ЕКОНОМІКА

UDC 339.92(477:4)

DOI: https://doi.org/10.32782/2520-2200/2025-5-1

Buriak Alona
PhD in Economics, Associate Professor of the Department
of International Economic Relations and Tourism,
National University "Yuriy Kondratyuk Poltava Polytechnic"
ORCID: https://orcid.org/0000-0002-0814-7459

Maslii Oleksandra
PhD in Economics, Associate Professor of the Department
of Finance, Banking and Taxation,
National University "Yuriy Kondratyuk Poltava Polytechnic"
ORCID: https://orcid.org/0000-0003-2184-968X

Cherviak Anna
PhD, Associate Professor of the Department
of Finance, Banking and Taxation,
National University "Yuriy Kondratyuk Poltava Polytechnic"
ORCID: https://orcid.org/0000-0002-2747-4041

IDENTIFICATION OF DIGITAL RISKS AS A BASIS FOR SECURITY-ORIENTED INTEGRATION OF UKRAINE INTO THE EU DIGITAL SINGLE MARKET

ІДЕНТИФІКАЦІЯ ЦИФРОВИХ РИЗИКІВ ЯК ОСНОВА БЕЗПЕКООРІЄНТОВАНОЇ ІНТЕГРАЦІЇ УКРАЇНИ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС

The article examines digital risk identification as a crucial factor in Ukraine's security-oriented integration into the EU Digital Single Market. It systematically highlights four key categories of digital risks – technological, organizational, social, and geopolitical – and analyzes their significant impact on national and economic security. Using data from ENISA, CERT-UA, and SSSCIP, the study notes a 37% decrease in cyberattacks alongside a 37% increase in digital resilience in 2022–2025. The research contrasts the EU's preventive, ex ante approach with Ukraine's predominantly reactive model, stressing the importance of aligning national strategies with GDPR, NIS2, and DORA. It further recommends establishing a unified digital risk audit system, expanding public-private partnerships, and leveraging AI-based monitoring tools to enhance Ukraine's overall cyber and economic resilience.

Keywords: economic security, EU digital single market, information security, digitalization, security-oriented information environment, digital integration.

У статті досліджено концептуальні засади ідентифікації цифрових ризиків як ключового чинника формування безпекоорієнтованої моделі інтеграції України до Єдиного цифрового ринку Європейського Союзу. Узагальнено підходи до трактування цифрових ризиків як багаторівневого явища, що охоплює технологічні, організаційні, соціальні та геополітичні компоненти, які прямо впливають на рівень національної економічної безпеки. На основі даних Державної служби спеціального зв'язку та захисту інформації України та European Union Agency for Cybersecurity проаналізовано динаміку цифрової стійкості держави у 2022–2025 рр., що демонструє суттєве зниження кількості кібератак та зростання індексу кіберстійкості на 37%. Виявлено структурні розбіжності між підходами України та Європейського Союзу до управління ризиками: у той час як країни Євросоюзу реалізують модель превентивного управління ex ante відповідно до рамкових документів ENISA Risk Framework, в Україні переважає реактивна, державоцентрична система реагування. Уточнено роль інституційних і технологічних чинників у забезпеченні сталого розвитку цифрової економіки, а також необхідність узгодження національної нормативної бази з європейськими регламентами GDPR, NIS2 та DORA. Розроблено аналітичну типологію ризиків цифровізації,

що відображає їх вплив на критичні сфери економіки, фінансову стабільність і довіру до національних інституцій. Запропоновано концептуальні напрями вдосконалення державної політики кібербезпеки, зокрема створення єдиної системи національного аудиту ризиків, розвитку публічно-приватних партнерств у сфері цифрового захисту, підвищення рівня цифрової компетентності та інвестицій, в тому числі іноземних у сучасні технології генеративного штучного інтелекту для адекватного моніторингу основних ризиків та загроз. Результати проведеного дослідження доводять, що ефективна ідентифікація цифрових ризиків є передумовою для формування безпекоорієнтованого середовища, здатного забезпечити стійку інтеграцію України до цифрової економіки Європейського Союзу і підвищити її конкурентоспроможність у глобальному просторі.

Ключові слова: економічна безпека, Єдиний цифровий ринок ЄС, інформаційна безпека, цифровізація, безпекоорієнтоване інформаційне середовище, цифрова інтеграція.

