurity across the Union (NIS 2 Directive)*. <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union>
20. EU-Ukraine Civil Society Platform. (2025). *Integration of Ukraine into the single digital market of the European Union: Challenges, opportunities and obstacles*. <http://eu-ua-csp.org.ua>

Ярослав Ізмайлов, доктор економічних наук, професор, професор кафедри адміністрування податків, Державний податковий університет, Україна

Ірина Єгорова, кандидат економічних наук, доцент, доцент кафедри міжнародних відносин, Державний університет економіки і технологій, Україна

Роман Барицький, аспірант, кафедра обліку та аудиту, Державний податковий університет, Україна

Розвиток цифровізації та протидія кіберзагрозам як чинники глобальної безпеки

АНОТАЦІЯ

Вступ. Розглянуто теоретичні основи цифровізації економіки, її роль у забезпеченні сталого розвитку та зростання продуктивності. Особливу увагу приділено проблемам кібербезпеки, які супроводжують цифрову трансформацію, особливо в умовах глобальної нестабільності. Розкрито особливості формування політики інформаційної безпеки в Україні та за кордоном. Запропоновано рекомендації щодо підвищення ефективності управління цифровими ризиками в публічному секторі та на рівні підприємств. Визначено пріоритети для вдосконалення нормативної бази та розбудови інституційної інфраструктури кіберзахисту. Зроблено висновки про необхідність гармонізації цифрових стратегій із системою національної безпеки.

Мета. Метою статті є обґрунтування важливості забезпечення безпеки держави від внутрішніх і зовнішніх загроз через удосконалення кібербезпеки та цифровізації економіки.

Метод (методологія). В процесі проведеного дослідження використані наступні методи: діалектичний, узагальнення, порівняння, системного аналізу, спостереження за господарською діяльністю, графічний та ін.

Результати. У сучасних умовах цифрова економіка набула стратегічного значення, ставши критично важливою складовою національної безпеки будь-якої країни на рівні з військовою. Ефективний захист держави від внутрішніх та зовнішніх ворогів неможливий без збалансованої та захищеної цифрової системи, в основі якої повинна лежати продумана політика захисту від кіберзагроз. З початку повномасштабної агресії Російської Федерації проти України, країнами-партнерами збираються та аналізуються переваги та недоліки не тільки певних видів зброї і тактик, а й стійкості до загроз цифровізації та діджиталізації державного та приватного сектору економіки. Крім військових загроз, інтенсивний розвиток технологій штучного інтелекту в світі відкриває нові горизонти та загрози для підвищення ефективності в різноманітних сферах економіки й управління. Встановлено, що розвиток сучасних технологій, зокрема штучного інтелекту, породжує нові загрози для національної безпеки, що потребують оперативної адаптації відповідної стратегії кіберзахисту. Наголошено на необхідності модернізації цифрової інфраструктури та активного впровадження цифрових рішень у стратегічно важливі сфери – оборону, охорону здоров'я тощо. Зроблено акцент на посиленні захисту критично важливих

об'єктів та персональних даних громадян, а також на формуванні ефективного нормативно-правового регулювання у сфері цифрових технологій. Визначено, що поєднання заходів із цифровізації та забезпечення кібербезпеки може створити значні синергетичні ефекти: посилення довіри до цифрових сервісів, стимулювання економічного зростання, підвищення ефективності державного управління та бізнесу.

Доведено що вирішення проблем цифрової безпеки є критично важливим для збереження економічної стабільності та національного суверенітету, а запропоновані ініціативи сприятимуть підвищенню інноваційного потенціалу та міжнародної конкурентоспроможності України.

Ключові слова: цифровізація; кібербезпека; цифрова економіка; штучний інтелект; інформаційна безпека; інституційна інфраструктура; цифрові ризики

Як цитувати: Ізмайлов Я., Єгорова І., Барицький Р. Розвиток цифровізації та протидія кіберзагрозам як чинники глобальної безпеки. *Економічний аналіз*. 2025. Том 35. № 2. С. 1-11. DOI: <https://doi.org/10.35774/econa2025.02.001>