Problem statement. In the current context, digital transformation serves as a system-forming factor for economic growth while simultaneously generating new security challenges. Hybrid wars, cyberattacks on critical infrastructure, information manipulation, and the rapid proliferation of artificial intelligence technologies exacerbate the vulnerability of the state's digital systems. For Ukraine, which is in the process of integrating into the EU Digital Single Market, the identification of digital risks becomes particularly crucial as a foundation for establishing a preventive security management system. This task holds strategic importance for harmonizing with European cybersecurity standards, enhancing investment attractiveness, and ensuring sustainable economic development in both wartime and post-war conditions.

Analysis of recent research and publications. Recent research increasingly emphasizes the dual nature of digital transformation as both a driver of economic growth and a potential source of systemic risks to national security. Razumkov Centre highlights that active digitalization processes, when implemented without harmonization with European regulatory frameworks, generate new classes of technological, organizational, and behavioral risks that can compromise economic stability [1, pp. 90–116]. These findings underscore the necessity for states to formalize risk assessment procedures, combining quantitative metrics, such as probability and potential losses, with qualitative indicators like institutional maturity and digital culture.

The European Union Agency for Cybersecurity [2] identifies a growing prevalence of complex cyber threats targeting critical infrastructure and underscores the importance of preventive, ex ante risk management approaches. Such strategies, as codified in the Digital Europe Strategy, NIS2, and DORA regulations, prioritize early detection, modeling, and mitigation of risks, contrasting with reactive frameworks observed in many emerging economies, including Ukraine. Similarly, Cho H., Sung J.-H., Kang H.-J., Jang J., Shin D. [4] develop quantitative models for cyber resilience assessment, highlighting the need for availability-based metrics and robust normalization methods to guide national cybersecurity strategies effectively.

Haas T.C. [9] illustrates sector-specific vulnerabilities, showing how inadequate cybersecurity measures can extend even into non-traditional domains such as wildlife protection and critical environmental monitoring. Complementing these findings, Ristvej J., Tonhauser M., Chovanec D. et al. [6] propose conceptual models aligned with EU NIS2 standards, advocating for multi-level frameworks that integrate national authorities, private stakeholders, and civil society in a preventive risk-management ecosystem.

State-level analyses provide further empirical evidence of risk reduction and resilience gains. CERT-UA [5] and the State Service of Special Communications and Information Protection of Ukraine [3] report notable declines in cyber incidents and improvements in organizational readiness between 2022 and 2025, reflecting the gradual institutionalization of digital risk management at both governmental and corporate levels. Coppolino et al. [11] demonstrate that the application of digital twin technology and AI-based monitoring systems can further enhance situational awareness and proactive mitigation of digital threats in critical infrastructure contexts.

Collectively, these studies suggest that Ukraine's gradual convergence with EU cybersecurity standards is both feasible and strategically necessary, provided that institutional coordination, investment in technology, and human capital development are systematically strengthened.

The aim of the article. The aim of the article is to provide a systematic justification of the role of digital risk identification in shaping a security-oriented model for Ukraine's integration into the EU digital single market, as well as to determine the key directions for aligning national risk management policies with European cybersecurity standards.

Presentation of the main research material. In the current context, digital transformation has become not only a driving force for economic growth but also a significant risk factor for national security. Military events, cyberattacks, data manipulation, and the uncontrolled proliferation

of artificial intelligence technologies have turned digitalization into an environment where potential threats often outweigh its benefits.

According to research [1], active digitalization in Ukraine after 2020 occurred without full regulatory integration into European standards, resulting in the emergence of a new class of risks – systemic, technological, and behavioral. Scientific studies [7; 12] emphasize that a state's digital vulnerability increasingly determines the actual level of economic security, as breaches of data integrity and information system functionality lead to direct financial losses and reputational risks.

The challenge of formalizing digitalization risks lies in the need for both quantitative and qualitative descriptions of threats, identification of their sources, estimation of their likelihood, assessment of their impact on critical economic sectors, and integration of this information into management decision-making systems.

The concept of "digital risk" is understood as the probability of an event related to the use of digital technologies that may cause negative economic, social, or security consequences. In this context, risk formalization involves not only their identification but also the construction of a system linking threat sources, response mechanisms, and economic security indicators.

According to the approaches presented in report [1, pp. 90 – 94], digitalization risks are classified into four conceptual groups (table 1):

1. Technological risks – vulnerabilities of digital systems, data loss, attacks on critical infrastructure.

2. Organizational risks – regulatory deficiencies, lack of data control, inconsistencies between sectors.

3. Social risks – digital inequality, insufficient user education, spread of disinformation.

4. Geopolitical risks – impacts of international conflicts, sanctions, and transnational corporations.

The typological analysis indicates that the most critical risks for Ukraine's economic security in 2025 are technological and geopolitical, the levels of which remain high despite the strengthening of the national cybersecurity system. In turn, social and organizational risks are long-term in nature and require the development of digital trust institutions aligned with GDPR, NIS2, and DORA regulations.

Ukraine's digital threat prevention system has a multi-level structure, ranging from national strategies to corporate protocols. Key mechanisms for preventing digital threats include:

Regulatory and legal mechanisms – cybersecurity standards, legal definition of digital risks, adaptation to EU regulations.

Organizational and managerial mechanisms – establishment of digital security centers, integration of CERT-UA systems, coordination with NATO.

Technological mechanisms – use of AI, Big Data, and cloud platforms for automatic anomaly detection.

Social and educational mechanisms – development of digital competencies, STEM education, and awareness-raising programs on cyber risks.

A key role is played by institutional synergy between state bodies (SSSCIP, Ministry of Digital Transformation, NSDC) and international partners (ENISA, EBRD, UNDP, NATO CCDCOE), which ensures a shift from reactive to preventive risk management.

According to [1, p. 110], around 42% of Ukrainian companies in 2024 implemented internal protocols for assessing digitalization risks, an 18% increase compared to 2021, indicating a strengthening of corporate-level digital security.

The European Union manages digital risks through integrated policies, including the Digital Europe Strategy, Digital Decade 2030, DORA, and the EU Cybersecurity Strategy. A key feature of these approaches is the shift from reactive to preventive management, focusing on early detection and risk modeling.

Comparative analysis shows that in 2024–2025, Ukraine has approached European cybersecurity

Table 1

Typology of digitalization risks and their impact on Ukraine's economic security

Risk Category	Key Manifestation	Economic Consequences	Example Indicators
Technological	Cyberattacks, server failures, data loss	IT company losses, sectoral GDP decline	Cyber resilience index, share of digital incidents
Organizational	Regulatory uncertainty	Loss of tax revenues, reduced trust	GDPR compliance level, share of digitized processes
Social	Digital inequality, disinformation	Decreased labor productivity, social tension	Digital skills index, share of online education
Geopolitical	Cyberwarfare, sanctions, external attacks	Risks to energy, transport, and financial sectors	Number of attacks on critical infrastructure

Source: compiled based on data from [1; 3]

standards; however, the main areas for further harmonization remain:

– developing a national risk management system in accordance with the ENISA Risk Framework;

– creating a centralized cyber incident response portal;

– implementing a national cyber risk audit for critical infrastructure enterprises;

– improving the educational and digital training of personnel.

Thus, Ukraine's digital risk management model is gradually shifting from a sectoral to an integrated risk management approach, corresponding to the EU's "cyber resilience by design" concept. The main difference identified in comparison is that EU countries focus on systematic interaction between the state, business, and civil society, whereas Ukraine still predominantly uses a state-centric approach. To overcome this asymmetry, researchers [4; 6–7; 9–12] propose the development of public-private partnerships in the field of digital security.

The dynamics of Ukraine's digital security development in 2022–2025 are characterized by increased cyber resilience, growing digital maturity of state administration institutions, and enhanced participation in EU cybersecurity initiatives. According to analytical reports by CERT-UA and the Ministry of Digital Transformation of Ukraine, the number of critical incidents decreased by 32% compared to 2022, while the digital readiness index increased by nearly 20 points.

To detail these trends, table 2 presents the key digital security indicators for Ukraine over the past four years.

According to Table 2, during 2022–2025, Ukraine has demonstrated systematic strengthening of digital security across three key dimensions:

Technological dimension – a significant 37% increase in the cyber resilience index indicates the effectiveness of the Cyber Resilience Ukraine and Digital Security Partnership programs, supported by the EU and UNDP.

Institutional dimension – the expansion of digital maturity in the public sector from 48% to 70% reflects a shift toward risk-oriented management of information flows in accordance with the ENISA Risk Framework standards.

Educational and competency dimension – a 74% increase in cyber education programs results from the establishment of a network of Cyber Academies within the EU4Digital initiative.

Despite positive trends, the share of GDP allocated to cybersecurity remains low (0,32%), three times below the EU average of 0,9%. This highlights the need to strengthen state funding for digital security systems and to expand business participation in joint programs for the protection of critical infrastructure.

Thus, Ukraine demonstrates steady convergence with European cybersecurity standards, developing its own digital security model oriented toward adaptation to wartime and post-war challenges.

Digitalization simultaneously acts as both a driver and a threat to the state's economic security. Without proper risk management, the digital environment can become a source of financial losses, social conflicts, and erosion of trust in institutions.

Formalization of digitalization risks requires a systemic approach that combines quantitative assessments (probability, losses, criticality) with qualitative factors (institutional maturity, digital culture).

Ukraine is gradually implementing European standards for digital risk management; however, a gap remains between regulatory provisions and

Table 2

Key digital security indicators of Ukraine in 2022–2025

Indicator	2022	2023	2024	2025 (forecast)	2022–2025 dynamics, %
Number of recorded cyberattacks	24,3	20,8	17,6	15,2	–37,4
Share of critical incidents, %	42	36	29	26	–38,1
Cyber resilience index (0–100 scale)	54	61	68	74	+37,0
Digital maturity level of the public sector, %	48	56	63	70	+45,8
Share of GDP allocated to cybersecurity, %	0,21	0,25	0,28	0,32	+52,4
Number of cyber education programs (public & private)	85	104	126	148	+74,1
Volume of international technical assistance in cybersecurity, EUR	37	54	69	82	+121,6
Share of enterprises implementing cybersecurity technologies, %	27	34	42	51	+88,9

Source: compiled based on data from [2–3; 5; 8]

practical implementation. International EU experience demonstrates the effectiveness of models based on ex ante risk management principles – i.e., preventive actions that reduce the likelihood of threats.

The development of Ukraine's security-oriented digital ecosystem should be based on four key directions: alignment with EU regulations, development of cybersecurity institutions, investment in technology, and human capital.

Conclusions. The research findings confirm that digital risks are a determining factor in the state's economic security. Ukraine has gradually converged with European cybersecurity standards; however, a gap remains between regulatory frameworks and practical implementation. To minimize this gap, it is essential to establish an integrated risk management system, including a national digital threat audit, the development of public-private partnership institutions, cyber education and workforce training, and increased investment in digital infrastructure. Prospects for further research lie in developing models for assessing digital resilience through intelligent data analysis systems, as well as in conducting comparative analyses of the effectiveness of digital integration strategies in Central and Eastern European countries.

References:

1. Razumkov Centre. (2020). Tsyfrova ekonomika: trendy, ryzyky ta sotsialni determinanty [Digital economy: Trends, risks and social determinants]. Kyiv, Ukraine, pp. 90–116.
2. ENISA. (2024). *ENISA Threat Landscape 2024.* European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu
3. Derzhavna sluzhba spetsialnoho zv'yazku ta zakhystu informatsii Ukrainy. (2025). *Zvit pro stan kiberzakhystu ta zabezpechennia funktsionuvannia natsionalnoi systemy kiberbezpeky u 2024–2025 rr.* [Report on the state of cybersecurity and functioning of the national cybersecurity system in 2024–2025]. Kyiv: DSSZZI. Available at: https://cip.gov.ua/ua/news (accessed November 11, 2025).
4. Cho H., Sung J.-H., Kang H.-J., Jang J. & Shin D. (2025). Quantifying Cyber Resilience: A Framework Based on Availability Metrics and AUC-Based Normalization. *Electronics,* no 14(12), 2465. DOI: https://doi.org/10.3390/electronics14122465
5. CERT-UA. (2025). *Annual Report 2024–2025.* State Service of Special Communications of Ukraine. Available at: https://cert.gov.ua
6. Ristvej J., Tonhauser M., Chovanec D., et al. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports,* no 15, 26902. DOI: https://doi.org/10.1038/s41598-025-12829-3
7. Buriak A. & Bachykalo K. (2023). The role of chambers of commerce and industry in ensuring the external economic security of the state. *Economy and Region,* vol. 4(91), pp. 249–254. DOI: https://doi.org/10.26906/EiR.2023.4(91).3220
8. Ministry of Digital Transformation of Ukraine. (2025). *Annual report on digital resilience and cybersecurity.* Available at: https://thedigital.gov.ua
9. Haas T. C. (2023). Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity,* no 9(1), tyad004. DOI: https://doi.org/10.1093/cybsec/tyad004
10. Buriak A. (2017). Investytsiine spivrobitnytstvo mizh Ukrainoiu ta YeS u promyslovosti: rehionalnyi rozriz [Investment cooperation between Ukraine and the EU in industry: regional dimension]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Ekonomika i menedzhment – Scientific Bulletin of the International Humanitarian University. Series: Economics and Management,* vol. 25/2017, pp. 49–53.
11. Coppolino L., Nardone R., Petruolo A., Romano L. & Souvent A. (2023). Exploiting digital twin technology for cybersecurity monitoring in smart grids. In *Proceeding 18th International Conference Availability, Reliability and Security (ARES),* Benevento, Italy, 1–10. DOI: https://doi.org/10.1145/3600160.3605043
12. Maslii O., Buriak A., Chaikina A. & Cherviak A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern-European Journal of Enterprise Technologies,* vol. 1(13(133)), pp. 35–45. DOI: https://doi.org/10.15587/1729-4061.2025.319256

Список використаних джерел:

1. Центр Разумкова. Цифрова економіка: тренди, ризики та соціальні детермінанти. Київ, 2020. С. 90–116.
2. ENISA *Threat Landscape 2024. European Union Agency for Cybersecurity.* URL: https://enisa.europa.eu
3. Державна служба спеціального зв'язку та захисту інформації України. *Звіт про стан кіберзахисту та забезпечення функціонування національної системи кібербезпеки у 2024–2025 рр.* Київ : ДССЗЗІ, 2025. URL: https://cip.gov.ua/ua/news
4. Cho H., Sung J.-H., Kang H.-J., Jang J., Shin D. Quantifying cyber resilience: a framework based on availability metrics and AUC-based normalization. *Electronics.* 2025. Vol. 14, No. 12. P. 2465. DOI: https://doi.org/10.3390/electronics14122465

5. CERT-UA Annual Report (2024–2025). *State Service of Special Communications of Ukraine.* URL: https://cert.gov.ua (дата звернення: 11.11.2025)
6. Ristvej J., Tonhauser M., Chovanec D. та ін. Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. *Scientific Reports.* 2025. Vol. 15. P. 26902. DOI: https://doi.org/10.1038/s41598-025-12829-3
7. Buriak A., Bachykalo K. The role of chambers of commerce and industry in ensuring the external economic security of the state. *Економіка і регіон.* 2023. № 4 (91). С. 249–254. DOI: https://doi.org/10.26906/EiR.2023.4(91).3220
8. Ministry of Digital Transformation of Ukraine (2025). *Annual Report on Digital Resilience and Cybersecurity.* URL: https://thedigital.gov.ua
9. Haas T. C. Adapting cybersecurity practice to reduce wildlife cybercrime. *Journal of Cybersecurity.* 2023. Vol. 9, Issue 1. tyad004. DOI: https://doi.org/10.1093/cybsec/tyad004
10. Буряк А.А. Інвестиційне співробітництво між Україною та ЄС у промисловості: регіональний розріз. *Науковий вісник Міжнародного гуманітарного університету. Серія: «Економіка і менеджмент».* 2017. № 25. С. 49–53.
11. Coppolino L., Nardone R., Petruolo A., Romano L., Souvent A. Exploiting digital twin technology for cybersecurity monitoring in smart grids. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES),* Benevento, Italy, 2023. P. 1–10. DOI: https://doi.org/10.1145/3600160.3605043
12. Maslii O., Buriak A., Chaikina A. & Cherviak A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. *Eastern-European Journal of Enterprise Technologies,* 1(13 (133), 35–45. DOI: https://doi.org/10.15587/1729-4061.2025.319256

Стаття надійшла: 25.10.2025
Стаття прийнята: 10.11.2025
Стаття опублікована: 21.11.2025